МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет»

УТВЕРЖДЕНО

Ученым советом ФГБОУ ВО «ВГУ»

от 30.05.2025 г. протокол № 5

Основная профессиональная образовательная программа высшего образования

10.05.01 Компьютерная безопасность

Специализация: Анализ безопасности компьютерных систем

Уровень высшего образования: специалитет

Квалификация: **Специалист**

Форма обучения: очная

Год начала подготовки: 2025

СОГЛАСОВАНО
Представитель работодателя:

Генеральный директор
АО ИК «ИНФОРМСВЯЗЬ-ЧЕРНОЗЕМЬЕ»

_____ Бодров А. Ю.

М.П.

Воронеж 2025

Утверждение изменений в ОПОП для реализации в 20__/20__ учебном году

ОПОП пересмотрена, обсуждена и одобрена для реализации в 20__/20__ учебном году на заседании ученого совета университета __.__.20__ г. протокол № ___

Заместитель председателя Ученого совета ФГБОУ ВО «ВГУ»
_____ Е.Е. Чупандина
__.__.20__ г.

Утверждение изменений в ОПОП для реализации в 20__/20__ учебном году

ОПОП пересмотрена, обсуждена и одобрена для реализации в 20__/20__ учебном году на заседании ученого совета университета __.__.20__ г. протокол № ___

Заместитель председателя Ученого совета ФГБОУ ВО «ВГУ»
_____ Е.Е. Чупандина
__.__.20__ г.

СОДЕРЖАНИЕ

1. Общие положения

Основная профессиональная образовательная программа (далее – ОПОП) по направлению подготовки/специальности 10.05.01 Компьютерная безопасность представляет собой комплекс основных характеристик образования (объем, содержание, планируемые результаты) и организационно-педагогических условий (материально-техническое, учебно-методическое, кадровое и финансовое обеспечение), который представлен в виде учебного плана, календарного учебного графика, рабочих программ учебных предметов, курсов, дисциплин (модулей), иных компонентов, оценочных и методических материалов, а также рабочей программы воспитания, календарного плана воспитательной работы, форм аттестации.

1.1. Нормативные документы

– Федеральный закон от 29.12.2012 № 273 – ФЗ «Об образовании в Российской Федерации»;

– Федеральный государственный образовательный стандарт по направлению подготовки/специальности 10.05.01 Компьютерная безопасность высшего образования, утвержденный приказом Минобрнауки России от «26» ноября 2020 г. №1459 (далее – ФГОС ВО).

1.2. Перечень сокращений, используемых в ОПОП

ФГОС ВО – федеральный государственный образовательный стандарт высшего образования;

ФУМО – федеральное учебно-методическое объединение;

УК - универсальные компетенции;

ОПК – общепрофессиональные компетенции;

ПК - профессиональные компетенции;

ПООП - примерная основная образовательная программа;

ОПОП – основная профессиональная образовательная программа;

ОТФ - обобщенная трудовая функция;

ТФ - трудовая функция;

ТД - трудовое действие;

ПС – профессиональный стандарт.

2. Характеристика профессиональной деятельности выпускников

2.1. Общее описание профессиональной деятельности выпускников

Области профессиональной деятельности, в которых выпускники, освоившие программу бакалавриата/магистратуры/специалитета, могут осуществлять профессиональную деятельность:

06 Связь, информационные и коммуникационные технологии;

Сферами профессиональной деятельности, в которых выпускники, освоившие программу, могут осуществлять профессиональную деятельность, являются):

сфера защита информации в компьютерных системах и сетях.

Выпускники могут осуществлять профессиональную деятельность и в других областях и (или) сферах профессиональной деятельности при условии соответствия уровня их образования и полученных компетенций требованиям к квалификации работника.

В рамках освоения образовательной программы выпускники готовятся к решению задач профессиональной деятельности следующих типов:

научно-исследовательский;

проектный;

контрольно-аналитический; организационно-управленческий;

эксплуатационный.

2.2. Перечень профессиональных стандартов

Перечень используемых профессиональных стандартов, соотнесенных с федеральным государственным образовательным стандартом по направлению подготовки/специальности 10.05.01 Компьютерная безопасность и используемых при формировании ОПОП приведен в приложении 1.

Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника данной образовательной программы, представлен в приложении 2.

3. Общая характеристика основной профессиональной образовательной программы

3.1. Профиль/специализация образовательной программы

Профиль образовательной программы в рамках направления подготовки/специальности 10.05.01 Компьютерная безопасность – Анализ безопасности компьютерных систем.

3.2. Квалификация, присваиваемая выпускникам образовательной программы

Квалификация, присваиваемая выпускникам образовательной программы: специалист.

3.3. Объем программы

Объем программы составляет 330 зачетных единиц вне зависимости от применяемых образовательных технологий, реализации программы по индивидуальному учебному плану.

Объем программы, реализуемый за один учебный год, составляет не более 70 з.е. вне зависимости от применяемых образовательных технологий, реализации программы по индивидуальному учебному плану (за исключением ускоренного обучения), а при ускоренном обучении – не более 80 з.е.

3.4. Срок получения образования:

в очной форме обучения составляет 5,5 лет.

3.5. Минимальный объем контактной работы

Минимальный объем контактной работы по образовательной программе составляет 5537 часов.

3.6. Язык обучения

Программа реализуется на русском языке.

3.7. Применение электронного обучения и дистанционных образовательных технологий (*в соответствии с ФГОС ВО*)

Реализация программы возможна с применением электронного обучения, дистанционных образовательных технологий в электронной информационно-образовательной среде (ЭИОС) университета и с использованием массовых открытых онлайн курсов (МООК), размещенных на открытых образовательных платформах.

3.8. Рабочая программа воспитания, календарный план воспитательной работы представлены в Приложении 7.

4. Планируемые результаты освоения ОПОП

4.1 Универсальные компетенции выпускников и индикаторы их достижения

В результате освоения программы у выпускника должны быть сформированы следующие **универсальные компетенции**

Таблица 4.1

Категория универсальных компетенций	Код	Формулировка компетенции	Код и формулировка индикатора достижения универсальной компетенции
Системное и критическое мышление	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними УК-1.2 Используя логико-методологический инструментарий, критически оценивает надежность источников информации, анализирует классические и современные философские концепции, определяет возможности их применения для выработки стратегии и разрешения проблемных ситуаций УК-1.3 Анализирует возможные варианты разрешения проблемной ситуации, критически оценивая их достоинства и недостатки
Разработка и реализация проектов	УК-2	Способен управлять проектом на всех этапах его жизненного цикла	УК-2.1. Формулирует конкретную, специфичную, измеримую во времени и пространстве цель, а также определяет дорожную карту движения к цели, исходя из имеющихся ресурсов и ограничений. УК-2.2. Проектирует решение конкретной задачи с учетом возможных ограничений действующих правовых норм. Составляет иерархическую структуру работ, распределяет по задачам финансовые и трудовые ресурсы, использует актуальное ПО. УК-2.3. Проектирует смету и бюджет проекта, оценивает эффективность результатов проекта УК-2.4. Составляет матрицу ответственности и матрицу коммуникаций проекта. УК-2.5. Использует гибкие технологии для реализации задач с изменяющимися во времени параметрами.
Командная работа и лидерство	УК-3	Способен организовывать и руководить работой команды,вырабатывая для достижения поставленной цели	УК-3.1. Планирует организацию работы команды и руководство ею с учетом индивидуально-психологических особенностей каждого ее члена УК-3.2. Вырабатывает конструктивную командную стратегию для достижения поставленной цели УК-3.3. Эффективно взаимодействует с участниками образовательного процесса, соблюдая психологически обоснованные правила и нормы общения
Коммуникация	УК-4	Способен применять современные коммуникативные	УК-4.1. Выбирает на иностранном языке коммуникативно приемлемые стратегии академического и профессионального

		технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	общения. УК-4.2. Владеет культурой письменного и устного оформления профессионально ориентированного научного текста на государственном языке РФ. УК-4.3. Умеет вести устные деловые переговоры в процессе профессионального взаимодействия на государственном языке РФ. УК-4.4. Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ. УК-4.5. Владеет интегративными коммуникативными умениями в устной и письменной иноязычной речи в ситуациях академического и профессионального общения. УК-4.6. Выбирает на государственном языке коммуникативно приемлемые стратегии академического и профессионального общения.
Межкультурное взаимодействие	УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Анализирует историко-культурные традиции различных социальных групп, опираясь на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования). УК-5.2. Выделяет специфические черты и маркеры разных культур, религий, с последующим использованием полученных знаний в профессиональной деятельности и межкультурной коммуникации. УК-5.3. Ориентируется в основных этапах развития истории и культуры России и ее достижениях, учитывает особенности российской цивилизации при взаимодействии с представителями различных культур, оценивая потенциальные вызовы и риски. УК-5.4.1Осознает свою гражданскую идентичность как принадлежность к государству, обществу, культурному наследию страны, ответственность за будущее страны; проявляет активную гражданскую позицию
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6.1. Оценивает свои личностные ресурсы, оптимально их использует для успешного выполнения порученного задания. УК-6.2. Определяет и реализовывает приоритеты своей деятельности и способы ее совершенствования
	УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной	УК-7.1. Выбирает здоровьесберегающие технологии для поддержания здорового образа жизни с учетом физиологических особенностей организма. УК-7.2. Планирует свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и

		деятельности	обеспечения работоспособности. УК-7.3. Соблюдает и пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности. УК-7.4. Осуществляет выбор вида спорта или системы физических упражнений для физического самосовершенствования, развития профессионально важных психофизических качеств и способностей в соответствии со своими индивидуальными способностями и будущей профессиональной деятельностью УК-7.5. Использует методику самоконтроля для определения уровня здоровья и физической подготовленности в соответствии с нормативными требованиями и условиями будущей профессиональной деятельности. УК-7.6. Приобретает личный опыт повышения двигательных и функциональных возможностей организма, обеспечивающий специальную физическую подготовленность в профессиональной деятельности
Безопасность жизнедеятельности	УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1. Идентифицирует и анализирует опасные и вредные факторы элементов среды обитания и в рамках осуществляемой деятельности; знает основные вопросы безопасности жизнедеятельности. УК-8.2. Способен осуществлять действия по предотвращению возникновения чрезвычайных ситуаций природного, техногенного, социального (биолого-социального) происхождения; грамотно действовать в чрезвычайных ситуациях мирного и военного времени, создавать безопасные условия реализации профессиональной деятельности. УК-8.3. Готов принимать участие в оказании первой и экстренной допсихологической помощи при травмах и неотложных состояниях, в том числе в условиях чрезвычайных ситуаций в мирное и военное время. УК-8.4. Способен обеспечить безопасные и/или комфортные условия труда на рабочем месте, в том числе с помощью средств защиты; выявить и устранить проблемы, связанные с нарушениями техники безопасности на рабочем месте.
Экономическая культура, в том числе финансовая грамотность	УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Понимает базовые принципы функционирования экономики. УК-9.2. Понимает основные виды государственной социально-экономической политики и их влияние на индивида. УК-9.3. Использует финансовые инструменты для управления личными финансами (личным бюджетом). УК-9.4. Применяет методы личного экономического и финансового планирования для достижения поставленных целей. УК-9.5. Контролирует собственные

			экономические и финансовые риски.
Гражданская позиция	УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	УК-10.1. Соблюдает антикоррупционные стандарты поведения, выявляет коррупционные риски, противодействует коррупционному поведению в профессиональной деятельности УК-10.2. Поддерживает высокий уровень личной и правовой культуры, выявляет проявления экстремистской идеологии и противодействует им в профессиональной деятельности. УК-10.3. Идентифицирует правонарушения террористической направленности, противодействует проявлениям терроризма в профессиональной деятельности

* При наличии во ФГОС

4.2. Общепрофессиональные компетенции выпускников и индикаторы их достижения

В результате освоения программы у выпускника должны быть сформированы следующие **общепрофессиональные компетенции**:

Таблица 4.2

Категория компетенций	Код	Формулировка компетенции	Код и формулировка индикатора достижения компетенции
	ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ОПК-1.1. Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. ОПК-1.2. Знает классификацию защищаемой информации по видам тайны и степеням конфиденциальности. ОПК-1.3. Знает классификацию и основные угрозы информационной безопасности для объекта информатизации.
	ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1. Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере. ОПК-2.2. Знает логико-математические основы построения электронных цифровых устройств. ОПК-2.3. Знает состав, назначение аппаратных средств и программного обеспечения персонального компьютера. ОПК-2.4. Знает классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей. ОПК-2.5. Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет. ОПК-2.6. Умеет составлять документы, используя прикладные программы офисного назначения. ОПК-2.7. Владеет средствами управления пользовательскими интерфейсами операционных систем. ОПК-2.8. Знает основные принципы конфигурирования и администрирования операционных систем.

			ОПК-2.9. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями. ОПК-2.10. Умеет применять основные методы программирования в выбранной операционной среде. ОПК-2.11. Знает характерные особенности современного программного обеспечения специального назначения. ОПК-2.12. Умеет производить установку, наладку, тестирование и обслуживание программного обеспечения, включая решения отечественного производства. ОПК-2.13. Умеет производить установку, наладку, тестирование и обслуживание сетевого программного обеспечения, включая решения отечественного производства. ОПК-2.14. Умеет производить установку, наладку, тестирование и обслуживание современных программных средств обеспечения информационной безопасности.
	ОПК-3	Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;	ОПК-3.1. Знает основные задачи векторной алгебры и аналитической геометрии. ОПК-3.2. Знает возможности координатного метода для исследования различных геометрических объектов. ОПК-3.3. Знает основные виды уравнений простейших геометрических объектов. ОПК-3.4. Умеет решать основные задачи линейной алгебры. ОПК-3.5. Умеет решать основные задачи аналитической геометрии на плоскости и в пространстве. ОПК-3.6. Владеет навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике. ОПК-3.7. Знает основные свойства важнейших алгебраических систем: групп, колец, полей. ОПК-3.8. Знает основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями. ОПК-3.9. Знает основные свойства колец многочленов над кольцами и полями. ОПК-3.10. Знает основные свойства отображений важнейших алгебраических систем. ОПК-3.11. Умеет производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ. ОПК-3.12. Умеет решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду. ОПК-3.13. Умеет производить оценку качества полученных решений прикладных задач.

			ОПК-3.14. Владеет методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах. ОПК-3.15. Владеет навыками решения типовых линейных уравнений над полем и кольцом вычетов. ОПК-3.16. Владеет навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований. ОПК-3.17. Знает основные понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности. ОПК-3.18. Знает язык и средства современной математической логики и теории логических исчислений. ОПК-3.19. Знает основные способы задания булевых функций и функций многозначной логики формулами и их свойства. ОПК-3.20. Знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов. ОПК-3.21. Умеет производить основные логические операции в исчислении высказываний и исчислении предикатов. ОПК-3.22. Умеет находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах. ОПК-3.23. Умеет оценивать сложность алгоритмов и вычислений ОПК-3.24. Умеет применять методы математической логики и теории алгоритмов к решению задач математической кибернетики. ОПК-3.25. Владеет навыками использования языка современной символической логики. ОПК-3.26. Владеет навыками упрощения формул алгебры высказываний и алгебры предикатов. ОПК-3.27. Владеет навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач. ОПК-3.28. Знает свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур. ОПК-3.29. Знает основные понятия и методы теории графов. ОПК-3.30. Знает основные понятия и методы теории конечных автоматов. ОПК-3.31. Знает основные понятия и методы комбинаторного анализа. ОПК-3.32. Умеет решать задачи периодичности и эквивалентности для линейных рекуррентных

			последовательностей и конечных автоматов. ОПК-3.33. Умеет применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач. ОПК-3.34. Умеет решать оптимизационные задачи на графах. ОПК-3.35. Умеет применять стандартные методы дискретной математики для решения профессиональных задач. ОПК-3.36. Владеет навыками решения типовых комбинаторных и теоретико-графовых задач. ОПК-3.37. Владеет навыками применения языка и средств дискретной математики при решении профессиональных задач. ОПК-3.38. Знает основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных. ОПК-3.39. Знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных. ОПК-3.40. Знает основные методы интегрального исчисления функций одной и нескольких действительных переменных. ОПК-3.41. Знает основные методы исследования числовых и функциональных рядов. ОПК-3.42. Знает основные задачи теории функций комплексного переменного. ОПК-3.43. Знает основные типы обыкновенных дифференциальных уравнений и методы их решения. ОПК-3.44. Умеет обосновывать основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных. ОПК-3.45. Умеет обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных. ОПК-3.46. Умеет обосновывать основные методы интегрального исчисления функций одной и нескольких действительных переменных. ОПК-3.47. Умеет обосновывать основные методы исследования числовых и функциональных рядов. ОПК-3.48. Владеет навыками использования справочных материалов по математическому анализу. ОПК-3.49. Знает основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства. ОПК-3.50. Знает классические предельные теоремы теории вероятностей. ОПК-3.51. Знает основные понятия теории случайных процессов. ОПК-3.52. Знает постановку задач и основные понятия математической статистики.

			ОПК-3.53. Знает стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений. ОПК-3.54. Знает стандартные методы проверки статистических гипотез. ОПК-3.55. Умеет обосновывать классические положения и стандартные методы теории вероятностей и случайных процессов. ОПК-3.56. Умеет обосновывать классические положения и стандартные методы математической статистики. ОПК-3.57. Умеет разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач. ОПК-3.58. Владеет навыками решения основных типов обыкновенных дифференциальных уравнений.
	ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1. Знает основные законы механики и оптики. ОПК-4.2. Знает основные законы термодинамики и молекулярной физики. ОПК-4.3. Знает основные законы электричества и магнетизма. ОПК-4.4. Знает основы теории колебаний и волн, оптики. ОПК-4.5. Знает основы квантовой физики. ОПК-4.6. Умеет использовать математические модели физических явлений и процессов. ОПК-4.7. Умеет решать типовые прикладные физические задачи. ОПК-4.8. Владеет методами исследования физических явлений и процессов. ОПК-4.9. Знает принципы работы элементов и функциональных узлов электронной аппаратуры. ОПК-4.10. Знает методы анализа и синтеза электронных схем. ОПК-4.11. Знает типовые схемотехнические решения основных узлов и блоков электронной аппаратуры. ОПК-4.12. Умеет работать с современной элементной базой электронной аппаратуры. ОПК-4.13. Умеет использовать стандартные методы и средства проектирования цифровых узлов и устройств. ОПК-4.14. Владеет навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры. ОПК-4.15. Владеет навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации. ОПК-4.16. Знает структуру и принципы работы современных и перспективных микропроцессоров. ОПК-4.17. Умеет анализировать и синтезировать электронные схемы. ОПК-4.18. Умеет определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их

			характеристики, тип видеокарты, состав и параметры периферийных устройств. ОПК-4.19. Владеет навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности. ОПК-4.20. Знает фундаментальные закономерности, связанные с получением сигналов и их передачей по каналам связи. ОПК-4.21. Знает фундаментальные закономерности, связанные с обработкой и преобразованием сигналов в информационных системах. ОПК-4.22. Знает функциональное назначение и принципы работы основных блоков современных средств защиты информации.
	ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1. Знает источники и классификацию угроз информационной безопасности. ОПК-5.2. Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России. ОПК-5.3. Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. ОПК-5.4. Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации. ОПК-5.5. Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации. ОПК-5.6. Знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации. ОПК-5.7. Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации. ОПК-5.8. Знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности. ОПК-5.9. Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав.

			ОПК-5.10. Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации. ОПК-5.11. Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации. ОПК-5.12. Умеет формулировать основные требования информационной безопасности при эксплуатации компьютерной системы. ОПК-5.13. Умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации. ОПК-5.14. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. ОПК-5.15. Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации. ОПК-5.16. Знает возможности технических средств перехвата информации. ОПК-5.17. Умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам. ОПК-5.18. Знает нормативные документами в области технической защиты информации. ОПК-5.19. Владеет методами и средствами технической защиты информации.
	ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации. ОПК-6.2. Знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях. ОПК-6.3. Знает систему организационных мер, направленных на защиту информации ограниченного доступа. ОПК-6.4. Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа. ОПК-6.5. Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем. ОПК-6.6. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем. ОПК-6.7. Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в

			организации. ОПК-6.8. Умеет определить политику контроля доступа работников к информации ограниченного доступа. ОПК-6.9. Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации. ОПК-6.10. Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.
	ОПК-7	Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	ОПК-7.1. Знает общие принципы построения, области и особенности применения языков программирования высокого уровня. ОПК-7.2. Знает язык программирования высокого уровня (объектно-ориентированное программирование). ОПК-7.3. Знает язык ассемблера персонального компьютера. ОПК-7.4. Умеет работать с интегрированной средой разработки программного обеспечения. ОПК-7.5. Умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач. ОПК-7.6. Владеет навыками разработки, документирования, тестирования и отладки программ. ОПК-7.7. Знает базовые структуры данных. ОПК-7.8. Знает основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы. ОПК-7.9. Знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения. ОПК-7.10. Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач. ОПК-7.11. Владеет навыками разработки алгоритмов решения типовых профессиональных задач. ОПК-7.12. Знает необходимые и достаточные условия оптимальности задачи математического программирования. ОПК-7.13. Умеет применять методы одномерной оптимизации при решении прикладных задач. ОПК-7.14. Умеет использовать методы многомерной безусловной оптимизации при решении профессиональных задач. ОПК-7.15. Знает методы условной оптимизации при решении прикладных задач. ОПК-7.16. Знает задачи вариационного исчисления, оптимального управления и линейного программирования.
	ОПК-8	Способен применять методы научных исследований при	ОПК-8.1. Знает строение мультипликативной группы колец вычетов. ОПК-8.2. Знает способы представления

		проведении разработок в области обеспечения безопасности компьютерных систем и сетей;	действительных чисел цепными дробями. ОПК-8.3. Знает основные свойства символов Лежандра и Якоби. ОПК-8.4. Знает критерии простоты и их использование для факторизации натуральных чисел. ОПК-8.5. Знает алгоритмы проверки чисел на простоту; построения больших простых чисел. ОПК-8.6. Умеет строить большие простые числа. ОПК-8.7. Умеет применять алгоритмы проверки чисел на простоту; построения больших простых чисел. ОПК-8.8. Умеет применять алгоритмы разложения чисел на множители. ОПК-8.9. Владеет навыками применения теории чисел в криптографии и других дисциплинах. ОПК-8.10. Умеет разрабатывать модели безопасности компьютерных систем с использованием необходимого математического аппарата и средств компьютерного моделирования. ОПК-8.11. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах. ОПК-8.12. Знает современные методы обработки информации и машинного обучения. ОПК-8.13. Умеет применять методы машинного обучения при проведении разработок в области обеспечения безопасности компьютерных систем. ОПК-8.14. Знает методологию экспериментальных исследований и испытаний. ОПК-8.15. Умеет применять методы экспериментального исследования при решении профессиональных задач.
	ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;	ОПК-9.1. Знает технические каналы утечки информации. ОПК-9.2. Знает возможности технических средств перехвата информации. ОПК-9.3. Умеет организовать защиту информации от утечки по техническим каналам на объектах информатизации. ОПК-9.4. Умеет пользоваться нормативными документами в области технической защиты информации. ОПК-9.5. Знает основные характеристики сигналов электросвязи, спектры и виды модуляции. ОПК-9.6. Знает принципы построения и функционирования систем и сетей передачи информации. способы передачи и распределения информации в телекоммуникационных системах и сетях. ОПК-9.7. Знает основные телекоммуникационные протоколы.

			ОПК-9.8. Умеет анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи. ОПК-9.9. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем. ОПК-9.10. Знает общие и специфические угрозы безопасности баз данных. ОПК-9.11. Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных. ОПК-9.12. Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных. ОПК-9.13. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации. ОПК-9.14. Знает основы физической защиты объектов информатизации. ОПК-9.15. Умеет анализировать и оценивать угрозы информационной безопасности объекта. ОПК-9.16. Владеет методами и средствами технической защиты информации. ОПК-9.17. Владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации.
	ОПК-10	Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ОПК-10.1. Знает основные задачи, решаемые криптографическими методами. ОПК-10.2. Знает математические модели шифров, подходы к оценке их стойкости. ОПК-10.3. Знает зарубежные и российские криптографические стандарты. ОПК-10.4. Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами. ОПК-10.5. Умеет применять математические методы при исследовании криптографических алгоритмов. ОПК-10.6. Владеет навыками использования типовых криптографических алгоритмов. ОПК-10.7. Знает типовые криптопротоколы, используемые в сетях связи. ОПК-10.8. Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем. ОПК-10.9. Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач. ОПК-10.10. Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств. ОПК-10.11. Владеет подходами к разработке и анализу безопасности криптографических протоколов. ОПК-10.12. Знает основные методы проверки

			чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах. ОПК-10.13. Знает базовые понятия теории эллиптических кривых. ОПК-10.14. Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях. ОПК-10.15. Умеет исследовать и решать сравнения в кольцах вычетов. ОПК-10.16. Умеет использовать достаточные условия простоты для построения больших простых чисел. ОПК-10.17. Умеет оценивать теоретическую сложность применяемых алгоритмов. ОПК-10.18. Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов. ОПК-10.19. Владеет методами построения быстрых вычислительных алгоритмов алгебры и теории чисел. ОПК-10.20. Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач. ОПК-10.21. Знает фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации. ОПК-10.22. Знает основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума. ОПК-10.23. Знает основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга). ОПК-10.24. Знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования. ОПК-10.25. Умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность). ОПК-10.26. Умеет решать типовые задачи кодирования и декодирования. ОПК-10.27. Владеет основами построения математических моделей текстовой информации и моделей систем передачи информации. ОПК-10.28. Владеет навыками применения математического аппарата для решения прикладных теоретико-информационных задач.
	ОПК-11	Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных	ОПК-11.1. Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем. ОПК-11.2. Знает основные виды политик управления доступом и информационными

		системах с учетом угроз безопасности информации и требований по защите информации;	потоками в компьютерных системах. ОПК-11.3. Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков. ОПК-11.4. Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем. ОПК-11.5. Умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками; ОПК-11.6. Знает средства и методы хранения и передачи аутентификационной информации. ОПК-11.7. Знает основные требования к подсистеме аудита и политике аудита. ОПК-11.8. Знает защитные механизмы и средства обеспечения безопасности операционных систем. ОПК-11.9. Умеет формулировать и настраивать политику безопасности основных операционных систем. ОПК-11.10. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.
	ОПК-12	Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;	ОПК-12.1. Знает принципы построения современных операционных систем и особенности их применения. ОПК-12.2. Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей. ОПК-12.3. Знает основные принципы конфигурирования и администрирования операционных систем. ОПК-12.4. Владеет навыками системного программирования. ОПК-12.5. Умеет осуществлять администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отечественного производства. ОПК-12.6. Знает методы восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. ОПК-12.7. Умеет восстанавливать работоспособность программ специального назначения при возникновении нештатных ситуаций.
	ОПК-13	Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их	ОПК-13.1. Умеет формулировать и настраивать политику безопасности основных операционных систем. ОПК-13.2. Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных

		безопасности;	семейств. ОПК-13.3. Знает общие принципы построения и использования современных языков программирования высокого уровня. ОПК-13.4. Знает язык программирования высокого уровня (объектно-ориентированное программирование). ОПК-13.5. Умеет работать с интегрированными средами разработки программного обеспечения. ОПК-13.6. Владеет навыками разработки, отладки, документирования и тестирования программ. ОПК-13.7. Владеет навыками использования инструментальных средств отладки и дизассемблирования программного кода. ОПК-13.8. Знает современные технологии программирования. ОПК-13.9. Знает показатели качества программного обеспечения. ОПК-13.10. Знает базовые структуры данных. ОПК-13.11. Знает основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности. ОПК-13.12. Умеет формализовать поставленную задачу. ОПК-13.13. Умеет разрабатывать эффективные алгоритмы и программы. ОПК-13.14. Умеет проводить оценку вычислительной сложности алгоритма. ОПК-13.15. Умеет планировать разработку сложного программного обеспечения. ОПК-13.16. Владеет методами оценки качества готового программного обеспечения. ОПК-13.17. Владеет навыками разработки алгоритмов для решения типовых профессиональных задач. ОПК-13.18. Умеет применять средства и методы анализа программного обеспечения для выявления закладок. ОПК-13.19. Умеет применять методы анализа проектных решений для обеспечения защищенности компьютерных систем. ОПК-13.20. Знает программные методы предотвращения несанкционированного доступа к данным. ОПК-13.21. Уметь применять современные средства обеспечения информационной безопасности программ и данных. ОПК-13.22. Знает основные программные методы защиты данных от несанкционированного доступа. ОПК-13.23. Умеет проводить анализ программных средств, применяемых для контроля и защиты информации. ОПК-13.24. Умеет проводить аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.
	ОПК-14	Способен проектировать базы данных,	ОПК-14.1. Знает характеристики и типы систем баз данных.

		администрировать системы управления базами данных в соответствии с требованиями по защите информации;	ОПК-14.2. Знает основные языки запросов. ОПК-14.3. Знает физическую организацию баз данных и принципы (основы) их защиты. ОПК-14.4. Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных. ОПК-14.5. Умеет настраивать и применять современные системы управления базами данных. ОПК-14.6. Владеет методикой и навыками составления запросов для поиска информации в базах данных. ОПК-14.7. Знает основные критерии защищенности баз данных и методы оценивания механизмов защиты. ОПК-14.8. Знает механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных. ОПК-14.9. Знает особенности применения криптографической защиты в СУБД. ОПК-14.10. Знает этапы проектирования системы защиты в СУБД. ОПК-14.11. Умеет пользоваться средствами защиты, предоставляемыми СУБД. ОПК-14.12. Умеет создавать дополнительные средства защиты баз данных. ОПК-14.13. Умеет проводить анализ и оценивание механизмов защиты баз данных. ОПК-14.14. Владеет методикой и навыками использования средств защиты, предоставляемых СУБД.
	ОПК-15	Способен администрировать компьютерные сети и контролировать корректность их функционирования;	ОПК-15.1. Знает архитектуру основных типов современных компьютерных систем. ОПК-15.2. Знает основы организации и построения компьютерных сетей. ОПК-15.3. Знает эталонную модель взаимодействия открытых систем. ОПК-15.4. Знает функции, принципы действия и алгоритмы работы сетевого оборудования. ОПК-15.5. Умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах. ОПК-15.6. Умеет осуществлять проектирование и оптимизацию функционирования компьютерных сетей. ОПК-15.7. Владеет навыками администрирования компьютерных сетей. ОПК-15.8. Владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением.
	ОПК-16	Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;	ОПК-16.1. Знает средства и методы хранения и передачи аутентификационной информации в компьютерных системах и сетях. ОПК-16.2. Знает механизмы реализации атак в сетях TCP/IP. ОПК-16.3. Знает основные протоколы идентификации и аутентификации абонентов сети. ОПК-16.4. Знает защитные механизмы и

			средства обеспечения сетевой безопасности. ОПК-16.5. Знает средства и методы предотвращения и обнаружения вторжений. ОПК-16.6. Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. ОПК-16.7. Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях. ОПК-16.8. Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. ОПК-16.9. Владеет навыками настройки межсетевых экранов. ОПК-16.10. Владеет методиками анализа сетевого трафика. ОПК-16.11. Знает основные виды деструктивных воздействий на программные продукты. ОПК-16.12. Умеет выявлять действие вредоносных программ, и определять характер их воздействия. ОПК-16.13. Знает современные методы анализа программных решений по обеспечению защищенности компьютерных систем. ОПК-16.14. Умеет производить оценку технического состояния аппаратных средств защиты информации. ОПК-16.15. Знает методологию применения технических средств диагностики состояния устройств защиты информации. ОПК-16.16. Умеет выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.
	ОПК-17	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	ОПК-17.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире. ОПК-17.2. Знает ключевые события истории России и мира, выдающихся деятелей России. ОПК-17.3. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий. ОПК-17.4. Умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России, опираясь на принципы историзма и научной объективности.
	ОПК-1.1	Способен проводить анализ защищенности и находить уязвимости компьютерной системы	ОПК-1.1.1. Знает принципы построения защищенных компьютерных систем и сетей. ОПК-1.1.2. Знает требования основных стандартов по оценке защищенности компьютерных систем и сетей. ОПК-1.1.3. Умеет определять уровень защищенности и доверия программно-

			аппаратных средств защиты информации. ОПК-1.1.4. Умеет классифицировать информационные системы по требованиям защиты информации. ОПК-1.1.5. Умеет определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе. ОПК-1.1.6. Умеет выполнять анализ компьютерной системы с целью определения уровня защищенности и доверия. ОПК-1.1.7. Умеет проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей.
	ОПК-1.2	Способен оценивать корректность программных реализаций алгоритмов защиты информации	ОПК-1.2.1. Знает основные средства и методы защиты программного обеспечения от анализа и нарушения целостности. ОПК-1.2.2. Знает теоретические основы устранения избыточности данных. ОПК-1.2.3. Знает основные алгоритмы кодирования данных и сжатия текстовой, графической, аудио- и видеоинформации. ОПК-1.2.4. Умеет проводить анализ программ и алгоритмов сжатия данных на предмет соответствия требованиям защиты информации. ОПК-1.2.5. Умеет применять средства и методы анализа программных реализаций для поиска уязвимостей. ОПК-1.2.6. Знает основные типы уязвимостей программного обеспечения.
	ОПК-1.3	Способен проводить тестирование и использовать средства верификации механизмов защиты информации	ОПК-1.3.1. Знает основные способы и средства верификации программ. ОПК-1.3.2. Знает основные способы тестирования средств защиты информации с использованием средств верификации программ. ОПК-1.3.3. Умеет применять основные методы верификации программ и алгоритмов на предмет соответствия требованиям защиты информации.

4.3. Профессиональные компетенции выпускников и индикаторы их достижения

В результате освоения программы у выпускника должны быть сформированы следующие **профессиональные компетенции**:

Таблица 4.3

Тип задач профессиональной деятельности	Код	Формулировка компетенции	Код и формулировка индикатора достижения компетенции
	ПК-1	Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения	ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования. ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств. ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в

			профессиональной деятельности.
	ПК-2	Способен проводить исследования на всех этапах жизненного цикла программных средств в профессиональной деятельности	ПК-2.1. Знает методы и средства планирования и организации исследований и разработок. ПК-2.2. Знает методы проведения экспериментов и наблюдений, обобщения и обработки информации, полученной в ходе исследований. ПК-2.3. Планирует стадии исследования или разработки в рамках поставленной задачи, выбирает или формирует программную среду для компьютерного моделирования и проведения экспериментов. ПК-2.4. Использует стандартное и оригинальное программное обеспечение, проводит компьютерный эксперимент, составляет его описание и формулирует выводы.
	ПК-3	Способен проводить анализ безопасности программных средств в компьютерных системах	ПК-3.1. Знает основные типы уязвимостей программного обеспечения и возможные пути их устранения. ПК-3.2. Знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования. ПК-3.3. Умеет анализировать программные средства на наличия уязвимостей. ПК-3.4. Умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента.

5. Структура и содержание ОПОП

5.1. Структура и объем ОПОП

ОПОП включает обязательную часть и часть, формируемую участниками образовательных отношений (вариативную).

Образовательная программа включает следующие блоки:

Таблица 5.1

Структура программы		Объем программы и ее блоков, в з.е.
Блок 1	Дисциплины (модули)	не менее 282 з.е.
Блок 2	Практика	не менее 27 з.е.
Блок 3	Государственная итоговая аттестация	не менее 6 з.е.
Объем программы		330 з.е.

Матрица соответствия компетенций, индикаторов их достижения и элементов ОПОП приведена в приложении 3.

В Блок 2 Практика включены следующие виды практик – *учебная и производственная*. В рамках ОПОП проводятся следующие практики: учебная практика исследовательская, производственная практика эксплуатационная, производственная практика преддипломная, производственная практика технологическая. Формы, способы и порядок проведения практик устанавливаются соответствующим Положением о порядке проведения практик.

В Блок 3 «Государственная итоговая аттестация» входит: подготовка к защите и защита выпускной квалификационной работы

Объем обязательной части, без учета объема государственной итоговой аттестации, составляет 75,8 % общего объема образовательной программы, что соответствует п. 2.10 ФГОС ВО.

5.2. Календарный учебный график

Календарный учебный график определяет периоды теоретического обучения, практик, НИР, экзаменационных сессий, государственной итоговой аттестации, каникул и их чередования в течение периода обучения, а также сводные данные по бюджету времени (в неделях).

Календарный учебный график по программе специалитета 10.05.01 Компьютерная безопасность (профиль «Анализ безопасности компьютерных систем») представлен в Приложении 4.

5.3. Учебный план

Документ, определяющий перечень дисциплин (модулей), практик, их объем (в зачетных единицах и академических часах), распределение по семестрам, по видам работ (лекции, практические, лабораторные, самостоятельная работа), наличие курсовых работ, проектов, форм промежуточной аттестации.

Учебный план по программе специалитета 10.05.01 Компьютерная безопасность (профиль «Анализ безопасности компьютерных систем») представлен в Приложении 5.

5.4. Рабочие программы дисциплин (модулей), практик

Аннотации рабочих программ дисциплин представлены в Приложении 6, аннотации рабочих программ практик представлены в Приложении 7. Рабочие программы размещены в ЭИОС ВГУ. Каждая рабочая программа содержит оценочные материалы для проведения текущей и промежуточной аттестации обучающихся по дисциплине (модулю), практике.

Рабочие программы размещены в ЭИОС ВГУ. Каждая рабочая программа содержит оценочные материалы для проведения текущей и промежуточной аттестации обучающихся по дисциплине (модулю), практике.

ФОС по образовательной программе, включающий комплекс заданий различного типа, используемых при проведении оценочных процедур по отдельным дисциплинам (модулям), практикам (текущего контроля / промежуточной аттестации / государственной итоговой (итоговой) аттестации), направленный на оценивание достижения обучающимися результатов освоения ОПОП (сформированности компетенций) представлен в Приложении 10.

5.5 Государственная итоговая аттестация

Государственная итоговая аттестация (ГИА) проводится после освоения обучающимся основной профессиональной образовательной программы в полном объеме.

Порядок проведения, формы, содержание, оценочные материалы, критерии оценки и методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы регламентируется Положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры Воронежского государственного университета, утвержденным Ученым советом ВГУ и программой государственной

итоговой аттестации по образовательной программе, утвержденной Ученым советом факультета компьютерных наук. Программа ГИА размещена в ЭИОС ВГУ.

При формировании программы ГИА совместно с работодателями, объединениями работодателей определяются наиболее значимые для профессиональной деятельности результаты обучения в качестве необходимых для присвоения установленной квалификации и проверяемые в ходе ГИА.

6. Условия осуществления образовательной деятельности

6.1. Общесистемные требования

Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам для проведения всех видов аудиторных занятий, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом.

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к ЭИОС из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

доступ к учебным планам, рабочим программам дисциплин (модулей), практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), практик;

формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы;

доступ к электронно-библиотечным системам (электронным библиотекам):

1. ЭБС «Университетская библиотека online» (Контракт №3010 06/28-24 от 28.12.2024 (с 28.12.2024 по 10.02.2026),
2. Информационно-телекоммуникационная система «Контекстум» (Национальный цифровой ресурс «РУКОНТ»). Договор ДС-208 от 01.02.2021 пролонгирован до 01.02.2027.
3. Электронная библиотека ВГУ, Договор №ДС-208 от 01.02.2021 с ООО «ЦКБ «БИБКОМ» и ООО «Агентство «Книга-Сервис» о создании Электронной библиотеки ВГУ, (с 01.02.2021 по 31.01.2027).

Для дисциплин, реализуемых с применением ЭО и ДОТ электронная информационно-образовательная среда Университета дополнительно обеспечивает: фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения программы;

проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети «Интернет» (в соответствии с разделом «Требования к условиям реализации программы» ФГОС ВО).

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий и квалификацией работников, ее использующих и поддерживающих. Функционирование электронной информационно-образовательной среды соответствует законодательству Российской Федерации.

6.2. Материально-техническое и учебно-методическое обеспечение программы

6.2.1. Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных данной программой, оснащены оборудованием, техническими средствами обучения, программными продуктами, состав которых

определяется в РПД, РПП. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

6.2.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определяется в рабочих программах дисциплин (модулей) и подлежит обновлению при необходимости).

6.2.3. Используемые в образовательном процессе печатные издания представлены в библиотечном фонде Университета из расчета не менее 0,25 экземпляра каждого из изданий, указанных в рабочих программах дисциплин (модулей), практик, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

6.2.4. Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в рабочих программах дисциплин (модулей) и подлежит обновлению (при необходимости).

Перечень материально-технического оборудования и программного обеспечения, представлен в Приложении 6.

6.3. Кадровые условия реализации программы

Реализация программы специалитета обеспечивается педагогическими работниками университета, а также лицами, привлекаемыми к реализации программы на иных условиях.

Квалификация педагогических работников Университета отвечает квалификационным требованиям, указанным в квалификационных справочниках, и (или) профессиональных стандартах (при наличии).

Не менее 98 процентов численности педагогических работников Университета, участвующих в реализации программы, и лиц, привлекаемых к реализации программы бакалавриата на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), ведут научную, учебно-методическую и (или) практическую работу, соответствующую профилю преподаваемой дисциплины (модуля), что соответствует п. 4.4.3 ФГОС ВО

Не менее 11 процентов численности педагогических работников Университета, участвующих в реализации программы бакалавриата, и лиц, привлекаемых к реализации программы бакалавриата на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), являются руководителями и (или) работниками иных организаций, осуществляющими трудовую деятельность в профессиональной сфере, соответствующей профессиональной деятельности, к которой готовятся выпускники (имеют стаж работы в данной профессиональной сфере не менее 3 лет), что соответствует п. 4.4.4 ФГОС

Не менее 78 процентов численности педагогических работников Университета и лиц, привлекаемых к образовательной деятельности Университета на иных условиях (исходя из количества замещаемых ставок, приведенного к целочисленным значениям), имеют ученую степень и (или) ученое звание, что соответствует п. 4.4.5

6.4 Финансовые условия реализации программы

Финансовое обеспечение реализации программы осуществляется в объеме не ниже значений базовых нормативов затрат на оказание государственных услуг по реализации образовательных программ высшего образования - программ *бакалавриата /специалитета/ магистратуры* и значений корректирующих коэффициентов к базовым нормативам затрат, определяемых Минобрнауки России.

6.5. Оценка качества образовательной деятельности и подготовки обучающихся

Качество образовательной деятельности и подготовки обучающихся по программе определяется в рамках системы внутренней оценки, а также внешней оценки качества образования.

В целях совершенствования программы при проведении регулярной внутренней оценки качества образовательной деятельности и подготовки обучающихся по программе привлекаются работодатели и (или) их объединения, иные юридические и (или) физические лица, включая педагогических работников Университета.

Внутренняя оценка качества образовательной деятельности проводится в рамках текущей, промежуточной и государственной (итоговой) аттестаций.

В рамках внутренней системы оценки качества образовательной деятельности по программе обучающимся предоставляется возможность оценивания условий, содержания, и качества образовательного процесса в целом и отдельных дисциплин (модулей) и практик.

Система внутренней оценки качества образования реализуется в соответствии с планом независимой оценки качества, утвержденным ученым советом факультета.

Внешняя оценка качества образовательной деятельности по программе проводится в рамках процедуры государственной аккредитации с целью подтверждения соответствия образовательной деятельности по программе требованиям ФГОС ВО с учетом соответствующей ПООП.

Нормативно-методические документы и материалы, регламентирующие и обеспечивающие качество подготовки обучающихся:

Положение о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета, утвержденное ученым советом ВГУ;

Положение о проведении промежуточной аттестации обучающихся по образовательным программам высшего образования, утвержденное решением Ученого совета ВГУ;

Положение о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры Воронежского государственного университета, утвержденное Ученым советом ВГУ;

Положение о независимой оценке качества образования в Воронежском государственном университете

Разработчики ОПОП:

Декан факультета_____А.А.Крыловецкий

Руководитель (куратор) программы_____ А.А.Сирота

Программа рекомендована Ученым советом факультета компьютерных наук от 21.05.2025 г., протокол № 5

Приложение 1

Перечень профессиональных стандартов, соотнесенных с федеральным государственным образовательным стандартом специальности 10.05.01 Компьютерная безопасность,
используемых при разработке образовательной программы
Анализ безопасности компьютерных систем

№ п/п	Код профессионального стандарта	Наименование профессионального стандарта
06 Связь, информационные и коммуникационные технологии		
1.	*06.001*	*Профессиональный стандарт «Программист», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2013 г. № 679н (зарегистрирован Министерством юстиции Российской Федерации 18 декабря 2013 г., регистрационный №30635), с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный № 45230)*
8.	*06.032*	*Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. №598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464)*

Приложение 2

Перечень обобщённых трудовых функций и трудовых функций, имеющих отношение к профессиональной деятельности выпускника
Образовательная программа 10.05.01 Компьютерная безопасность
Уровень образования специалитет
Направление подготовки Анализ безопасности компьютерных систем

Код и наименование профессионального стандарта	**Обобщенные трудовые функции**			**Трудовые функции**	
	код	наименование	уровень квалификации	Наименование	код
06.032 «Специалист по безопасности компьютерных систем и сетей»	C	Оценивание уровня безопасности компьютерных систем и сетей	*7*	Проведение анализа безопасности компьютерных систем	C/03.7
				Проведение сертификации программно-аппаратных средств защиты информации и анализ результатов	C/04.7
				Проведение инструментального мониторинга защищенности компьютерных систем и сетей	C/05.7
06.001 «Программист»	C	Интеграция программных модулей и компонент и верификация выпусков программного продукта	*5*	Разработка процедур интеграции программных модулей	C/01.5
				Осуществление интеграции программных модулей и компонент и верификации выпусков программного продукта	C/02.5
	D	*Разработка требований и проектирование программного обеспечения*			

Приложение 3

Матрица соответствия компетенций, индикаторов их достижения и элементов ОПОП

	Наименование	Формируемые индикаторы достижения компетенций
Б1	**Наименование дисциплины (модуля), практики**	УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5; УК-3.1; УК-3.2; УК-3.3; УК-4.1; УК-4.2; УК-4.3; УК-4.4; УК-4.5; УК-4.6; УК-5.1; УК-5.2; УК-5.3; УК-5.4.1; УК-6.1; УК-6.2; УК-7.1; УК-7.2; УК-7.3; УК-7.4; УК-7.5; УК-7.6; УК-8.1; УК-8.2; УК-8.3; УК-8.4; УК-9.1; УК-9.2; УК-9.3; УК-9.4; УК-9.5; УК-10.1; УК-10.2; УК-10.3; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-3.4; ОПК-3.5; ОПК-3.6; ОПК-3.7; ОПК-3.8; ОПК-3.9; ОПК-3.10; ОПК-3.11; ОПК-3.12; ОПК-3.13; ОПК-3.14; ОПК-3.15; ОПК-3.16; ОПК-3.17; ОПК-3.18; ОПК-3.19; ОПК-3.20; ОПК-3.21; ОПК-3.22; ОПК-3.23; ОПК-3.24; ОПК-3.25; ОПК-3.26; ОПК-3.27; ОПК-3.28; ОПК-3.29; ОПК-3.30; ОПК-3.31; ОПК-3.32; ОПК-3.33; ОПК-3.34; ОПК-3.35; ОПК-3.36; ОПК-3.37; ОПК-3.38; ОПК-3.39; ОПК-3.40; ОПК-3.41; ОПК-3.42; ОПК-3.43; ОПК-3.44; ОПК-3.45; ОПК-3.46; ОПК-3.47; ОПК-3.48; ОПК-3.49; ОПК-3.50; ОПК-3.51; ОПК-3.52; ОПК-3.53; ОПК-3.54; ОПК-3.55; ОПК-3.56; ОПК-3.57; ОПК-3.58; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-4.4; ОПК-4.5; ОПК-4.6; ОПК-4.7; ОПК-4.8; ОПК-4.9; ОПК-4.10; ОПК-4.11; ОПК-4.12; ОПК-4.13; ОПК-4.14; ОПК-4.15; ОПК-4.16; ОПК-4.17; ОПК-4.18; ОПК-4.19; ОПК-4.20; ОПК-4.21; ОПК-4.22; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-5.6; ОПК-5.7; ОПК-5.8; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-5.14; ОПК-5.15; ОПК-5.16; ОПК-5.17; ОПК-5.18; ОПК-5.19; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6.8; ОПК-6.9; ОПК-6.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16; ОПК-8.1; ОПК-8.2; ОПК-8.3; ОПК-8.4; ОПК-8.5; ОПК-8.6; ОПК-8.7; ОПК-8.8; ОПК-8.9; ОПК-8.10; ОПК-8.11; ОПК-8.12; ОПК-8.13; ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-9.4; ОПК-9.5; ОПК-9.6; ОПК-9.7; ОПК-9.8; ОПК-9.9; ОПК-9.10; ОПК-9.11; ОПК-9.12; ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-10.4; ОПК-10.5; ОПК-10.6; ОПК-10.7; ОПК-10.8; ОПК-10.9; ОПК-10.10; ОПК-10.11; ОПК-10.12; ОПК-10.13; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19; ОПК-10.20; ОПК-10.21; ОПК-10.22; ОПК-10.23; ОПК-10.24; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28; ОПК-11.1; ОПК-1.1.1; ОПК-11.2; ОПК-1.1.2; ОПК-11.3; ОПК-1.1.3; ОПК-1.1.4; ОПК-11.4; ОПК-1.1.5; ОПК-11.5; ОПК-1.1.6; ОПК-11.6; ОПК-1.1.7; ОПК-11.7; ОПК-11.8; ОПК-11.9; ОПК-11.10; ОПК-12.1; ОПК-1.2.1; ОПК-12.2; ОПК-1.2.2; ОПК-12.3; ОПК-1.2.3; ОПК-1.2.4; ОПК-12.4; ОПК-1.2.5; ОПК-12.5; ОПК-12.6; ОПК-1.2.6; ОПК-12.7; ОПК-1.3.1; ОПК-13.1; ОПК-13.2; ОПК-1.3.2; ОПК-1.3.3; ОПК-13.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-14.1; ОПК-14.2; ОПК-14.3; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.7; ОПК-14.8; ОПК-14.9; ОПК-14.10; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14; ОПК-15.1; ОПК-15.2; ОПК-15.3; ОПК-15.4; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8; ОПК-16.1; ОПК-16.2; ОПК-16.3; ОПК-16.4; ОПК-16.5; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10; ОПК-16.11; ОПК-16.12; ОПК-16.13; ОПК-16.14; ОПК-16.15; ОПК-16.16; ОПК-17.1; ОПК-17.2; ОПК-17.3; ОПК-17.4; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4
Б1.О	**Обязательная часть**	УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5; УК-3.1; УК-3.2; УК-3.3; УК-4.1; УК-4.2; УК-4.3; УК-4.4; УК-4.5; УК-4.6; УК-5.1; УК-5.2; УК-5.3; УК-6.1; УК-6.2; УК-7.1; УК-7.2; УК-7.3; УК-8.1; УК-8.2; УК-8.3; УК-8.4; УК-9.1; УК-9.2; УК-9.3; УК-9.4; УК-9.5; УК-10.1; УК-10.2; УК-10.3; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-3.4; ОПК-3.5; ОПК-3.6; ОПК-3.7; ОПК-3.8; ОПК-3.9; ОПК-3.10; ОПК-3.11; ОПК-3.12; ОПК-3.13; ОПК-3.14; ОПК-3.15; ОПК-3.16; ОПК-3.17; ОПК-3.18; ОПК-3.19; ОПК-3.20; ОПК-3.21; ОПК-3.22; ОПК-3.23; ОПК-3.24;

		ОПК-3.25; ОПК-3.26; ОПК-3.27; ОПК-3.28; ОПК-3.29; ОПК-3.30; ОПК-3.31; ОПК-3.32; ОПК-3.33; ОПК-3.34; ОПК-3.35; ОПК-3.36; ОПК-3.37; ОПК-3.38; ОПК-3.39; ОПК-3.40; ОПК-3.41; ОПК-3.42; ОПК-3.43; ОПК-3.44; ОПК-3.45; ОПК-3.46; ОПК-3.47; ОПК-3.48; ОПК-3.49; ОПК-3.50; ОПК-3.51; ОПК-3.52; ОПК-3.53; ОПК-3.54; ОПК-3.55; ОПК-3.56; ОПК-3.57; ОПК-3.58; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-4.4; ОПК-4.5; ОПК-4.6; ОПК-4.7; ОПК-4.8; ОПК-4.9; ОПК-4.10; ОПК-4.11; ОПК-4.12; ОПК-4.13; ОПК-4.14; ОПК-4.15; ОПК-4.16; ОПК-4.17; ОПК-4.18; ОПК-4.19; ОПК-4.20; ОПК-4.21; ОПК-4.22; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-5.6; ОПК-5.7; ОПК-5.8; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-5.14; ОПК-5.15; ОПК-5.16; ОПК-5.17; ОПК-5.18; ОПК-5.19; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6.8; ОПК-6.9; ОПК-6.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16; ОПК-8.1; ОПК-8.2; ОПК-8.3; ОПК-8.4; ОПК-8.5; ОПК-8.6; ОПК-8.7; ОПК-8.8; ОПК-8.9; ОПК-8.10; ОПК-8.11; ОПК-8.12; ОПК-8.13; ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-9.4; ОПК-9.5; ОПК-9.6; ОПК-9.7; ОПК-9.8; ОПК-9.9; ОПК-9.10; ОПК-9.11; ОПК-9.12; ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-10.4; ОПК-10.5; ОПК-10.6; ОПК-10.7; ОПК-10.8; ОПК-10.9; ОПК-10.10; ОПК-10.11; ОПК-10.12; ОПК-10.13; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19; ОПК-10.20; ОПК-10.21; ОПК-10.22; ОПК-10.23; ОПК-10.24; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28; ОПК-1.1.1; ОПК-11.1; ОПК-1.1.2; ОПК-11.2; ОПК-1.1.3; ОПК-11.3; ОПК-1.1.4; ОПК-11.4; ОПК-11.5; ОПК-1.1.5; ОПК-1.1.6; ОПК-11.6; ОПК-11.7; ОПК-1.1.7; ОПК-11.8; ОПК-11.9; ОПК-11.10; ОПК-1.2.1; ОПК-12.1; ОПК-12.2; ОПК-1.2.2; ОПК-1.2.3; ОПК-12.3; ОПК-1.2.4; ОПК-12.4; ОПК-1.2.5; ОПК-12.5; ОПК-1.2.6; ОПК-12.6; ОПК-12.7; ОПК-13.1; ОПК-1.3.1; ОПК-13.2; ОПК-1.3.2; ОПК-13.3; ОПК-1.3.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-14.1; ОПК-14.2; ОПК-14.3; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.7; ОПК-14.8; ОПК-14.9; ОПК-14.10; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14; ОПК-15.1; ОПК-15.2; ОПК-15.3; ОПК-15.4; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8; ОПК-16.1; ОПК-16.2; ОПК-16.3; ОПК-16.4; ОПК-16.5; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10; ОПК-16.11; ОПК-16.12; ОПК-16.13; ОПК-16.14; ОПК-16.15; ОПК-16.16; ОПК-17.1; ОПК-17.2; ОПК-17.3; ОПК-17.4
Б1.О.01	Философия	УК-1.1; УК-1.2; УК-1.3
Б1.О.02	История России	УК-5.1; УК-5.2; ОПК-17.1; ОПК-17.2; ОПК-17.3; ОПК-17.4
Б1.О.03	Иностранный язык	УК-4.1; УК-4.5
Б1.О.04	Безопасность жизнедеятельности	УК-8.1; УК-8.2; УК-8.3; УК-8.4
Б1.О.05	Физическая культура и спорт	УК-7.1; УК-7.2; УК-7.3
Б1.О.06	Коммуникативные технологии профессионального общения	УК-4.2; УК-4.3; УК-4.4; УК-4.6
Б1.О.07	Современные теории и технологии развития личности	УК-3.1; УК-3.2; УК-3.3; УК-6.1; УК-6.2
Б1.О.08	Правовые и организационные основы	УК-10.1; УК-10.2; УК-10.3

	противодействия противоправному поведению	
Б1.О.09	Проектный менеджмент	УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5
Б1.О.10	Экономика и финансовая грамотность	УК-9.1; УК-9.2; УК-9.3; УК-9.4; УК-9.5
Б1.О.11	Введение в специальность	ОПК-1.1; ОПК-5.2
Б1.О.12	Основы российской государственности	УК-5.3
Б1.О.13	Механика и оптика	ОПК-4.1; ОПК-4.4; ОПК-4.6; ОПК-4.7; ОПК-4.8
Б1.О.14	Электричество и магнетизм	ОПК-4.3; ОПК-4.4; ОПК-4.6; ОПК-4.7; ОПК-4.8
Б1.О.15	Термодинамика	ОПК-4.2; ОПК-4.6; ОПК-4.7; ОПК-4.8
Б1.О.16	Квантовая теория	ОПК-4.5; ОПК-4.6; ОПК-4.7; ОПК-4.8
Б1.О.17	Электроника и схемотехника	ОПК-4.9; ОПК-4.10; ОПК-4.11; ОПК-4.12; ОПК-4.13; ОПК-4.14; ОПК-4.15; ОПК-4.17
Б1.О.18	Математический анализ	ОПК-3.38; ОПК-3.39; ОПК-3.40; ОПК-3.41; ОПК-3.42; ОПК-3.44; ОПК-3.45; ОПК-3.46; ОПК-3.47; ОПК-3.48
Б1.О.19	Геометрия	ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-3.5; ОПК-3.6
Б1.О.20	Теория вероятностей и математическая статистика	ОПК-3.49; ОПК-3.50; ОПК-3.51; ОПК-3.52; ОПК-3.53; ОПК-3.54; ОПК-3.55; ОПК-3.56; ОПК-3.57
Б1.О.21	Алгебра	ОПК-3.7; ОПК-3.8; ОПК-3.9; ОПК-3.10; ОПК-3.11; ОПК-3.12; ОПК-3.13; ОПК-3.14; ОПК-3.15; ОПК-3.16
Б1.О.22	Аппаратные средства вычислительной техники	ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-4.16; ОПК-4.17; ОПК-4.18; ОПК-4.19; ОПК-15.1
Б1.О.23	Линейная алгебра	ОПК-3.4; ОПК-3.7; ОПК-3.8; ОПК-3.9; ОПК-3.10; ОПК-3.11; ОПК-3.12; ОПК-3.13; ОПК-3.14; ОПК-3.15; ОПК-3.16
Б1.О.24	Математическая логика и теория алгоритмов	ОПК-3.17; ОПК-3.18; ОПК-3.19; ОПК-3.20; ОПК-3.21; ОПК-3.22; ОПК-3.23; ОПК-3.24; ОПК-3.25; ОПК-3.26; ОПК-3.27
Б1.О.25	Дискретная математика	ОПК-3.28; ОПК-3.29; ОПК-3.30; ОПК-3.31; ОПК-3.32; ОПК-3.33; ОПК-3.34; ОПК-3.35; ОПК-3.36; ОПК-3.37
Б1.О.26	Дифференциальные уравнения	ОПК-3.43; ОПК-3.58
Б1.О.27	Методы вычислений	ОПК-3.11; ОПК-3.13; ОПК-3.20
Б1.О.28	Методы оптимизации	ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16

Б1.О.29	Теория информации	ОПК-10.21; ОПК-10.22; ОПК-10.23; ОПК-10.24; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28
Б1.О.30	Технологии обработки информации	ОПК-8.12; ОПК-8.13
Б1.О.31	Информатика	ОПК-2.1; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-3.20; ОПК-10.21; ОПК-10.22; ОПК-10.23
Б1.О.32	Операционные системы	ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-12.1; ОПК-12.2; ОПК-12.3; ОПК-12.4; ОПК-12.5; ОПК-12.6
Б1.О.33	Сети и системы передачи информации	ОПК-9.5; ОПК-9.6; ОПК-9.7; ОПК-9.8
Б1.О.34	Компьютерные сети	ОПК-15.1; ОПК-15.2; ОПК-15.3; ОПК-15.4; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8
Б1.О.35	Объектно-ориентированное программирование	ОПК-2.9; ОПК-2.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-13.4; ОПК-13.7
Б1.О.36	Введение в программирование	ОПК-2.9; ОПК-2.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-13.3; ОПК-13.5; ОПК-13.7; ОПК-13.8
Б1.О.37	Методы программирования	ОПК-2.9; ОПК-2.10; ОПК-7.1; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-13.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17
Б1.О.38	Системы управления базами данных	ОПК-14.1; ОПК-14.2; ОПК-14.3; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.9; ОПК-14.10; ОПК-14.11; ОПК-14.14
Б1.О.39	Основы информационной безопасности	ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-5.4
Б1.О.40	Модели безопасности компьютерных систем	ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.8; ОПК-6.10; ОПК-8.10; ОПК-8.11; ОПК-11.1; ОПК-11.2; ОПК-11.3; ОПК-11.4; ОПК-11.5
Б1.О.41	Защита в операционных системах	ОПК-9.11; ОПК-9.12; ОПК-11.6; ОПК-11.7; ОПК-11.8; ОПК-11.9; ОПК-11.10; ОПК-12.2; ОПК-12.4; ОПК-13.1; ОПК-13.2
Б1.О.42	Основы построения защищенных компьютерных сетей	ОПК-8.11; ОПК-9.9; ОПК-9.11; ОПК-9.12; ОПК-11.10; ОПК-15.7; ОПК-15.8; ОПК-16.1; ОПК-16.2; ОПК-16.3; ОПК-16.4; ОПК-16.5; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10
Б1.О.43	Основы построения защищенных баз данных	ОПК-8.11; ОПК-9.10; ОПК-9.11; ОПК-9.12; ОПК-14.7; ОПК-14.8; ОПК-14.9; ОПК-14.10; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14
Б1.О.44	Защита программ и данных	ОПК-5.14; ОПК-5.15; ОПК-5.16; ОПК-7.5; ОПК-7.6; ОПК-7.9; ОПК-7.10; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-16.11; ОПК-16.12; ОПК-16.13
Б1.О.45	Методы и средства криптографической защиты информации	ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-10.4; ОПК-10.5; ОПК-10.6
Б1.О.46	Криптографические протоколы	ОПК-10.7; ОПК-10.8; ОПК-10.9; ОПК-10.10; ОПК-10.11; ОПК-10.20

Б1.О.47	Теоретико-числовые методы в криптографии	ОПК-8.1; ОПК-8.2; ОПК-8.3; ОПК-8.4; ОПК-8.5; ОПК-8.6; ОПК-8.7; ОПК-8.8; ОПК-8.9; ОПК-10.12; ОПК-10.13; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19
Б1.О.48	Управление ресурсами в системах информационной безопасности	ОПК-5.4; ОПК-6.3
Б1.О.49	Организационное и правовое обеспечение информационной безопасности	ОПК-5.3; ОПК-5.5; ОПК-5.6; ОПК-5.7; ОПК-5.8; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6.8; ОПК-6.9; ОПК-6.10
Б1.О.50	Инсталляция и настройка программного обеспечения	ОПК-2.3; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14; ОПК-4.19; ОПК-12.1; ОПК-12.5; ОПК-12.6; ОПК-12.7; ОПК-15.8; ОПК-16.8; ОПК-16.9; ОПК-16.10
Б1.О.51	Защита информации от утечки по техническим каналам	ОПК-5.14; ОПК-5.15; ОПК-5.16; ОПК-5.17; ОПК-5.18; ОПК-5.19; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6.8; ОПК-6.9; ОПК-6.10; ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-9.4; ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17
Б1.О.52	Теория радиотехнических систем	ОПК-4.4; ОПК-4.6; ОПК-4.7; ОПК-4.8; ОПК-4.9; ОПК-4.10; ОПК-4.11; ОПК-4.12; ОПК-4.13; ОПК-4.14; ОПК-4.15; ОПК-4.17; ОПК-4.20; ОПК-4.21; ОПК-4.22; ОПК-9.5; ОПК-9.8; ОПК-10.22; ОПК-10.23; ОПК-10.24; ОПК-16.14; ОПК-16.15; ОПК-16.16
Б1.О.53	Уравнения математической физики	ОПК-3.43; ОПК-3.58; ОПК-4.6
Б1.О.54	Комплексный анализ	ОПК-3.42
Б1.О.55	Дисциплины специализации	ОПК-2.5; ОПК-7.2; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-1.1.1; ОПК-1.1.2; ОПК-1.1.3; ОПК-1.1.4; ОПК-1.1.5; ОПК-1.1.6; ОПК-1.1.7; ОПК-1.2.1; ОПК-1.2.2; ОПК-1.2.3; ОПК-1.2.4; ОПК-1.2.5; ОПК-1.2.6; ОПК-1.3.1; ОПК-1.3.2; ОПК-1.3.3; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17
Б1.О.55.01	Методы верификации	ОПК-1.3.1; ОПК-1.3.2; ОПК-1.3.3
Б1.О.55.02	Алгоритмы кодирования и сжатия информации	ОПК-1.2.2; ОПК-1.2.3; ОПК-1.2.4
Б1.О.55.03	Методы и стандарты оценки защищенности компьютерных систем	ОПК-1.1.1; ОПК-1.1.2; ОПК-1.1.3; ОПК-1.1.4; ОПК-1.1.5; ОПК-1.1.6; ОПК-1.1.7
Б1.О.55.04	Интеллектуальные системы обработки информации	ОПК-7.4; ОПК-7.6; ОПК-7.10; ОПК-7.11
Б1.О.55.05	Алгоритмы и структуры данных	ОПК-7.7; ОПК-7.8; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17

Б1.В	Часть, формируемая участниками образовательных отношений	УК-3.2; УК-3.3; УК-5.4.1; УК-7.4; УК-7.5; УК-7.6; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4
Б1.В.01	Стеганография и цифровые водяные знаки	ПК-1.2; ПК-1.3; ПК-3.2; ПК-3.4
Б1.В.02	Моделирование систем	ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4
Б1.В.03	Технологии защищенного документооборота и блокчейн	ПК-1.2; ПК-1.3; ПК-3.2; ПК-3.4
Б1.В.04	Методология экспериментальных исследований и испытаний	ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4
Б1.В.05	Анализ уязвимостей программного обеспечения	ПК-3.1; ПК-3.3
Б1.В.06	Дисциплины военного модуля	
Б1.В.07	Элективные дисциплины по физической культуре и спорту (модуль)	УК-7.4; УК-7.5; УК-7.6
Б1.В.07.ДВ.01	Дисциплины модуля	УК-7.4; УК-7.5; УК-7.6
Б1.В.07.ДВ.01.01	Легкая атлетика	УК-7.4; УК-7.5; УК-7.6
Б1.В.07.ДВ.01.02	Волейбол	
Б1.В.07.ДВ.01.03	Бадминтон	
Б1.В.07.ДВ.01.04	Баскетбол	
Б1.В.07.ДВ.01.05	Гандбол	
Б1.В.07.ДВ.01.06	Мини-футбол	
Б1.В.07.ДВ.01.07	Настольный теннис	

Б1.В.07.ДВ.01.08	Лыжные гонки	
Б1.В.07.ДВ.01.09	Плавание	
Б1.В.07.ДВ.01.10	Спортивная борьба	
Б1.В.07.ДВ.01.11	Спортивная аэробика	
Б1.В.ДВ.01	Дисциплины (модули) по выбору 1 (ДВ.1)	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.01.01	Язык программирования Java	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.01.02	Язык программирования C#	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.01.03	Правовые и организационные основы добровольческой (волонтерской) деятельности	УК-3.2
Б1.В.ДВ.01.04	Основы конструктивного взаимодействия лиц с ограниченными возможностями здоровья в образовательном процессе	УК-3.3
Б1.В.ДВ.01.05	Общественный проект "Обучение служением"	УК-5.4.1
Б1.В.ДВ.02	Дисциплины (модули) по выбору 2 (ДВ.2)	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.02.01	Языки программирования	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.02.02	Алгоритмы машинной графики	ПК-1.2; ПК-1.3
Б1.В.ДВ.02.03	Психолого-педагогическое сопровождение лиц с ограниченными возможностями	УК-3.3

	здоровья	
Б1.В.ДВ.03	Дисциплины (модули) по выбору 3 (ДВ.3)	ПК-1.2; ПК-1.3
Б1.В.ДВ.03.01	Биометрические методы идентификации личности	ПК-1.2; ПК-1.3
Б1.В.ДВ.03.02	Язык HTML	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.04	Дисциплины (модули) по выбору 4 (ДВ.4)	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.04.01	Параллельные алгоритмы обработки данных	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.04.02	Технологии интернет вещей	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.05	Дисциплины (модули) по выбору 5 (ДВ.5)	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.05.01	Разработка приложений на C++	ПК-1.1; ПК-1.2; ПК-1.3
Б1.В.ДВ.05.02	Обработка изображений	ПК-1.1; ПК-1.2; ПК-1.3
Б2	Практика	УК-1.1; УК-1.2; УК-1.3; УК-3.1; УК-3.2; УК-3.3; УК-6.1; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14; ОПК-4.18; ОПК-4.19; ОПК-5.3; ОПК-5.4; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-5.17; ОПК-5.19; ОПК-6.6; ОПК-6.7; ОПК-6.9; ОПК-6.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16; ОПК-8.10; ОПК-8.11; ОПК-8.13; ОПК-8.15; ОПК-9.3; ОПК-9.4; ОПК-9.9; ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-10.4; ОПК-10.5; ОПК-10.6; ОПК-10.9; ОПК-10.10; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19; ОПК-10.20; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28; ОПК-1.1.1; ОПК-1.1.2; ОПК-1.1.3; ОПК-1.1.4; ОПК-11.4; ОПК-11.5; ОПК-1.1.5; ОПК-1.1.6; ОПК-1.1.7; ОПК-11.9; ОПК-11.10; ОПК-1.2.1; ОПК-1.2.2; ОПК-1.2.3; ОПК-1.2.4; ОПК-12.4; ОПК-1.2.5; ОПК-12.5; ОПК-1.2.6; ОПК-12.7; ОПК-13.1; ОПК-1.3.1; ОПК-13.2; ОПК-1.3.2; ОПК-13.3; ОПК-1.3.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10; ОПК-16.12; ОПК-16.14; ОПК-16.16; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4
Б2.О	Обязательная часть	УК-1.1; УК-1.2; УК-1.3; УК-3.1; УК-3.2; УК-3.3; УК-6.1; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14; ОПК-4.18; ОПК-4.19; ОПК-5.3; ОПК-5.4; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-5.17; ОПК-5.19; ОПК-6.6; ОПК-6.7; ОПК-6.9; ОПК-6.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16; ОПК-8.10; ОПК-8.11; ОПК-8.13; ОПК-8.15; ОПК-9.3; ОПК-9.4; ОПК-9.9;

		ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-10.4; ОПК-10.5; ОПК-10.6; ОПК-10.9; ОПК-10.10; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19; ОПК-10.20; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28; ОПК-1.1.1; ОПК-1.1.2; ОПК-1.1.3; ОПК-1.1.4; ОПК-11.4; ОПК-1.1.5; ОПК-11.5; ОПК-1.1.6; ОПК-1.1.7; ОПК-11.9; ОПК-11.10; ОПК-1.2.1; ОПК-1.2.2; ОПК-1.2.3; ОПК-1.2.4; ОПК-12.4; ОПК-12.5; ОПК-1.2.5; ОПК-1.2.6; ОПК-12.7; ОПК-13.1; ОПК-1.3.1; ОПК-13.2; ОПК-1.3.2; ОПК-13.3; ОПК-1.3.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10; ОПК-16.12; ОПК-16.14; ОПК-16.16
Б2.О.01(У)	Учебная практика (экспериментально-исследовательская)	УК-1.1; УК-3.1; УК-3.2; УК-3.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14; ОПК-4.18; ОПК-4.19
Б2.О.02(У)	Учебный сбор	
Б2.О.03(Н)	Производственная практика (научно-исследовательская работа)	УК-1.1; УК-1.2; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16; ОПК-8.10; ОПК-8.11; ОПК-8.13; ОПК-8.15; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-13.1; ОПК-13.2; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.21; ОПК-13.23; ОПК-13.24
Б2.О.04(Пд)	Производственная практика (преддипломная)	УК-1.1; УК-1.2; УК-1.3; УК-6.1; ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-13.1; ОПК-13.2; ОПК-13.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24
Б2.О.05(П)	Войсковая стажировка	
Б2.О.06(П)	Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	ОПК-5.3; ОПК-5.4; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-5.17; ОПК-5.19; ОПК-6.6; ОПК-6.7; ОПК-6.9; ОПК-6.10; ОПК-9.3; ОПК-9.4; ОПК-9.9; ОПК-9.16; ОПК-9.17; ОПК-10.4; ОПК-10.5; ОПК-10.6; ОПК-10.9; ОПК-10.10; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19; ОПК-10.20; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28; ОПК-1.1.1; ОПК-1.1.2; ОПК-1.1.3; ОПК-11.4; ОПК-1.1.4; ОПК-11.5; ОПК-1.1.5; ОПК-1.1.6; ОПК-1.1.7; ОПК-11.9; ОПК-11.10; ОПК-1.2.1; ОПК-1.2.2; ОПК-1.2.3; ОПК-12.4; ОПК-1.2.4; ОПК-12.5; ОПК-1.2.5; ОПК-1.2.6; ОПК-12.7; ОПК-1.3.1; ОПК-13.1; ОПК-1.3.2; ОПК-13.2; ОПК-1.3.3; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.21; ОПК-13.23; ОПК-13.24; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10; ОПК-16.12; ОПК-16.14; ОПК-16.16
Б2.В	Часть, формируемая участниками образовательных отношений	ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4
Б2.В.01(П)	Производственная практика (технологическая)	ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4
Б3	Государственная итоговая аттестация	УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5; УК-3.1; УК-3.2; УК-3.3; УК-4.1; УК-4.2; УК-4.3; УК-4.4; УК-4.5; УК-4.6; УК-5.1; УК-5.2; УК-6.1; УК-6.2; УК-7.1; УК-7.2; УК-7.3; УК-7.4; УК-7.5; УК-7.6; УК-8.1; УК-8.2; УК-8.3; УК-8.4; УК-9.1; УК-9.2; УК-9.3; УК-9.4; УК-9.5; УК-10.1; УК-10.2; УК-10.3; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14;

		ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-3.4; ОПК-3.5; ОПК-3.6; ОПК-3.7; ОПК-3.8; ОПК-3.9; ОПК-3.10; ОПК-3.11; ОПК-3.12; ОПК-3.13; ОПК-3.14; ОПК-3.15; ОПК-3.16; ОПК-3.17; ОПК-3.18; ОПК-3.19; ОПК-3.20; ОПК-3.21; ОПК-3.22; ОПК-3.23; ОПК-3.24; ОПК-3.25; ОПК-3.26; ОПК-3.27; ОПК-3.28; ОПК-3.29; ОПК-3.30; ОПК-3.31; ОПК-3.32; ОПК-3.33; ОПК-3.34; ОПК-3.35; ОПК-3.36; ОПК-3.37; ОПК-3.38; ОПК-3.39; ОПК-3.40; ОПК-3.41; ОПК-3.42; ОПК-3.43; ОПК-3.44; ОПК-3.45; ОПК-3.46; ОПК-3.47; ОПК-3.48; ОПК-3.49; ОПК-3.50; ОПК-3.51; ОПК-3.52; ОПК-3.53; ОПК-3.54; ОПК-3.55; ОПК-3.56; ОПК-3.57; ОПК-3.58; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-4.4; ОПК-4.5; ОПК-4.6; ОПК-4.7; ОПК-4.8; ОПК-4.9; ОПК-4.10; ОПК-4.11; ОПК-4.12; ОПК-4.13; ОПК-4.14; ОПК-4.15; ОПК-4.16; ОПК-4.17; ОПК-4.18; ОПК-4.19; ОПК-4.20; ОПК-4.21; ОПК-4.22; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-5.6; ОПК-5.7; ОПК-5.8; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-5.14; ОПК-5.15; ОПК-5.16; ОПК-5.17; ОПК-5.18; ОПК-5.19; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6.8; ОПК-6.9; ОПК-6.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16; ОПК-8.1; ОПК-8.2; ОПК-8.3; ОПК-8.4; ОПК-8.5; ОПК-8.6; ОПК-8.7; ОПК-8.8; ОПК-8.9; ОПК-8.10; ОПК-8.11; ОПК-8.12; ОПК-8.13; ОПК-8.14; ОПК-8.15; ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-9.4; ОПК-9.5; ОПК-9.6; ОПК-9.7; ОПК-9.8; ОПК-9.9; ОПК-9.10; ОПК-9.11; ОПК-9.12; ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-10.4; ОПК-10.5; ОПК-10.6; ОПК-10.7; ОПК-10.8; ОПК-10.9; ОПК-10.10; ОПК-10.11; ОПК-10.12; ОПК-10.13; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19; ОПК-10.20; ОПК-10.21; ОПК-10.22; ОПК-10.23; ОПК-10.24; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28; ОПК-11.1; ОПК-1.1.1; ОПК-1.1.2; ОПК-11.2; ОПК-1.1.3; ОПК-11.3; ОПК-11.4; ОПК-1.1.4; ОПК-11.5; ОПК-1.1.5; ОПК-1.1.6; ОПК-11.6; ОПК-1.1.7; ОПК-11.7; ОПК-11.8; ОПК-11.9; ОПК-11.10; ОПК-12.1; ОПК-1.2.1; ОПК-12.2; ОПК-1.2.2; ОПК-1.2.3; ОПК-12.3; ОПК-12.4; ОПК-1.2.4; ОПК-12.5; ОПК-1.2.5; ОПК-12.6; ОПК-1.2.6; ОПК-12.7; ОПК-1.3.1; ОПК-13.1; ОПК-1.3.2; ОПК-13.2; ОПК-13.3; ОПК-1.3.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-14.1; ОПК-14.2; ОПК-14.3; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.7; ОПК-14.8; ОПК-14.9; ОПК-14.10; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14; ОПК-15.1; ОПК-15.2; ОПК-15.3; ОПК-15.4; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8; ОПК-16.1; ОПК-16.2; ОПК-16.3; ОПК-16.4; ОПК-16.5; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10; ОПК-16.11; ОПК-16.12; ОПК-16.13; ОПК-16.14; ОПК-16.15; ОПК-16.16; ОПК-17.1; ОПК-17.2; ОПК-17.3; ОПК-17.4; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4
Б3.01(Д)	Подготовка к защите и защита выпускной квалификационной работы	УК-1.1; УК-1.2; УК-1.3; УК-2.1; УК-2.2; УК-2.3; УК-2.4; УК-2.5; УК-3.1; УК-3.2; УК-3.3; УК-4.1; УК-4.2; УК-4.3; УК-4.4; УК-4.5; УК-4.6; УК-5.1; УК-5.2; УК-6.1; УК-6.2; УК-7.1; УК-7.2; УК-7.3; УК-7.4; УК-7.5; УК-7.6; УК-8.1; УК-8.2; УК-8.3; УК-8.4; УК-9.1; УК-9.2; УК-9.3; УК-9.4; УК-9.5; УК-10.1; УК-10.2; УК-10.3; ОПК-1.1; ОПК-1.2; ОПК-1.3; ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-2.5; ОПК-2.6; ОПК-2.7; ОПК-2.8; ОПК-2.9; ОПК-2.10; ОПК-2.11; ОПК-2.12; ОПК-2.13; ОПК-2.14; ОПК-3.1; ОПК-3.2; ОПК-3.3; ОПК-3.4; ОПК-3.5; ОПК-3.6; ОПК-3.7; ОПК-3.8; ОПК-3.9; ОПК-3.10; ОПК-3.11; ОПК-3.12; ОПК-3.13; ОПК-3.14; ОПК-3.15; ОПК-3.16; ОПК-3.17; ОПК-3.18; ОПК-3.19; ОПК-3.20; ОПК-3.21; ОПК-3.22; ОПК-3.23; ОПК-3.24; ОПК-3.25; ОПК-3.26; ОПК-3.27; ОПК-3.28; ОПК-3.29; ОПК-3.30; ОПК-3.31; ОПК-3.32; ОПК-3.33; ОПК-3.34; ОПК-3.35; ОПК-3.36; ОПК-3.37; ОПК-3.38; ОПК-3.39; ОПК-3.40; ОПК-3.41; ОПК-3.42; ОПК-3.43; ОПК-3.44; ОПК-3.45; ОПК-3.46; ОПК-3.47; ОПК-3.48; ОПК-3.49; ОПК-3.50; ОПК-3.51; ОПК-3.52; ОПК-3.53; ОПК-3.54; ОПК-3.55; ОПК-3.56; ОПК-3.57; ОПК-3.58; ОПК-4.1; ОПК-4.2; ОПК-4.3; ОПК-4.4; ОПК-4.5; ОПК-4.6; ОПК-4.7; ОПК-4.8; ОПК-4.9; ОПК-4.10; ОПК-4.11; ОПК-4.12; ОПК-4.13; ОПК-4.14; ОПК-4.15; ОПК-4.16; ОПК-4.17; ОПК-4.18; ОПК-4.19; ОПК-4.20; ОПК-4.21; ОПК-4.22; ОПК-5.1; ОПК-5.2; ОПК-5.3; ОПК-5.4; ОПК-5.5; ОПК-5.6; ОПК-5.7; ОПК-5.8; ОПК-5.9; ОПК-5.10; ОПК-5.11; ОПК-5.12; ОПК-5.13; ОПК-5.14; ОПК-5.15; ОПК-5.16; ОПК-5.17; ОПК-5.18; ОПК-5.19; ОПК-6.1; ОПК-6.2; ОПК-6.3; ОПК-6.4; ОПК-6.5; ОПК-6.6; ОПК-6.7; ОПК-6.8; ОПК-6.9; ОПК-6.10; ОПК-7.1; ОПК-7.2; ОПК-7.3; ОПК-7.4; ОПК-7.5; ОПК-7.6; ОПК-7.7; ОПК-7.8; ОПК-7.9; ОПК-7.10; ОПК-7.11; ОПК-7.12; ОПК-7.13; ОПК-7.14; ОПК-7.15; ОПК-7.16; ОПК-8.1; ОПК-8.2; ОПК-8.3; ОПК-8.4; ОПК-8.5; ОПК-8.6; ОПК-8.7; ОПК-8.8; ОПК-8.9; ОПК-8.10; ОПК-8.11; ОПК-8.12;

		ОПК-8.13; ОПК-8.14; ОПК-8.15; ОПК-9.1; ОПК-9.2; ОПК-9.3; ОПК-9.4; ОПК-9.5; ОПК-9.6; ОПК-9.7; ОПК-9.8; ОПК-9.9; ОПК-9.10; ОПК-9.11; ОПК-9.12; ОПК-9.13; ОПК-9.14; ОПК-9.15; ОПК-9.16; ОПК-9.17; ОПК-10.1; ОПК-10.2; ОПК-10.3; ОПК-10.4; ОПК-10.5; ОПК-10.6; ОПК-10.7; ОПК-10.8; ОПК-10.9; ОПК-10.10; ОПК-10.11; ОПК-10.12; ОПК-10.13; ОПК-10.14; ОПК-10.15; ОПК-10.16; ОПК-10.17; ОПК-10.18; ОПК-10.19; ОПК-10.20; ОПК-10.21; ОПК-10.22; ОПК-10.23; ОПК-10.24; ОПК-10.25; ОПК-10.26; ОПК-10.27; ОПК-10.28; ОПК-11.1; ОПК-1.1.1; ОПК-1.1.2; ОПК-11.2; ОПК-1.1.3; ОПК-11.3; ОПК-11.4; ОПК-1.1.4; ОПК-11.5; ОПК-1.1.5; ОПК-1.1.6; ОПК-11.6; ОПК-1.1.7; ОПК-11.7; ОПК-11.8; ОПК-11.9; ОПК-11.10; ОПК-12.1; ОПК-1.2.1; ОПК-12.2; ОПК-1.2.2; ОПК-1.2.3; ОПК-12.3; ОПК-12.4; ОПК-1.2.4; ОПК-12.5; ОПК-1.2.5; ОПК-12.6; ОПК-1.2.6; ОПК-12.7; ОПК-1.3.1; ОПК-13.1; ОПК-1.3.2; ОПК-13.2; ОПК-13.3; ОПК-1.3.3; ОПК-13.4; ОПК-13.5; ОПК-13.6; ОПК-13.7; ОПК-13.8; ОПК-13.9; ОПК-13.10; ОПК-13.11; ОПК-13.12; ОПК-13.13; ОПК-13.14; ОПК-13.15; ОПК-13.16; ОПК-13.17; ОПК-13.18; ОПК-13.19; ОПК-13.20; ОПК-13.21; ОПК-13.22; ОПК-13.23; ОПК-13.24; ОПК-14.1; ОПК-14.2; ОПК-14.3; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.7; ОПК-14.8; ОПК-14.9; ОПК-14.10; ОПК-14.11; ОПК-14.12; ОПК-14.13; ОПК-14.14; ОПК-15.1; ОПК-15.2; ОПК-15.3; ОПК-15.4; ОПК-15.5; ОПК-15.6; ОПК-15.7; ОПК-15.8; ОПК-16.1; ОПК-16.2; ОПК-16.3; ОПК-16.4; ОПК-16.5; ОПК-16.6; ОПК-16.7; ОПК-16.8; ОПК-16.9; ОПК-16.10; ОПК-16.11; ОПК-16.12; ОПК-16.13; ОПК-16.14; ОПК-16.15; ОПК-16.16; ОПК-17.1; ОПК-17.2; ОПК-17.3; ОПК-17.4; ПК-1.1; ПК-1.2; ПК-1.3; ПК-2.1; ПК-2.2; ПК-2.3; ПК-2.4; ПК-3.1; ПК-3.2; ПК-3.3; ПК-3.4
ФТД	Факультативные дисциплины	ОПК-2.3; ПК-3.2; ПК-3.4
ФТД.01	Защита персональных данных	ПК-3.2; ПК-3.4
ФТД.02	Реляционные системы управления базами данных	ОПК-2.3

Приложение 4

Календарный учебный график 2025-2026 г.

Мес	Сентябрь					Октябрь				Ноябрь				Декабрь					Январь				Февраль			
Пн	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23
Вт	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	3	10	17	24
Ср	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	4	11	18	25
Чт	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	5	12	19	26
Пт	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	27
Сб	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28
Вс	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1	8	15	22	1
Нед	1		2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Пн																		*				К			*
Вт									*									*				К			
Ср																		*	Э	Э	К	К			
Чт																	*	*							
Пт																	*								
Сб																	*								

Мес	Март					Апрель				Май					Июнь				Июль				Август				
Пн	2	9	16	23	2	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31
Вт	3	10	17	24	3	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	
Ср	4	11	18	25	4	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	
Чт	5	12	19	26	5	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	
Пт	6	13	20	27	6	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	
Сб	7	14	21	28	7	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	
Вс	8	15	22	29	8	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	
Нед	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
Пн	*																										К
Вт																											
Ср															Э	Э	Э	К	К	К	К	К	К	К	К		
Чт															Э												
Пт								*						*	Э												
Сб										*					Э												

Календарный учебный график 2026-2027 г.

Мес	Сентябрь					Октябрь				Ноябрь					Декабрь				Январь				Февраль			
Пн		7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1	8	15	22
Вт	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23
Ср	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	3	10	17	24
Чт	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	4	11	18	25
Пт	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	5	12	19	26
Сб	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	27
Вс	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28
Нед	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Пн																		*				Э	К		
Вт																		*				К	К	*	
Ср										*								*				К			
Чт																		*				К			
Пт																	*	*				К			
Сб																	*	Э				К			

Мес	Март					Апрель				Май					Июнь				Июль				Август				
Пн	1	8	15	22	1	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30
Вт	2	9	16	23	2	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31
Ср	3	10	17	24	3	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	
Чт	4	11	18	25	4	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	
Пт	5	12	19	26	5	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	
Сб	6	13	20	27	6	10	17	24	31	7	14	21	28	5	12	19	26	3	10	17	24	31	7	14	21	28	
Вс	7	14	21	28	7	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	
Нед	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53				
Пн											Э				Э				К								
Вт											Э				К												
Ср											Э	Э	Э	Э	К	К	К	К	К	К	К	К					
Чт											Э				К												
Пт											Э				К												
Сб											*				К												

Календарный учебный график 2027-2028 г.

Мес	Сентябрь					Октябрь				Ноябрь					Декабрь				Январь					Февраль				Март				Апрель				Май				Июнь				Июль					Август			
Пн		6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28
Вт		7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1	8	15	22	29	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29
Ср	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30
Чт	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	3	10	17	24	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31
Пт	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	4	11	18	25	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	
Сб	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	5	12	19	26	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	
Вс	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	27	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	
Нед	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
Пн																						Э														*					*				Э								К
Вт																						Э															*								Э								К
Ср																			*		Э	Э	К			*			*														Э	К	К	К	К	К	К	К	К
Чт										*												Э																		Э	Э			К								К
Пт																				Э		К																					К								
Сб																		*		Э		К																		Э				К								

Календарный учебный график 2028-2029 г.

Мес	Сентябрь					Октябрь					Ноябрь				Декабрь				Январь					Февраль				Март				Апрель				Май				Июнь				Июль					Август			
Пн		4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	5	12	19	26	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27
Вт		5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	27	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28
Ср		6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29
Чт		7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1	8	15	22	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30
Пт	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31
Сб	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	3	10	17	24	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	
Вс	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	4	11	18	25	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	
Нед	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
Пн																				*		Э	К																		Э												К
Вт																						Э	К													*					Э	*											К
Ср																			*		Э	Э	Э	К												*					Э	Э	Э	У	У	К	К	К	К	К	К	К	К
Чт																				Э				К				*												Э	Э											К
Пт																				Э				К		*														Э	Э											К
Сб										*										Э				К																Э	Э											

Календарный учебный график 2029-2030 г.

Мес	Сентябрь					Октябрь					Ноябрь				Декабрь					Январь				Февраль				Март				Апрель					Май				Июнь				Июль					Август				
Пн		3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	4	11	18	25	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26
Вт		4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	5	12	19	26	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27
Ср		5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	27	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28
Чт		6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29
Пт		7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1	8	15	22	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30
Сб	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31
Вс	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	3	10	17	24	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	
Нед	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53
Пн											*								*			Э				П	П		П	Э										П												
Вт																		*	*			Э				П	П		П												П												
Ср																		*			Э	Э			П	П	П		П						*						*												
Чт																		*			Э	Э			П	П	П		Э							*					П												
Пт																		*		Э		К			П	*	П		Э												П												
Сб																		*		Э		К		*	П	П	П		Э								П					П												

Календарный учебный график 2030-2031 г.

Мес	Сентябрь						Октябрь					Ноябрь				Декабрь					Январь					Февраль				Март					Апрель					Май					Июнь					Июль					Август					
Пн		2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	3	10	17	24	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1
Вт		3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	4	11	18	25	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2
Ср		4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	5	12	19	26	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	3
Чт		5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6	13	20	27	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	4
Пт		6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	7	14	21	28	7	14	21	28	4	11	18	25	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	5
Сб		7	14	21	28	5	12	19	26	2	9	16	23	30	7	14	21	28	4	11	18	25	1	8	15	22	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28	5	12	19	26	2	9	16	23	30	6
Вс	1	8	15	22	29	6	13	20	27	3	10	17	24	1	8	15	22	29	5	12	19	26	2	9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22	29	6	13	20	27	3	10	17	24	31	
Нед	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
Пн											*			Э					Пд	*				Д			*	К	=																									
Вт														Э					Пд	*				Д			К	К	=																									
Ср													Э	Э					*	*				Д			К	К	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=
Чт													Э	Э	Пд	Пд	Пд	Пд	*	Д	Д	Д	Д	К	К	К	=	=																									
Пт													Э	Пд					*	Д				К			К	=	=																									
Сб													Э	Пд					*	Д				К			К	=	=																									

Сводные данные

		Курс 1			Курс 2			Курс 3			Курс 4			Курс 5			Курс 6			Итого
		Сем. 1	Сем. 2	Всего	Сем. 3	Сем. 4	Всего	Сем. 5	Сем. 6	Всего	Сем. 7	Сем. 8	Всего	Сем. 9	Сем. A	Всего	Сем. B	Сем. C	Всего	
	Теоретическое обучение и практики	17 4/6	18	35 4/6	17 2/6	16	33 2/6	18	18	36	17 3/6	15	32 3/6	18 3/6	9 3/6	28	11 1/6		11 1/6	176 4/6
Э	Экзаменационные сессии	2	2 4/6	4 4/6	3 2/6	4	7 2/6	2	2 4/6	4 4/6	4	2 4/6	6 4/6	2	2 4/6	4 4/6	1 2/6		1 2/6	29 2/6
У	Учебная практика											2	2							2
П	Производственная практика														8	8				8
Пд	Преддипломная практика																4 4/6		4 4/6	4 4/6
Д	Подготовка к процедуре защиты и защита выпускной квалификационной работы																4		4	4
К	Продолжительность каникул	10 дн	57 дн	67 дн	8 дн	57 дн	65 дн	10 дн	57 дн	67 дн	7 дн	54 дн	61 дн	10 дн	55 дн	65 дн	27 дн		27 дн	352 дн
*	Нерабочие праздничные дни (не включая воскресенья)	8 дн	5 дн	13 дн	8 дн	5 дн	13 дн	8 дн	5 дн	13 дн	8 дн	5 дн	13 дн	8 дн	5 дн	13 дн	9 дн		9 дн	74 дн
Продолжительность		157 дн	208 дн	365 дн	162 дн	203 дн	365 дн	159 дн	207 дн	366 дн	167 дн	198 дн	365 дн	163 дн	202 дн	365 дн	186 дн		186 дн	
Студентов																				
Групп																				

Приложение 5

Пример учебного плана
Учебный план 1 курс

№	Индекс	Наименование	Семестр 1									Семестр 2									Итого за курс									Каф.	Семестр
			Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель		
				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль			
ИТОГО (с факультативами)				**1017**							**28,25**	19 4/6		**1209**							**31,75**	20 4/6		**2226**							**60**	40 2/6		
ИТОГО по ОП (без факультативов)				**1017**							**28,25**			**1209**							**31,75**			**2226**							**60**			
УЧЕБНАЯ НАГРУЗКА, (акад.час/нед)		ОП, факультативы (в период ТО)		**53,5**										**59,2**										**56,4**									
		ОП, факультативы (в период экз. сес.)		**36**										**54**										**45**									
		Ауд. нагр. (ОП - элект. курсы по физ.к.)		**34,5**										**34**										**34,3**									
		Конт. раб. (ОП - элект. курсы по физ.к.)		**34,5**										**34**										**34,3**									
		Ауд. нагр. (элект. курсы по физ.к.)												**2,7**										**1,4**									
ДИСЦИПЛИНЫ (МОДУЛИ)				**1017**	**608**	**258**	**38**	**312**	**337**	**72**	**28,25**	ТО: 17 2/3☐ Э: 2		**1209**	**660**	**282**	**60**	**318**	**405**	**144**	**31,75**	ТО: 18[Э: 2 2/3		**2226**	**1268**	**540**	**98**	**630**	**742**	**216**	**60**	ТО: 35 2/3☐ Э: 4 2/3		
1	Б1.О.02	История России		**63**	50	34		16	13		1,75		ЗаО	**81**	66	34		32	15		2,25		ЗаО	**144**	116	68		48	28		4		28	12
2	Б1.О.03	Иностранный язык	ЗаО	**72**	34			34	38		2		ЗаО	**72**	34			34	38		2		ЗаО(2)	**144**	68			68	76		4		52	1234
3	Б1.О.05	Физическая культура и спорт	За	**72**	66	8		58	6		2												За	**72**	66	8		58	6		2		21	1
4	Б1.О.08	Правовые и организационные основы противодействия противоправному поведению											За	**72**	36	18		18	36		2		За	**72**	36	18		18	36		2		94	2
5	Б1.О.11	Введение в специальность	За	**72**	16	16			56		2												За	**72**	16	16			56		2		148	1
6	Б1.О.12	Основы российской государственности	За	**72**	48	16		32	24		2												За	**72**	48	16		32	24		2		161	1
7	Б1.О.13	Механика и оптика											ЗаО	**108**	50	34	16		58		3		ЗаО	**108**	50	34	16		58		3		118	2
8	Б1.О.18	Математический анализ	Эк	**171**	100	50		50	35	36	4,75		Эк	**153**	100	50		50	17	36	4,25		Эк(2)	**324**	200	100		100	52	72	9		118	12
9	Б1.О.19	Геометрия	ЗаО	**72**	50	34		16	22		2												ЗаО	**72**	50	34		16	22		2		118	1
10	Б1.О.22	Аппаратные средства вычислительной техники											За	**72**	50	34		16	22		2		За	**72**	50	34		16	22		2		116	2
11	Б1.О.23	Линейная алгебра											Эк	**144**	68	34		34	40	36	4		Эк	**144**	68	34		34	40	36	4		118	2
12	Б1.О.25	Дискретная математика											ЗаО	**144**	68	34		34	40	36	4		ЗаО	**144**	68	34		34	40	36	4		118	23
13	Б1.О.31	Информатика	Эк	**144**	68	34		34	40	36	4												Эк	**144**	68	34		34	40	36	4		116	1
14	Б1.О.36	Введение в программирование	ЗаО	**108**	68	34	34		40		3												ЗаО	**108**	68	34	34		40		3		117	1
15	Б1.О.55	Дисциплины специализации											Эк	**180**	68	34	34		76	36	5		Эк	**180**	68	34	34		76	36	5			269В
16	Б1.О.55.05	Алгоритмы и структуры данных											Эк	**180**	68	34	34		76	36	5		Эк	**180**	68	34	34		76	36	5		117	2
17	Б1.В.06	Дисциплины военного модуля	За	**171**	108	32	4	72	63		4,75		За	**117**	72	10	10	52	45		3,25		За(2)	**288**	180	42	14	124	108		8			123456789А
18	Б1.В.06.01	Военно-специальные дисциплины												**18**	8		4	4	10		0,5			**18**	8		4	4	10		0,5			23456789
19	Б1.В.06.01.03	Артиллерийское вооружение												**18**	8		4	4	10		0,5			**18**	8		4	4	10		0,5		177	234
20	Б1.В.06.02	Тактические и тактико-специальные дисциплины		**63**	36	22		14	27		1,75		За	**99**	64	10	6	48	35		2,75		За	**162**	100	32	6	62	62		4,5			123678
21	Б1.В.06.02.01	Тактика		**45**	26	18		8	19		1,25			**45**	26	2	6	18	19		1,25			**90**	52	20	6	26	38		2,5		176	12368
22	Б1.В.06.02.03	Военная топография и топогеодезическая подготовка		**18**	10	4		6	8		0,5		За	**54**	38	8		30	16		1,5		За	**72**	48	12		36	24		2		177	12
23	Б1.В.06.03	Общевоенные дисциплины	За	**108**	72	10	4	58	36		3												За	**108**	72	10	4	58	36		3		176	189
24	Б1.В.07	Элективные дисциплины по физической культуре и спорту (модуль)											За	**66**	48			48	18				За	**66**	48			48	18				21	23456
25	Б1.В.07.ДВ.01.01	Легкая атлетика											За	**66**	48			48	18				За	**66**	48			48	18				21	23456
26	*Б1.В.07.ДВ.01.02*	*Волейбол*											За	**66**	48			48	18				За	**66**	48			48	18					23456
27	*Б1.В.07.ДВ.01.03*	*Бадминтон*											За	**66**	48			48	18				За	**66**	48			48	18					23456
28	*Б1.В.07.ДВ.01.04*	*Баскетбол*											За	**66**	48			48	18				За	**66**	48			48	18					23456
29	*Б1.В.07.ДВ.01.05*	*Гандбол*											За	**66**	48			48	18				За	**66**	48			48	18					23456
30	*Б1.В.07.ДВ.01.06*	*Мини-футбол*											За	**66**	48			48	18				За	**66**	48			48	18					23456
31	*Б1.В.07.ДВ.01.07*	*Настольный теннис*											За	**66**	48			48	18				За	**66**	48			48	18					23456
32	*Б1.В.07.ДВ.01.08*	*Лыжные гонки*											За	**66**	48			48	18				За	**66**	48			48	18					23456
33	*Б1.В.07.ДВ.01.09*	*Плавание*											За	**66**	48			48	18				За	**66**	48			48	18					23456
34	*Б1.В.07.ДВ.01.10*	*Спортивная борьба*											За	**66**	48			48	18				За	**66**	48			48	18					23456
35	*Б1.В.07.ДВ.01.11*	*Спортивная аэробика*											За	**66**	48			48	18				За	**66**	48			48	18					23456
ФОРМЫ КОНТРОЛЯ			Эк(2) За(4) ЗаО(3)										Эк(3) За(4) ЗаО(4)										Эк(5) За(8) ЗаО(7)											
ПРАКТИКИ		(План)																															
ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ		(План)																															
КАНИКУЛЫ												1 3/6										8 1/6									9 4/6		

Учебный план 2 курс

№	Индекс	Наименование	Семестр 3									Семестр 4									Итого за курс									Каф.	Семестр
			Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель		
				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль			
ИТОГО (с факультативами)				**1155**							**30,25**	20 4/6		**1137**							**29,75**	20		**2292**							**60**	40 4/6		
ИТОГО по ОП (без факультативов)				**1155**							**30,25**			**1137**							**29,75**			**2292**							**60**			
УЧЕБНАЯ НАГРУЗКА, (акад.час/нед)		ОП, факультативы (в период ТО)		**58,4**										**57,6**										**58**									
		ОП, факультативы (в период экз. сес.)		**43,2**										**54**										**48,6**									
		Ауд. нагр. (ОП - элект. курсы по физ.к.)		**35,5**										**33,5**										**34,5**									
		Конт. раб. (ОП - элект. курсы по физ.к.)		**35,5**										**33,5**										**34,5**									
		Ауд. нагр. (элект. курсы по физ.к.)		**2,8**										**3**										**2,9**									
ДИСЦИПЛИНЫ (МОДУЛИ)				**1155**	**662**	**234**	**138**	**290**	**349**	**144**	**30,25**	ТО: 17 1/3□ Э: 3 1/3		**1137**	**584**	**192**	**114**	**278**	**337**	**216**	**29,75**	ТО: 16 Э: 4		**2292**	**1246**	**426**	**252**	**568**	**686**	**360**	**60**	ТО: 33 1/3□ Э: 7 1/3		
1	Б1.О.03	Иностранный язык	ЗаО	**72**	36			36	36		2		Эк	**108**	32			32	40	36	3		Эк ЗаО	**180**	68			68	76	36	5		52	1234
2	Б1.О.14	Электричество и магнетизм	ЗаО	**108**	66	34	16	16	42		3												ЗаО	**108**	66	34	16	16	42		3		118	3
3	Б1.О.20	Теория вероятностей и математическая статистика	Эк	**126**	68	34		34	22	36	3,5		Эк	**162**	80	32	32	16	46	36	4,5		Эк(2)	**288**	148	66	32	50	68	72	8		118	34
4	Б1.О.21	Алгебра											Эк	**144**	64	32		32	44	36	4		Эк	**144**	64	32		32	44	36	4		118	4
5	Б1.О.25	Дискретная математика	Эк	**144**	68	34		34	40	36	4												Эк	**144**	68	34		34	40	36	4		118	23
6	Б1.О.26	Дифференциальные уравнения	ЗаО	**72**	50	34		16	22		2												ЗаО	**72**	50	34		16	22		2		118	3
7	Б1.О.27	Методы вычислений											За	**180**	80	32	32	16	64	36	5		За	**180**	80	32	32	16	64	36	5		118	4
8	Б1.О.35	Объектно-ориентированное программирование	Эк	**108**	50	16	34		22	36	3												Эк	**108**	50	16	34		22	36	3		117	3
9	Б1.О.37	Методы программирования	ЗаО	**90**	50	16	34		40		2,5		Эк	**126**	64	16	32	16	26	36	3,5		Эк ЗаО	**216**	114	32	66	16	66	36	6		117	34
10	Б1.О.39	Основы информационной безопасности	Эк	**144**	68	34		34	40	36	4												Эк	**144**	68	34		34	40	36	4		148	3
11	Б1.О.49	Организационное и правовое обеспечение информационной безопасности											ЗаО	**72**	48	16		32	24		2		ЗаО	**72**	48	16		32	24		2		148	4
12	Б1.О.53	Уравнения математической физики											За	**72**	48	32		16	24		2		За	**72**	48	32		16	24		2		118	4
13	Б1.О.54	Комплексный анализ											За	**72**	48	32		16	24		2		За	**72**	48	32		16	24		2		118	4
14	Б1.В.06	Дисциплины военного модуля	За(2)	**135**	108	16	20	72	27		3,75		Эк	**135**	72		18	54	27	36	3,75		Эк За(2)	**270**	180	16	38	126	54	36	7,5			123456789A
15	Б1.В.06.01	Военно-специальные дисциплины	За	**81**	58	8	6	44	23		2,25		Эк	**135**	72		18	54	27	36	3,75		Эк За	**216**	130	8	24	98	50	36	6			23456789
16	Б1.В.06.01.01	Стрельба и управление огнем		**27**	18	8	2	8	9		0,75			**27**	24		6	18	3		0,75			**54**	42	8	8	26	12		1,5		177	3456789
17	Б1.В.06.01.03	Артиллерийское вооружение	За	**54**	40		4	36	14		1,5		Эк	**108**	48		12	36	24	36	3		Эк За	**162**	88		16	72	38	36	4,5		177	234
18	Б1.В.06.02	Тактические и тактико-специальные дисциплины	За	**54**	50	8	14	28	4		1,5												За	**54**	50	8	14	28	4		1,5			123678
19	Б1.В.06.02.01	Тактика	За	**54**	50	8	14	28	4		1,5												За	**54**	50	8	14	28	4		1,5		176	12368
20	Б1.В.07	Элективные дисциплины по физической культуре и спорту (модуль)	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36				21	23456
21	Б1.В.07.ДВ.01.01	Легкая атлетика	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36				21	23456
22	*Б1.В.07.ДВ.01.02*	*Волейбол*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
23	*Б1.В.07.ДВ.01.03*	*Бадминтон*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
24	*Б1.В.07.ДВ.01.04*	*Баскетбол*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
25	*Б1.В.07.ДВ.01.05*	*Гандбол*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
26	*Б1.В.07.ДВ.01.06*	*Мини-футбол*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
27	*Б1.В.07.ДВ.01.07*	*Настольный теннис*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
28	*Б1.В.07.ДВ.01.08*	*Лыжные гонки*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
29	*Б1.В.07.ДВ.01.09*	*Плавание*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
30	*Б1.В.07.ДВ.01.10*	*Спортивная борьба*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
31	*Б1.В.07.ДВ.01.11*	*Спортивная аэробика*	За	**66**	48			48	18				За	**66**	48			48	18				За(2)	**132**	96			96	36					23456
32	Б1.В.ДВ.02.01	Языки программирования	ЗаО	**90**	50	16	34		40		2,5												ЗаО	**90**	50	16	34		40		2,5		117	3
33	*Б1.В.ДВ.02.02*	*Алгоритмы машинной графики*	ЗаО	**90**	50	16	34		40		2,5												ЗаО	**90**	50	16	34		40		2,5		118	3
34	*Б1.В.ДВ.02.03*	*Психолого-педагогическое сопровождение лиц с ограниченными возможностями здоровья*	ЗаО	**90**	50	16	34		40		2,5												ЗаО	**90**	50	16	34		40		2,5		111	3
ФОРМЫ КОНТРОЛЯ			Эк(4) За(3) ЗаО(5)										Эк(5) За(4) ЗаО										Эк(9) За(7) ЗаО(6)											
ПРАКТИКИ		(План)																															
ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ		(План)																															
КАНИКУЛЫ												1 1/6										8 1/6										9 2/6		

Учебный план 3 курс

№	Индекс	Наименование	Семестр 5										Семестр 6										Итого за курс										Каф.	Семестр
			Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель		
				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль	Всего			
ИТОГО (с факультативами)				**1101**							**28,75**	20		**1189**							**31,25**	20 4/6		**2290**							**60**	40 4/6		
ИТОГО по ОП (без факультативов)				**1101**							**28,75**			**1189**							**31,25**			**2290**							**60**			
УЧЕБНАЯ НАГРУЗКА, (акад.час/нед)		ОП, факультативы (в период ТО)		**55,2**										**58,1**										**56,7**										
		ОП, факультативы (в период экз. сес.)		**54**										**54**										**54**										
		Ауд. нагр. (ОП - элект. курсы по физ.к.)		**31,7**										**30,3**										**31**										
		Конт. раб. (ОП - элект. курсы по физ.к.)		**31,7**										**30,3**										**31**										
		Ауд. нагр. (элект. курсы по физ.к.)		**2,7**										**2,7**										**2,7**										
ДИСЦИПЛИНЫ (МОДУЛИ) И РАССРЕД. ПРАКТИКИ				**1101**	**618**	**248**	**116**	**254**	**375**	**108**	**28,75**	ТО: 18 Э: 2		**1189**	**592**	**244**	**158**	**190**	**453**	**144**	**31,25**	ТО: 18 Э: 2 2/3		**2290**	**1210**	**492**	**274**	**444**	**828**	**252**	**60**	ТО: 36 Э: 4 2/3		
1	Б1.О.07	Современные теории и технологии развития личности											ЗаО	**72**	50	16		34	22		2		ЗаО	**72**	50	16		34	22		2		107	6
2	Б1.О.16	Квантовая теория											Эк	**108**	50	34		16	22	36	3		Эк	**108**	50	34		16	22	36	3		118	6
3	Б1.О.17	Электроника и схемотехника	Эк	**144**	68	34	34		40	36	4												Эк	**144**	68	34	34		40	36	4		116	5
4	Б1.О.24	Математическая логика и теория алгоритмов	За	**144**	72	36		36	72		4												За	**144**	72	36		36	72		4		118	5
5	Б1.О.28	Методы оптимизации	ЗаО	**108**	68	34		34	40		3												ЗаО	**108**	68	34		34	40		3		118	5
6	Б1.О.29	Теория информации	Эк	**144**	68	34		34	40	36	4												Эк	**144**	68	34		34	40	36	4		116	5
7	Б1.О.32	Операционные системы	Эк	**108**	50	34	16		22	36	3												Эк	**108**	50	34	16		22	36	3		116	5
8	Б1.О.33	Сети и системы передачи информации											ЗаО	**108**	66	34	16	16	42		3		ЗаО	**108**	66	34	16	16	42		3		116	6
9	Б1.О.40	Модели безопасности компьютерных систем											Эк	**108**	50	34		16	22	36	3		Эк	**108**	50	34		16	22	36	3		148	6
10	Б1.О.41	Защита в операционных системах											ЗаО	**108**	68	34	34		40		3		ЗаО	**108**	68	34	34		40		3		116	6
11	Б1.О.48	Управление ресурсами в системах информационной безопасности	За	**72**	32	16		16	40		2												За	**72**	32	16		16	40		2		149	5
12	Б1.О.51	Защита информации от утечки по техническим каналам											Эк	**144**	68	34	34		40	36	4		Эк	**144**	68	34	34		40	36	4		148	6
13	Б1.О.55	Дисциплины специализации											ЗаО	**108**	68	34	34		40		3		ЗаО	**108**	68	34	34		40		3			269В
14	Б1.О.55.03	Методы и стандарты оценки защищенности компьютерных систем											ЗаО	**108**	68	34	34		40		3		ЗаО	**108**	68	34	34		40		3		148	6
15	Б1.В.01	Стеганография и цифровые водяные знаки											Эк	**144**	50	16	34		58	36	4		Эк	**144**	50	16	34		58	36	4		148	6
16	Б1.В.06	Дисциплины военного модуля	За	**153**	108	8	14	86	45		4,25		За	**117**	72	8	6	58	45		3,25		За(2)	**270**	180	16	20	144	90		7,5			123456789А
17	Б1.В.06.01	Военно-специальные дисциплины	За	**153**	108	8	14	86	45		4,25		За	**99**	66	2	6	58	33		2,75		За(2)	**252**	174	10	20	144	78		7			23456789
18	Б1.В.06.01.01	Стрельба и управление огнем		**63**	48	8	2	38	15		1,75		За	**63**	44	2	2	40	19		1,75		За	**126**	92	10	4	78	34		3,5		177	3456789
19	Б1.В.06.01.02	Боевая работа	За	**90**	60		12	48	30		2,5			**36**	22		4	18	14		1		За	**126**	82		16	66	44		3,5		177	567
20	Б1.В.06.02	Тактические и тактико-специальные дисциплины												**18**	6	6			12		0,5			**18**	6	6			12		0,5			123678
21	Б1.В.06.02.01	Тактика												**18**	6	6			12		0,5			**18**	6	6			12		0,5		176	12368
22	Б1.В.07	Элективные дисциплины по физической культуре и спорту (модуль)	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34				21	23456
23	Б1.В.07.ДВ.01.01	Легкая атлетика	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34				21	23456
24	*Б1.В.07.ДВ.01.02*	*Волейбол*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
25	*Б1.В.07.ДВ.01.03*	*Бадминтон*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
26	*Б1.В.07.ДВ.01.04*	*Баскетбол*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
27	*Б1.В.07.ДВ.01.05*	*Гандбол*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
28	*Б1.В.07.ДВ.01.06*	*Мини-футбол*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
29	*Б1.В.07.ДВ.01.07*	*Настольный теннис*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
30	*Б1.В.07.ДВ.01.08*	*Лыжные гонки*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
31	*Б1.В.07.ДВ.01.09*	*Плавание*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
32	*Б1.В.07.ДВ.01.10*	*Спортивная борьба*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
33	*Б1.В.07.ДВ.01.11*	*Спортивная аэробика*	За	**66**	48			48	18				За	**64**	48			48	16				За(2)	**130**	96			96	34					23456
34	Б1.В.ДВ.01.01	Язык программирования Java	За	**72**	32	16	16		40		2												За	**72**	32	16	16		40		2		117	5
35	*Б1.В.ДВ.01.02*	*Язык программирования C#*	За	**72**	32	16	16		40		2												За	**72**	32	16	16		40		2		117	5
36	*Б1.В.ДВ.01.03*	*Правовые и организационные основы добровольческой (волонтерской) деятельности*	За	**72**	32	16	16		40		2												За	**72**	32	16	16		40		2		99	5
37	*Б1.В.ДВ.01.04*	*Основы конструктивного взаимодействия лиц с ограниченными возможностями здоровья в образовательном процессе*	За	**72**	32	16	16		40		2												За	**72**	32	16	16		40		2		111	5
38	*Б1.В.ДВ.01.05*	*Общественный проект "Обучение служением"*	За	**72**	8			8	64		2												За	**72**	8			8	64		2		118	5
39	Б1.В.ДВ.05.01	Разработка приложений на C++	ЗаО	**90**	72	36	36		18		2,5												ЗаО	**90**	72	36	36		18		2,5		148	5
40	*Б1.В.ДВ.05.02*	*Обработка изображений*	ЗаО	**90**	72	36	36		18		2,5												ЗаО	**90**	72	36	36		18		2,5		148	5
41	**Б2.О.01(У)**	**Учебная практика (экспериментально-исследовательская)**											За КР	**108**	2			2	106		3		За КР	**108**	2			2	106		3		148	6
ФОРМЫ КОНТРОЛЯ			Эк(3) За(5) ЗаО(2)										Эк(4) За(3) ЗаО(4) КР										Эк(7) За(8) ЗаО(6) КР											
ПРАКТИКИ		(План)																																
ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ		(План)																																
КАНИКУЛЫ												1 2/6									8 1/6										9 3/6		

Учебный план 4 курс

№	Индекс	Наименование	Семестр 7									Семестр 8									Итого за курс									Каф.	Семестр
			Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель		
				Всего	Конт такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	СР	Конт роль			
ИТОГО (с факультативами)				**1161**							**32,25**	21 3/6		**1071**							**29,75**	19 4/6		**2232**							**62**	41 1/6		
ИТОГО по ОП (без факультативов)				**1161**							**32,25**			**999**							**27,75**			**2160**							**60**			
УЧЕБНАЯ НАГРУЗКА, (акад.час/нед)		ОП, факультативы (в период ТО)		**54**										**54,6**										**54,3**									
		ОП, факультативы (в период экз. сес.)		**54**										**54**										**54**									
		Ауд. нагр. (ОП - элект. курсы по физ.к.)		**36**										**25,9**										**31**									
		Конт. раб. (ОП - элект. курсы по физ.к.)		**36**										**25,9**										**31**									
		Ауд. нагр. (элект. курсы по физ.к.)																															
ДИСЦИПЛИНЫ (МОДУЛИ)				**1161**	**630**	**264**	**154**	**212**	**315**	**216**	**32,25**	ТО: 17 1/2□ Э: 4		**963**	**402**	**206**	**102**	**94**	**417**	**144**	**26,75**	ТО: 15□ Э: 2 2/3		**2124**	**1032**	**470**	**256**	**306**	**732**	**360**	**59**	ТО: 32 1/2□ Э: 6 2/3		
1	Б1.О.01	Философия	ЗаО	**108**	68	34		34	40		3												ЗаО	**108**	68	34		34	40		3		109	7
2	Б1.О.04	Безопасность жизнедеятельности											За	**72**	32	16		16	40		2		За	**72**	32	16		16	40		2		181	8
3	Б1.О.09	Проектный менеджмент											ЗаО	**72**	28	14		14	44		2		ЗаО	**72**	28	14		14	44		2		149	8
4	Б1.О.10	Экономика и финансовая грамотность	ЗаО	**72**	50	16		34	22		2												ЗаО	**72**	50	16		34	22		2		83	7
5	Б1.О.15	Термодинамика	Эк	**108**	50	34		16	22	36	3												Эк	**108**	50	34		16	22	36	3		118	7
6	Б1.О.30	Технологии обработки информации	Эк	**144**	68	34	34		40	36	4												Эк	**144**	68	34	34		40	36	4		148	7
7	Б1.О.34	Компьютерные сети	Эк	**144**	66	34	16	16	42	36	4												Эк	**144**	66	34	16	16	42	36	4		116	7
8	Б1.О.38	Системы управления базами данных	Эк	**144**	84	34	34	16	24	36	4												Эк	**144**	84	34	34	16	24	36	4		116	7
9	Б1.О.42	Основы построения защищенных компьютерных сетей											Эк	**144**	70	42	28		38	36	4		Эк	**144**	70	42	28		38	36	4		116	8
10	Б1.О.43	Основы построения защищенных баз данных											Эк	**144**	56	28	28		52	36	4		Эк	**144**	56	28	28		52	36	4		117	8
11	Б1.О.44	Защита программ и данных											Эк	**108**	42	28	14		30	36	3		Эк	**108**	42	28	14		30	36	3		155	8
12	Б1.О.45	Методы и средства криптографической защиты информации	ЗаО	**108**	68	34	34		40		3												ЗаО	**108**	68	34	34		40		3		148	7
13	Б1.О.50	Инсталляция и настройка программного обеспечения											За	**72**	32	16	16		40		2		За	**72**	32	16	16		40		2		117	8
14	Б1.В.02	Моделирование систем	Эк	**144**	68	34	34		40	36	4												Эк	**144**	68	34	34		40	36	4		148	7
15	Б1.В.03	Технологии защищенного документооборота и блокчейн											За КР	**144**	56	28	14	14	88		4		За КР	**144**	56	28	14	14	88		4		148	8
16	Б1.В.06	Дисциплины военного модуля	Эк За	**189**	108	10	2	96	45	36	5,25		Эк	**135**	72	20	2	50	27	36	3,75		Эк(2) За	**324**	180	30	4	146	72	72	9			123456789A
17	Б1.В.06.01	Военно-специальные дисциплины	Эк	**117**	60	6	2	52	21	36	3,25			**36**	32	14		18	4		1		Эк	**153**	92	20	2	70	25	36	4,25			23456789
18	Б1.В.06.01.01	Стрельба и управление огнем		**27**	22	6	2	14	5		0,75			**36**	32	14		18	4		1			**63**	54	20	2	32	9		1,75		177	3456789
19	Б1.В.06.01.02	Боевая работа	Эк	**90**	38			38	16	36	2,5												Эк	**90**	38			38	16	36	2,5		177	567
20	Б1.В.06.02	Тактические и тактико-специальные дисциплины	За	**72**	48	4		44	24		2		Эк	**90**	36	2	2	32	18	36	2,5		Эк За	**162**	84	6	2	76	42	36	4,5			123678
21	Б1.В.06.02.01	Тактика											Эк	**90**	36	2	2	32	18	36	2,5		Эк	**90**	36	2	2	32	18	36	2,5		176	12368
22	Б1.В.06.02.02	Артиллерийская разведка	За	**72**	48	4		44	24		2												За	**72**	48	4		44	24		2		177	7
23	Б1.В.06.03	Общевоенные дисциплины												**9**	4	4			5		0,25			**9**	4	4			5		0,25		176	189
24	ФТД.02	Реляционные системы управления базами данных											За	**72**	14	14			58		2		За	**72**	14	14			58		2		116	8
ФОРМЫ КОНТРОЛЯ			Эк(6) За ЗаО(3)										Эк(4) За(4) ЗаО КР										Эк(10) За(5) ЗаО(4) КР										
ПРАКТИКИ (План)														108	2			2	106		3	2		108	2			2	106		3	2		
	Б2.О.02(У)	Учебный сбор											ЗаО	108	2			2	106		3	2	ЗаО	108	2			2	106		3	2	176	8
ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ (План)																																	
КАНИКУЛЫ												1										7 5/6										8 5/6		

Учебный план 5 курс

№	Индекс	Наименование	Семестр 9									Семестр А									Итого за курс									Каф.	Семестр
			Контроль	Академических часов						з.е.	Недель	Контроль	Академических часов						з.е.	Недель	Контроль	Академических часов						з.е.				
				Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль			Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль			Всего	Кон такт.	Лек	Лаб	Пр	СР	Конт роль	Всего	Недель		
ИТОГО (с факультативами)				**1098**						**30,5**	20 3/6		**1134**						**31,5**	20 1/6		**2232**						**62**	40 4/6		
ИТОГО по ОП (без факультативов)				**1026**						**28,5**			**1134**						**31,5**			**2160**						**60**			
УЧЕБНАЯ НАГРУЗКА, (акад.час/нед)		ОП, факультативы (в период ТО)		**53,6**									**58,8**									**56,2**									
		ОП, факультативы (в период экз. сес.)		**54**									**54**									**54**									
		Ауд. нагр. (ОП - элект. курсы по физ.к.)		**16,8**									**28**									**22,4**									
		Конт. раб. (ОП - элект. курсы по физ.к.)		**16,8**									**28**									**22,4**									
		Ауд. нагр. (элект. курсы по физ.к.)																														
ДИСЦИПЛИНЫ (МОДУЛИ) И РАССРЕД. ПРАКТИКИ				**1098**	**342**	**166**	**108**	**68**	**648**	**108**	**30,5**	ТО: 18 1/2□ Э: 2		**702**	**266**	**116**	**124**	**26**	**292**	**144**	**19,5**	ТО: 9 1/2□ Э: 2 2/3		**1800**	**608**	**282**	**232**	**94**	**940**	**252**	**50**	ТО: 28□ Э: 4 2/3		
1	Б1.О.46	Криптографические протоколы										Эк	**144**	56	28	28		52	36	4		Эк	**144**	56	28	28		52	36	4		148	A
2	Б1.О.47	Теоретико-числовые методы в криптографии	Эк	**180**	108	54	54		36	36	5											Эк	**180**	108	54	54		36	36	5		148	9
3	Б1.О.52	Теория радиотехнических систем										Эк	**180**	74	24	24	26	70	36	5		Эк	**180**	74	24	24	26	70	36	5		116	A
4	Б1.О.55	Дисциплины специализации	ЗаО	**108**	72	36	36		36		3											ЗаО	**108**	72	36	36		36		3			269В
5	Б1.О.55.01	Методы верификации	ЗаО	**108**	72	36	36		36		3											ЗаО	**108**	72	36	36		36		3		148	9
6	Б1.В.04	Методология экспериментальных исследований и испытаний										Эк	**144**	48	24	24		60	36	4		Эк	**144**	48	24	24		60	36	4		148	A
7	Б1.В.05	Анализ уязвимостей программного обеспечения										ЗаО	**108**	40	16	24		68		3		ЗаО	**108**	40	16	24		68		3		148	A
8	Б1.В.06	Дисциплины военного модуля	Эк За	**180**	72	24		48	72	36	5	Эк	**36**						36	1		Эк(2) За	**216**	72	24		48	72	72	6			123456789A
9	Б1.В.06.01	Военно-специальные дисциплины	Эк	**117**	28			28	53	36	3,25											Эк	**117**	28			28	53	36	3,25			23456789
10	Б1.В.06.01.01	Стрельба и управление огнем	Эк	**117**	28			28	53	36	3,25											Эк	**117**	28			28	53	36	3,25		177	3456789
11	Б1.В.06.03	Общевоенные дисциплины	За	**63**	44	24		20	19		1,75											За	**63**	44	24		20	19		1,75		176	189
12	Б1.В.06.04(К)	Итоговый междисциплинарный экзамен военного модуля										Эк	**36**						36	1		Эк	**36**						36	1		176	A
13	Б1.В.ДВ.03.01	Биометрические методы идентификации личности	Эк	**162**	54	36	18		72	36	4,5											Эк	**162**	54	36	18		72	36	4,5		148	9
14	*Б1.В.ДВ.03.02*	*Язык HTML*	Эк	**162**	54	36	18		72	36	4,5											Эк	**162**	54	36	18		72	36	4,5		117	9
15	Б1.В.ДВ.04.01	Параллельные алгоритмы обработки данных										ЗаО	**90**	48	24	24		42		2,5		ЗаО	**90**	48	24	24		42		2,5		116	A
16	*Б1.В.ДВ.04.02*	*Технологии интернет вещей*										ЗаО	**90**	48	24	24		42		2,5		ЗаО	**90**	48	24	24		42		2,5		116	A
17	**Б2.О.03(Н)**	**Производственная практика (научно-исследовательская работа)**	ЗаО	**396**	4			4	392		11											ЗаО	**396**	4			4	392		11		148	9
18	ФТД.01	Защита персональных данных	За	**72**	32	16		16	40		2											За	**72**	32	16		16	40		2		116	9
ФОРМЫ КОНТРОЛЯ			Эк(3) За(2) ЗаО(2)									Эк(4) ЗаО(2)										Эк(7) За(2) ЗаО(4)										
ПРАКТИКИ		(План)											432	6			6	426		12	8		432	6			6	426		12	8		
	Б2.О.05(П)	Войсковая стажировка										ЗаО	216	3			3	213		6	4	ЗаО	216	3			3	213		6	4	176	A
	Б2.О.06(П)	Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности										ЗаО	216	3			3	213		6	4	ЗаО	216	3			3	213		6	4	148	A
ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ		(План)																														
КАНИКУЛЫ											1 2/6										8									9 2/6		

Учебный план 6 курс

№	Индекс	Наименование	Семестр B									Семестр C									Итого за курс									Каф.	Семестр
			Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель	Контроль	Академических часов							з.е.	Недель		
				Всего	Конт такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	СР	Конт роль	Всего			
ИТОГО (с факультативами)				**1080**							**30**	21 1/6												**1080**							**30**	21 1/6		
ИТОГО по ОП (без факультативов)				**1080**							**30**													**1080**							**30**			
УЧЕБНАЯ НАГРУЗКА, (акад.час/нед)		ОП, факультативы (в период ТО)		**48,4**																				**24,2**										
		ОП, факультативы (в период экз. сес.)		**54**																				**27**										
		Ауд. нагр. (ОП - элект. курсы по физ.к.)		**14,6**																				**7,3**										
		Конт. раб. (ОП - элект. курсы по физ.к.)		**14,6**																				**7,3**										
		Ауд. нагр. (элект. курсы по физ.к.)																																
ДИСЦИПЛИНЫ (МОДУЛИ) И РАССРЕД. ПРАКТИКИ				**612**	**163**	**80**	**30**	**53**	**377**	**72**	**17**	ТО: 11 1/6□ Э: 1 1/3										ТО: □ Э:		**612**	**163**	**80**	**30**	**53**	**377**	**72**	**17**	ТО: 11 1/6□ Э: 1 1/3		
1	Б1.О.06	Коммуникативные технологии профессионального общения	За	**72**	40	20		20	32		2												За	**72**	40	20		20	32		2		65	В
2	Б1.О.55	Дисциплины специализации	Эк(2)	**360**	120	60	30	30	168	72	10												Эк(2)	**360**	120	60	30	30	168	72	10			269В
3	Б1.О.55.02	Алгоритмы кодирования и сжатия информации	Эк	**180**	60	30		30	84	36	5												Эк	**180**	60	30		30	84	36	5		148	В
4	Б1.О.55.04	Интеллектуальные системы обработки информации	Эк	**180**	60	30	30		84	36	5												Эк	**180**	60	30	30		84	36	5		148	В
5	**Б2.В.01(П)**	**Производственная практика (технологическая)**	ЗаО	**180**	3			3	177		5												ЗаО	**180**	3			3	177		5		148	В
ФОРМЫ КОНТРОЛЯ			Эк(2) За ЗаО																				Эк(2) За ЗаО											
ПРАКТИКИ		(План)		252	2			2	250		7	4 2/3												252	2			2	250		7	4 2/3		
	Б2.О.04(Пд)	Производственная практика (преддипломная)	ЗаО	252	2			2	250		7	4 2/3											ЗаО	252	2			2	250		7	4 2/3	148	В
ГОСУДАРСТВЕННАЯ ИТОГОВАЯ АТТЕСТАЦИЯ		(План)		216					207	9	6	4												216					207	9	6	4		
	Б3.01(Д)	Подготовка к защите и защита выпускной квалификационной работы	Эк	216					207	9	6	4											Эк	216					207	9	6	4	148	В
КАНИКУЛЫ												3 5/6																				3 5/6		

Приложение 6

Материально-техническое обеспечение

Материально-техническое обеспечение основной образовательной программы высшего образования – программы бакалавриата/ программы магистратуры/ программы специалитета

_____

(*код, наименование основной образовательной программы – профиль/специализация*)

N п/п	Наименование учебных предметов, курсов, дисциплин (модулей), практики, иных видов учебной деятельности, предусмотренных учебным планом образовательной программы	Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом (в случае реализации образовательной программы в сетевой форме дополнительно указывается наименование организации, с которой заключен договор)
1	2	3	4
	Б1.О.01 Философия Б1.О.02 История России Б1.О.06 Коммуникативные технологии профессионального общения Б1.О.07 Современные теории и технологии развития личности Б1.О.08 Правовые и организационные основы противодействия противоправному поведению Б1.О.09 Проектный менеджмент Б1.О.10 Экономика и финансовая грамотность Б1.О.12 Основы российской государственности Б1.О.14 Электричество и магнетизм	Аудитории 477, 479, 380, 381, 382, 383, 384, 385, 387, 290, 291, 292, 293, 295, 297, 301п, 303п, 305п, 307п, 314п, 316п, 505п Перечень оборудования, имеющегося в указанных аудиториях, представлен в приложении 6-1. Перечень программного обеспечения, имеющегося во всех указанных аудиториях, представлен в приложении 6-2.	Адреса указанных помещений даны в приложении 6-3

	Б1.О.15	Термодинамика		
	Б1.О.16	Квантовая теория		
	Б1.О.18	Математический анализ		
	Б1.О.19	Геометрия		
	Б1.О.20	Теория вероятностей и математическая статистика		
	Б1.О.21	Алгебра		
	Б1.О.22	Аппаратные средства вычислительной техники		
	Б1.О.23	Линейная алгебра		
	Б1.О.24	Математическая логика и теория алгоритмов		
	Б1.О.25	Дискретная математика		
	Б1.О.26	Дифференциальные уравнения		
	Б1.О.27	Методы вычислений		
	Б1.О.28	Методы оптимизации		
	Б1.О.29	Теория информации		
	Б1.О.31	Информатика		
	Б1.О.33	Сети и системы передачи информации		
	Б1.О.34	Компьютерные сети		
	Б1.О.37	Методы программирования		
	Б1.О.38	Системы управления базами данных		
	Б1.О.39	Основы информационной безопасности		
	Б1.О.40	Модели безопасности компьютерных систем		
	Б1.О.48	Управление ресурсами в системах информационной безопасности		
	Б1.О.49	Организационное и правовое обеспечение информационной безопасности		
	Б1.О.52	Теория радиотехнических систем		
	Б1.О.53	Уравнения математической физики		

	Б1.О.54	Комплексный анализ		
	Б1.О.55	Дисциплины специализации		
	Б1.О.55.02	Алгоритмы кодирования и сжатия информации		
	Б1.В.03	Технологии защищенного документооборота и блокчейн		
	Б1.О.11	Введение в специальность	Аудитории 477, 479, 380, 381, 382, 383, 384, 385, 387, 290, 291, 292, 293, 295, 297, 301п, 303п, 314п, 316п, 505п Перечень оборудования, имеющегося в указанных аудиториях, представлен в приложении 6-1. Перечень программного обеспечения, имеющегося во всех указанных аудиториях, представлен в приложении 6-2.	Адреса указанных помещений даны в приложении 6-3
	Б1.О.13	Механика и оптика		
	Б1.О.17	Электроника и схемотехника		
	Б1.О.30	Технологии обработки информации		
	Б1.О.32	Операционные системы		
	Б1.О.35	Объектно-ориентированное программирование		
	Б1.О.36	Введение в программирование		
	Б1.О.41	Защита в операционных системах		
	Б1.О.42	Основы построения защищенных компьютерных сетей		
	Б1.О.43	Основы построения защищенных баз данных		
	Б1.О.44	Защита программ и данных		
	Б1.О.45	Методы и средства криптографической защиты информации		
	Б1.О.46	Криптографические протоколы		
	Б1.О.47	Теоретико-числовые методы в криптографии		
	Б1.О.50	Инсталляция и настройка программного обеспечения		
	Б1.О.51	Защита информации от утечки по техническим каналам		
	Б1.О.55.01	Методы верификации		

	Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем Б1.О.55.04 Интеллектуальные системы обработки информации Б1.О.55.05 Алгоритмы и структуры данных Б1.В.01 Стеганография и цифровые водяные знаки Б1.В.02 Моделирование систем Б1.В.04 Методология экспериментальных исследований и испытаний Б1.В.05 Анализ уязвимостей программного обеспечения Б1.В.06.03 Общевоенные дисциплины		
	Б1.В.06 Дисциплины военного модуля Б1.В.06.01 Военно-специальные дисциплины Б1.В.06.01.01 Стрельба и управление огнем Б1.В.06.01.02 Боевая работа Б1.В.06.01.03 Артиллерийское вооружение Б1.В.06.02 Тактические и тактико-специальные дисциплины Б1.В.06.02.01 Тактика Б1.В.06.02.02 Артиллерийская разведка Б1.В.06.02.03 Военная топография и топогеодезическая подготовка Б1.В.06.03 Общевоенные дисциплины		
	Физическая культура и спорт	Зал игровых видов спорта (442 кв. м.),	394018, г. Воронеж, пл. Университетская, д. 1, пом. I,

		помещения для переодевания (2), душевые комнаты (2) Оборудование: щиты баскетбольные (4), табло баскетбольное электронное (1), табло судейское (2), стойки волейбольные (2), вышка судейская (2), сетка волейбольная (2), антенны волейбольные (2), карманы для волейбольных антенн (2), защита для волейбольных стоек (1), стойки для бадминтона (8), сетка для бадминтона (4), перекладина низкая 90 см (2), коврик для прыжков в длину с места (2), платформа для сгибания и разгибания рук в упоре лежа (1), шведская стенка (8), скамейка гимнастическая 4 м (11), мат гимнастический (11), тумба для измерения гибкости (1), линейка для измерения гибкости (2), лестница координационная (5), канат 10 м (1), ворота мини-футбольные с сетками (2), стол для настольного тенниса (1), сетка для настольного тенниса (1), винтовка пневматическая спортивная МР532 (1), пневматическое ружье «Диана» (1), сейф под винтовки (1). Инвентарь: мяч волейбольный (30), мяч баскетбольный (20), ракетки для бадминтона (40), воланы для бадминтона (30), обруч металлический (5), скакалки (30), ракетки для настольного тенниса (6), мячи для настольного тенниса (9), конусы разметочные (20).	ауд. 300
	Элективные дисциплины по физической культуре и спорту	Зал игровых видов спорта (442 кв. м.), помещения для переодевания (2), душевые комнаты (2) Оборудование: щиты баскетбольные (4), табло баскетбольное электронное (1), табло судейское (2), стойки волейбольные (2), вышка судейская (2), сетка волейбольная (2), антенны волейбольные (2), карманы для волейбольных антенн (2), защита для волейбольных стоек (1), стойки для бадминтона (8), сетка для бадминтона	394018, г. Воронеж, пл. Университетская, д. 1, пом. I, ауд. 300

		(4), перекладина низкая 90 см (2), коврик для прыжков в длину с места (2), платформа для сгибания и разгибания рук в упоре лежа (1), шведская стенка (8), скамейка гимнастическая 4 м (11), мат гимнастический (11), тумба для измерения гибкости (1), линейка для измерения гибкости (2), лестница координационная (5), канат 10 м (1), ворота мини-футбольные с сетками (2), стол для настольного тенниса (1), сетка для настольного тенниса (1), винтовка пневматическая спортивная МР532 (1), пневматическое ружье «Диана» (1), сейф под винтовки (1). Инвентарь: мяч волейбольный (30), мяч баскетбольный (20), ракетки для бадминтона (40), воланы для бадминтона (30), обруч металлический (5), скакалки (30), ракетки для настольного тенниса (6), мячи для настольного тенниса (9), конусы разметочные (20).	
	Иностранный язык	Учебная аудитория 308п: видеомагнитофоны Philips, Samsung, аудиомагнитофоны Panasonic, Sony. Специализированная мебель. Учебная аудитория 309п: видеомагнитофоны Philips, Samsung, аудиомагнитофоны Panasonic, Sony. Специализированная мебель.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 308п 394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 309п
	Безопасность жизнедеятельности	Учебная аудитория, учебный виртуальный (симуляционный) клинико-диагностический центр Специализированная мебель, Роботизированный манекен симулятор взрослого человека для отработки сестринских навыков (консоль преподавателя и консоль студента), роботизированный манекен-симулятор взрослого для отработки навыков оказания неотложной помощи (консоли преподавателя и студента), симуляционная он-лайн система отработки навыков ЭКГ, цифровой манекен аускультации сердца и легких; манекен-симулятор взрослого	394018, г. Воронеж, ул. Пушкинская, д. 16, ауд. 111

		мужчины для отработки навыков ухода за пациентом; манекен-тренажер взрослой женщины для отработки навыков сестринского ухода; манекен-симулятор взрослого для отработки навыков проведения сердечно-легочной реанимации; прозрачный манекен-симулятор для отработки навыков промывания желудка; профессиональный тренажер оценки эффективности навыка инъекций и пункций; тренажер для отработки навыков внутривенных инъекций, инфузий и пункций (рука от плеча до кисти с электронной помпой для циркуляции крови); тренажер для отработки навыков внутримышечных инъекций в плечо; тренажер для отработки навыков внутримышечных инъекций в ягодицу (с моделью анатомического строения); тренажер-накладка для отработки навыков внутримышечных, подкожных и внутрикожных инъекций; тренажер для отработки навыков внутримышечных инъекций в ягодицу Учебная аудитория Специализированная мебель, индивидуальные противохимические пакеты, пакеты перевязочные индивидуальные, комплект индивидуальный медицинский гражданской защиты, общевойсковой защитный комплект, противогазы, респираторы, таблицы по теме «Средства индивидуальной защиты», «Коллективные средства защиты», дозиметр-радиометр, бытовой дозиметр «Эколог», измеритель мощности экспозиционной дозы, комплект индивидуальных дозиметров, войсковой прибор химической разведки, тренажер сердечно-легочной реанимации, жгуты кровоостанавливающие с дозированной компрессией для само- и взаимопомощи, устройства для проведения искусственного	 394018, г. Воронеж, ул. Пушкинская, д. 16, ауд. 112

		дыхания "Рот-устройство-рот" Учебная аудитория Специализированная мебель, проектор, ноутбук, экран для проектора, обучающие фильмы, видеоролики департамента гражданской защиты по мероприятиям первой помощи, WinPro 8 RUS Upgrd OLP NL Acdmc, Office Standard 2019 Single OLV NL Each Aca-demic Edition Additional Product, браузер Google Chrome	 394018, г. Воронеж, ул. Пушкинская, д. 16, ауд. 114
	Помещение для самостоятельной работы	Аудитории 385, 290, 301п, 303п, 305п, 314п, 316п	Адреса указанных помещений даны в приложении 6-3
	Учебная практика, экспериментально-исследовательская	Аудитории 477, 293, 295 Перечень оборудования, имеющегося в указанных аудиториях, представлен в приложении 6-1. Перечень программного обеспечения, имеющегося во всех указанных аудиториях, представлен в приложении 6-2.	Адреса указанных помещений даны в приложении 6-3
	Учебный сбор		
	Производственная практика, научно-исследовательская работа	Аудитории 316П Перечень оборудования, имеющегося в указанных аудиториях, представлен в приложении 6-1. Перечень программного обеспечения, имеющегося во всех указанных аудиториях, представлен в приложении 6-2.	Адреса указанных помещений даны в приложении 6-3
	Производственная практика, преддипломная	Аудитории 316П Перечень оборудования, имеющегося в указанных аудиториях, представлен в приложении 6-1. Перечень программного обеспечения, имеющегося во всех указанных аудиториях, представлен в приложении 6-2.	Адреса указанных помещений даны в приложении 6-3

	Войсковая стажировка		
	Производственная практика, по получению профессиональных умений и навыков в области профессиональной деятельности	Аудитории 316П Перечень оборудования, имеющегося в указанных аудиториях, представлен в приложении 6-1. Перечень программного обеспечения, имеющегося во всех указанных аудиториях, представлен в приложении 6-2.	Адреса указанных помещений даны в приложении 6-3
		В соответствии с договором № 427 от 20.05.2019 г. о практической подготовке обучающихся	107023, г. Москва, ул. Измайловский Вал, д. 30 ООО «Философия.ИТ» (Лига цифровой экономики)
		В соответствии с договором № 564 от 11.05.2021 г. о практической подготовке обучающихся	394036, г. Воронеж, ул. Карла Маркса, д. 53, оф. 501 ООО «Ангелы ИТ»
		В соответствии с договором № 273 от 24.02.2021 г. о практической подготовке обучающихся	125009, г. Москва, ул. Воздвиженка, д. 10 Акционерное общество «Банк ДОМ.РФ»
		В соответствии с договором № 22/01-2 от 20.01.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Свободы, д. 69, оф. 45 ООО «ЭЛ-ЭКС»
		В соответствии с договором № 22/02-10 от 21.02.2022 г. о практической подготовке обучающихся	394006, г. Воронеж, ул. Карла Маркса, д. 46 Управление Федеральной налоговой службы по Воронежской области
		В соответствии с договором № 22/05-20 от 05.05.22 г. о практической подготовке обучающихся	г. Воронеж, ул. Средне-Московская, д. 1Д, пом. 1 ООО «СёрфСтудио»
		В соответствии с договором № 22/01-1 от 20.01.2022 г. о практической подготовке обучающихся	г. Воронеж, ул. Текстильщиков, д. 5Б, пом. 177 ООО «ФИТТИН»
		В соответствии с договором № 22/05-51 от 12.05.2022 г. о практической подготовке обучающихся	Юридический адрес: 394018, г. Воронеж, ул. Плехановская, д. 33, кв. 24; фактический адрес: 394007, г. Воронеж, Спортивная набережная, д. 4В, офис 2 ООО «Инлайн Консалтинг»

		В соответствии с договором № 22/05-21 от 05.05.2022 г. о практической подготовке обучающихся	394000, г. Воронеж, ул. Пятницкого, 55 ООО ТК «Контакт»
		В соответствии с № 22/05-36 от 12.05.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Средне-Московская, д. 6а, помещение V ООО «Техномаркет»
		В соответствии с договором № 22/05-33 от 12.05.2022 г. о практической подготовке обучающихся	394006, г. Воронеж, ул. 20-Летия Октября, д. 103, оф. 430 ООО «САФИБ»
		В соответствии с договором № 22/26043-Д - 22/05 - 155 от 24.05.2022 о практической подготовке обучающихся	119017, г. Москва, ул. Большая Ордырка, дом 24; почтовый адрес: 115230, г. Москва, 1-й Нагатинский проезд, д. 10, стр. 1, БЦ «Newton Plaza» АО «Гринатом»
		В соответствии с договором № ДОГ-3500-22-000000176 – 22/06-28 от 27.05.2022 г. зарег. 06.06.2022 г. о практической подготовке обучающихся	162602, Вологодская обл., г. Череповец, ул. Ленина, д. 123А ОАО «Северсталь — Инфоком»
		В соответствии с договором № 22/05-148 от 20.05.2022 г. о практической подготовке обучающихся	127015, г. Москва, ул. Вятская, д. 35, стр. 4 АО «Неофлекс Консалтинг»
		В соответствии с договором № 22/09-3 от 15.09.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Володарского, д. 64 АО «Компания ТрансТелеКом»
		В соответствии с договором № 22/06-358 от 22.06.2022 г. о практической подготовке обучающихся	394056, Воронежская обл., Воронеж г., Приморская ул., дом 110, к. 2 ООО «Деловое программное обеспечение»
		В соответствии с договором № 711 от 31.05.2021 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Плехановская, д. 14 АО «Концерн «Созвездие»
		В соответствии с договором № 23/04-75 от 27.04.2023 г. о практической подготовке обучающихся	Юридический адрес: 117997, г. Москва, ул. Вавилова, д. 19; почтовый адрес: 394006, г. Воронеж, ул. 9 Января, д. 28 ПАО «Сбербанк»

	Производственная практика, технологическая	Аудитории 316П Перечень оборудования, имеющегося в указанных аудиториях, представлен в приложении 6-1. Перечень программного обеспечения, имеющегося во всех указанных аудиториях, представлен в приложении 6-2.	Адреса указанных помещений даны в приложении 6-3
		В соответствии с договором № 427 от 20.05.2019 г. о практической подготовке обучающихся	107023, г. Москва, ул. Измайловский Вал, д. 30 ООО «Философия.ИТ» (Лига цифровой экономики)
		В соответствии с договором № 564 от 11.05.2021 г. о практической подготовке обучающихся	394036, г. Воронеж, ул. Карла Маркса, д. 53, оф. 501 ООО «Ангелы ИТ»
		В соответствии с договором № 273 от 24.02.2021 г. о практической подготовке обучающихся	125009, г. Москва, ул. Воздвиженка, д. 10 Акционерное общество «Банк ДОМ.РФ»
		В соответствии с договором № 22/01-2 от 20.01.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Свободы, д. 69, оф. 45 ООО «ЭЛ-ЭКС»
		В соответствии с договором № 22/02-10 от 21.02.2022 г. о практической подготовке обучающихся	394006, г. Воронеж, ул. Карла Маркса, д. 46 Управление Федеральной налоговой службы по Воронежской области
		В соответствии с договором № 22/05-20 от 05.05.22 г. о практической подготовке обучающихся	г. Воронеж, ул. Средне-Московская, д. 1Д, пом. 1 ООО «СёрфСтудио»
		В соответствии с договором № 22/01-1 от 20.01.2022 г. о практической подготовке обучающихся	г. Воронеж, ул. Текстильщиков, д. 5Б, пом. 177 ООО «ФИТТИН»
		В соответствии с договором № 22/05-51 от 12.05.2022 г. о практической подготовке обучающихся	Юридический адрес: 394018, г. Воронеж, ул. Плехановская, д. 33, кв. 24; фактический адрес: 394007, г. Воронеж, Спортивная набережная, д. 4В, офис 2 ООО «Инлайн Консалтинг»
		В соответствии с договором № 22/05-21 от 05.05.2022 г. о практической подготовке	394000, г. Воронеж, ул. Пятницкого, 55 ООО ТК «Контакт»

		обучающихся	
		В соответствии с № 22/05-36 от 12.05.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Средне-Московская, д. 6а, помещение V ООО «Техномаркет»
		В соответствии с договором № 22/05-33 от 12.05.2022 г. о практической подготовке обучающихся	394006, г. Воронеж, ул. 20-Летия Октября, д. 103, оф. 430 ООО «САФИБ»
		В соответствии с договором № 22/26043-Д - 22/05 - 155 от 24.05.2022 о практической подготовке обучающихся	119017, г. Москва, ул. Большая Ордынка, дом 24; почтовый адрес: 115230, г. Москва, 1-й Нагатинский проезд, д. 10, стр. 1, БЦ «Newton Plaza» АО «Гринатом»
		В соответствии с договором № ДОГ-3500-22-000000176 – 22/06-28 от 27.05.2022 г. зарег. 06.06.2022 г. о практической подготовке обучающихся	162602, Вологодская обл., г. Череповец, ул. Ленина, д. 123А ОАО «Северсталь — Инфоком»
		В соответствии с договором № 22/05-148 от 20.05.2022 г. о практической подготовке обучающихся	127015, г. Москва, ул. Вятская, д. 35, стр. 4 АО «Неофлекс Консалтинг»
		В соответствии с договором № 22/09-3 от 15.09.2022 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Володарского, д. 64 АО «Компания ТрансТелеКом»
		В соответствии с договором № 22/06-358 от 22.06.2022 г. о практической подготовке обучающихся	394056, Воронежская обл., Воронеж г., Приморская ул., дом 110, к. 2 ООО «Деловое программное обеспечение»
		В соответствии с договором № 711 от 31.05.2021 г. о практической подготовке обучающихся	394018, г. Воронеж, ул. Плехановская, д. 14 АО «Концерн «Созвездие»
		В соответствии с договором № 23/04-75 от 27.04.2023 г. о практической подготовке обучающихся	Юридический адрес: 117997, г. Москва, ул. Вавилова, д. 19; почтовый адрес: 394006, г. Воронеж, ул. 9 Января, д. 28 ПАО «Сбербанк»

Приложение 6-1

Материально-техническое оснащений аудиторий

Наименование помещения (номер аудитории)	Имеющееся оборудование	Адрес
190а	Лабораторное оборудование медицинской кибернетики: рабочие места - персональные компьютеры на базе Intel i3-2120, мониторы ЖК 19" (3 шт.); электро-энцефалограф Нейрон-спектр-4 (2 шт.); кардиограф Полиспектр-12 (1 шт.); оптические микроскопы Р-1 (2 шт.); 3D-принтер (1 шт.); паяльные станции (2 шт.).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 190а
290	Учебная аудитория: персональные компьютеры на базе i7-7800x-4ГГц (12 шт.) и персональные компьютеры на базе i5-10400-2.90ГГц (14 шт.), мониторы ЖК 27" (26 шт). Лабораторное оборудование искусственного интеллекта: рабочие места - модули АО НПЦ "ЭЛВИС": процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эмулятор MC-USB-JTAG (9 шт.).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 290
291	Учебная аудитория: персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 22" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 291
292	Учебная аудитория: компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6" FHD Lenovo V155-15API.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 292
293	Учебная аудитория: персональные компьютеры на базе Core i7-11700K-3.6 ГГц, мониторы ЖК 24" (15 шт.), мультимедийный проектор, экран. Лабораторное оборудование компьютерной графики видеоадаптеры GeForce RTX 3070.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 293

295	Учебная аудитория: персональные компьютеры на базе Процессор AMD-Ryzen-7-5700X-3,4ГГц, мониторы ЖК 27" (24 шт.), мультимедийный проектор, экран. Лабораторное оборудование информационной безопасности операционных систем и программных средств защиты информации от несанкционированного доступа: учебный стенд «Программные средства защиты информации от несанкционированного доступа».	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 295
297	Учебная аудитория: ноутбуки HP EliteBook на базе Intel Core i5-8250U-3.4 ГГц, мониторы ЖК 24" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 297
380	Учебная аудитория: компьютер преподавателя i3-3240-3,4ГГц,монитор с ЖК 22", мультимедийный проектор, экран. Система Интернет-видеоконференцсвязи (корп. 1а ауд. 380) Состав системы Интернет-видеоконференцсвязи: ВКС LifeSize Team220 Camera 200 Dual, аудиосистема Defender Mercury 34 SPK-705, интерактивная доска со встроенным проектором "SmartBoard 480iv V25" Лабораторное оборудование по теоретической механике и оптике: машина Атвуда, маятник Максвелла, универсальный маятник, маятник Обербека, крутильный маятник, наклонный маятник, прибор для исследования столкновения шаров, определение скорости полета пули с помощью крутильно-баллистического маятника, изучение законов вращательного движения тел, исследование сложных колебаний, установка для измерения модуля упругости проволоки.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 380
381	Учебная аудитория: персональные компьютеры на базе Apple iMac 21,5" i3-3,6ГГц (12 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 381

382	Учебная аудитория: персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24" (16 шт.), ТВ панель-флипчарт.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 382
383	Учебная аудитория: персональные компьютеры на базе i7-9700F-3ГГц, мониторы ЖК 27" (16 шт.), мультимедийный проектор, экран. Лабораторное оборудование мобильных приложений и игр: рабочие места - персональные компьютеры на базе Intel i7-9700F, видеоадаптеры nVidia GeForce RTX2070, мониторы ЖК 27" (16 шт.); Системы виртуальной реальности HTC Vive Cosmos (2шт.); Беспроводный маршрутизатор TP-Link Archer C7.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 383
384	Учебная аудитория: персональные компьютеры на базе Intel i7-12700K-3,6ГГц, мониторы ЖК 27" (16 шт.), ТВ панель-флипчарт.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 384
385	Учебная аудитория: персональные компьютеры на базе Intel i5-12600KF-3,6ГГц, мониторы ЖК 27" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 385
387	Учебная аудитория: мультимедийный проектор, экран. Персональные компьютеры на базе i5-10400-2,9ГГц, мониторы ЖК 27" (12 шт.).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 387
477	Учебная аудитория: компьютер преподавателя i5-3220-3.3ГГц, мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 477
479	Учебная аудитория: компьютер преподавателя i5-8400-2,8ГГц, мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 479

301	Учебная аудитория: персональные компьютеры на базе Intel i3-8100-3,6ГГц, мониторы ЖК 17" (15 шт.), мультимедийный проектор, экран. Лабораторное оборудование суперкомпьютерного центра: кластер с пиковой производительностью 40 Tflops. Состав кластера: 10 узлов, каждый имеет два 12-ядерных процессора Intel Xeon E5-2680V3, 128 Гбайт ОЗУ, SSD 256 Гбайт. 7 узлов из 10 содержат по 2 ускорителя Intel Xeon Phi 7120, 3 узла - 2 ускорителя Tesla K80M. Все узлы объединены высокоскоростной сетью InfiniBand 56 Gbps; управляющий узел кластера (также сервером для хранения файлов): два 6-ядерных процессора, 64 Гбайт оперативной памяти и дисковую подсистему объемом 14 ТБайт; сервер для занятий по параллельному программированию: Intel X5650@2.67GHz 12 ядер 24 потоков, ОЗУ 36ГБ, дисковая подсистема объемом 300ГБ.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 301

303	Учебная аудитория: персональные компьютеры на базе i3-8100-3,9ГГц, мониторы ЖК 24" (13 шт.), мультимедийный проектор, экран. Лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности: стойка (коммуникационный шкаф), управляемый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528. Учебно-методический комплекс "Программно-аппаратная защита сетей с защитой от НСД" ОАО "ИнфоТеКС". Лабораторное оборудование технической защиты информации, состав ST033P "Пиранья" - многофункциональный поисковый прибор, ST03.DA - дифференциальный низкочастотный усилитель, ST03.TEST - контрольное устройство; комплекс виброакустической защиты "Соната": Соната-ИП3, Соната-СА-65М, Соната-СВ-45М; генератор-виброизлучатель (5 октав) "ГШ-1000У"; генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации; система автоматизированная оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок <Сигурд>. Программно-аппаратный комплекс для мониторинга радиообстановки в диапазоне 9 кГц - 21 ГГц «Кассандра К21». Комплекс оценки эффективности защиты речевой информации от утечки по акустическому и виброакустическому каналам, 20 – 12500 Гц.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 303
305	Учебная аудитория: ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 305

307	Учебная аудитория: персональные компьютеры на базе i3-3220-3,3ГГц, мониторы ЖК 19" (6 шт.), мультимедийный проектор, экран. Лабораторное оборудование электроники, электротехники и схемотехники: стенд для практических занятий по электрическим цепям (KL-100); стенд для изучения аналоговых электрических схем (KL-200); стенд для изучения цифровых схем (KL-300).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 307
308	Учебная аудитория: видеомагнитофоны Philips, Samsung, аудиомагнитофоны Panasonic, Sony.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 308
309	Учебная аудитория: видеомагнитофоны Philips, Samsung, аудиомагнитофоны Panasonic, Sony.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 309
314	Учебная аудитория: персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 24" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 314
316	Учебная аудитория: персональные компьютеры на базе i5-10400-2.9ГГц, мониторы ЖК 19" (30 шт.), мультимедийный проектор, экран. Лабораторное оборудование безопасности компьютерных сетей: стойка (коммуникационный шкаф), управляемый коммутатор CISCO Catalyst 2950, маршрутизатор CISCO 2811-ISR, аппаратный межсетевой экран CISCO серии ASA-5500. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с перечисленным сетевым оборудованием. Программный анализатор сетевого трафика WireShark. Программный симулятор Packet Tracer, для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ. Учебно-методический комплекс "Безопасность компьютерных сетей" ОАО "ИнфоТеКС".	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 316

403	Учебная аудитория: персональные компьютеры на базе i3-2320-3,3ГГц, мониторы ЖК 22" (7 шт.), мультимедийный проектор, экран. Лабораторное оборудование физической лаборатории с комплектом оборудования по квантовой физике: Установка для изучения космических лучей (ФПК-01); установка для определения резонансного потенциала методом Франка и Герца (ФПК-02); установка для определения длины свободного пробега частиц в воздухе (ФПК-03); установка для изучения энергетического спектра электронов (ФПК-05); установка для изучения p-n перехода (ФПК-06); установка для изучения температурной зависимости электропроводности металлов и полупроводников (ФПК-07); установка для изучения эффекта Холла в полупроводниках (ФПК-08); установка для изучения спектра атома водорода (ФПК-09); установка для изучения внешнего фотоэффекта (ФПК-10); установка для изучения абсолютно черного тела (ФПК-11); установка для изучения работы сцинтилляционного счетчика (ФПК-12); установка для изучения и анализа свойств материалов с помощью сцинтилляционного счетчика (ФПК-13).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 403
505	Учебная аудитория: компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17", мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 505

420	Лабораторное оборудование по электротехники и электроники: лабораторные стенды: полупроводниковые диоды, фотодиод, биполярный транзистор, полевой транзистор, операционный усилитель, многокаскадовый RC-усилитель, амплитудный модулятор и демодулятор, LC-генератор с индуктивной обратной связью, кварцевый генератор, RC-генератор с фазосдвигающей цепью, мультивибратор, триггер на биполярном транзисторе, основные схемы выпрямителей, универсальные логические элементы ТТЛ, регистр сдвига, счетчик	394018, г. Воронеж, площадь Университетская, д. 1, корп.1, ауд. 420
425	Лабораторное оборудование сетей и систем передачи информации: стойка (коммуникационный шкаф), 3 коммутатора CISCO WS-C2960-24TT-L, 3 маршрутизатора CISCO 2801, 2 WiFi-маршрутизатора Linksys WRT54G.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1, ауд. 425

Приложение 6-2

Перечень программного обеспечения, используемого в образовательном процессе

№ пп	Наименование ПО	Производитель ПО (или торговая марка, Или правообладатель) при наличии
1	ОС Windows v.7, 8, 10	Microsoft (прим. 1)
2	СУБД Oracle Database 11g Express Edition	Oracle
3	Microsoft Visio, Access, OneNote v. 2010-2019	Microsoft
4	Visual Studio, v. 2010-2019	Microsoft
5	Набор утилит (архиваторы, файл-менеджеры)	GNU, BSD
6	ОС GNU/Linux (CentOS) v.6-8	RedHat, GNU
7	LibreOffice v.5-7	The Document Foundation, GNU
8	Среда разработки Eclipse	Eclipse Foundation
9	GlassFish Java EE	Eclipse Foundation
10	Python ver 3.8	Python Software Foundation
11	MySQL Workbench Community	GNU
12	PyCharm Community	JetBrains
13	IntelliJ IDEA	JetBrains
14	Среда разработки NetBeans IDE	ORACLE
15	Дистрибутив Anaconda/Python	BSD
16	Системы моделрования системной Динамики Vensim	Ventana Systemms Inc.
17	Системы моделирования бизнес процессов BizAgi	BizAgi
18	Системы управления проектами Wrike	Wrike Inc.
19	Системы моделирования Modelio	Modeliosoft
20	Среда вычислений и модельно-ориентированного проектирования ENGEE	Образовательная платформа Этюд" со средой вычислений и модельно-ориентированного проектирования ENGEE (прим. 2)
21	HUGIN EXPERT / HUGIN Lite (open-source)	HUGIN EXPERT A/S
22	Справочно-правовая система (СПС)	Консультант+ (прим. 7)

	Консультант+ для образования	
23	Система программ 1С:Предприятие (учебная версия)	1С
24	Microsoft SQL Server	Microsoft
25	Packet Tracer	CISCO Systems
26	Virtual Box	ORACLE
27	Microsoft Windows Virtual PC	Microsoft
28	VLC media player	VideoLAN, GNU
29	Google Workspace for Education Fundamentals (ранее G Suite for Education и Google-Apps for Education)	Google Inc.
30	SecretNet Studio 8 (демоверсия)	ООО Код Безопасности
31	Dr. Web Enterprise Security Suite	Компания «Доктор Веб» (прим. 3)
32	XSpider	Компания Positive Technologies (прим. 4)
33	СКЗИ «КриптоПро Рутокен CSP»	Компания КриптоПро (прим. 5)
34	ViPNet	ОАО ИнфоТеКС (прим. 6)
35	ERwin Data Modeler Standard Edition	CA Technologies (лицензия до 2025 г., Contract#: 40217535)
36	Платформа электронного обучения LMS-Moodle, основа Образовательного портала «Электронный университет ВГУ»	Moodle Pty Ltd, GNU General Public License
37	PHP	PHP Group
38	Notepad++	GNU
39	PuTTY	MIT
40	Ramus Educational	Алексей Чижевский
41	ОС GNU/Linux (Ubuntu)	Canonical Ltd, GNU
42	Foxit PDF Reader	корпорация FOXIT SOFTWARE INC., проприетарная бесплатная лицензия
43	Операционная система РЕД ОС	ООО Ред Софт (прим. 9)
44	Система виртуализации РЕД Виртуализация	ООО Ред Софт (прим. 9)

Примечание 1. Все клиентские и серверные ОС и ПО Microsoft активированы в рамках подписок «Imagine. Последняя подписка по договору 3010-16/96-18 от 29.12.2018 (для активных подписчиков, возобновляется бесплатно на 1 год, последний раз в 2023г.)

Примечание 2. Лицензионный договор N75-1224/3010-15/1035-24 от 19.12.2024 о предоставлении права использования программы для ЭВМ "Образовательная платформа Этюд", N13724 от 01.06.2022 в реестре российского ПО со средой вычислений и модельно-ориентированного проектирования ENGEE (N13508 от 11.05.2022) - академическая лицензия на 36 месяцев
Примечание 3. ПО Dr. Web Enterprise Security Suite Комплексная защита Dr. Web Desktop Security Suite, 1400 ПК договор 3010-07/04-22 от 25.01.2022
Примечание 4. XSpider, лицензия на 16 хостов, сертифицированная версия, акт предоставления прав N Pr000778 от 05.06.2018
Примечание 5. Лицензия на право использования СКЗИ <КриптоПро Рутокен CSP>, акт предоставления прав N Pr000778 от 05.06.2018
Примечание 6. Академическая лицензия (на 5 лет) на Учебно-методический комплекс <Программно-аппаратная защита сетей с защитой от НСД> в составе: ПО ViPNet Administrator 4.x - 2 шт., ПО ViPNet Coordinator Windows 4.x - 2 шт., ПО ViPNet Coordinator Linux - 2 шт., ПО ViPNet Client 4.x - 20 шт., ПО ViPNet Policy Manager 4.x - 1 шт., 1 узел управления Policy Manager - 20 шт., ПО ViPNet StateWatcher 4.x - 1 шт., 1 узел мониторинга StateWatcher - 20 шт. Контракт на поставку № 3010-07/74-20 от 24.12.2020.
Примечание 7. Лицензионный договор 14-2000/RD от 10.04.2000
Примечание 8. Лицензионное соглашение с Netcracker Technology Corporation No. 1 от 14.10.2014.
Примечание 9. Соглашение о сотрудничестве между ВГУ и ООО «Ред Софт» от 18.05.2022г. №261/05-22У и соответствующие акты приема-передачи прав на операционные системы «РЕД ОС» и «Система виртуализации РЕД Виртуализация».

Приложение 6-3

Адреса (местоположения) помещений

Наименование помещения (номер аудитории)	Адрес (местоположение) помещения
190а	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 190а
290	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 290
291	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 291
292	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 292
293	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 293
295	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 295
297	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 297
380	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 380
381	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 381
382	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 382
383	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 383
384	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 384
385	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 385
387	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 387
477	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 477
479	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 479
301	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 301
303	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 303
305	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 305
307	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 307
308	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 308
309	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 309
314	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 314
316	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 316
403	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 403
505	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 505
420	394018, г. Воронеж, площадь Университетская, д. 1, корп.1, ауд. 420
425	394018, г. Воронеж, площадь Университетская, д. 1, корп.1, ауд. 425

Приложение 7

МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Декан ФКН
А.А. Крыловецкий
21.05.2025

РАБОЧАЯ ПРОГРАММА ВОСПИТАНИЯ

1. Код и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:
«Анализ безопасности компьютерных систем»

3. Квалификация выпускника: специалист

4. Составители программы: Крыловецкая Т.А., к.ф.-м.н.
(ФИО, ученая степень, ученое звание)

5. Программа рекомендована Ученым советом факультета компьютерных наук от 21.05.2025 г., протокол № 5

6. Учебный год: 2025-2026

1. Цель и задачи программы:

Цель программы – воспитание высоконравственной, духовно развитой и физически здоровой личности, обладающей социально и профессионально значимыми личностными качествами и компетенциями, способной творчески осуществлять профессиональную деятельность и нести моральную ответственность за принимаемые решения в соответствии с социокультурными и духовно-нравственными ценностями.

Задачи программы:

– формирование единого воспитательного пространства, направленного на создание условий для активной жизнедеятельности обучающихся, их гражданского и профессионального самоопределения и самореализации;

– вовлечение обучающихся в общественно-ценностные социализирующие отношения по всем направлениям воспитательной работы в вузе/на факультете;

– освоение обучающимися духовно-нравственных ценностей, гражданско-патриотических ориентиров, необходимых для устойчивого развития личности, общества, государства;

– содействие обучающимся в личностном и профессиональном самоопределении, проектировании индивидуальных образовательных траекторий и образа будущей профессиональной деятельности, поддержка деятельности обучающихся по самопознанию и саморазвитию.

2. Теоретико-методологические основы организации воспитания

В основе реализации программы лежат следующие *подходы:*

– ***системный*, который означает взаимосвязь и взаимообусловленность всех компонентов воспитательного процесса – от цели до результата;**

– ***организационно-деятельно*стный, в основе которого лежит единство сознания, деятельности и поведения и который предполагает такую организацию коллектива и личности, когда каждый обучающийся проявляет активность, инициативу, творчество, стремление к самовыражению;**

– ***личностно-ориентированный*, утверждающий признание человека высшей ценностью воспитания, активным субъектом воспитательного процесса, уникальной личностью;**

– ***комплексный подход*, подразумевающий объединение усилий всех субъектов воспитания (индивидуальных и групповых), институтов воспитания (подразделений) на уровне социума, вуза, факультета и самой личности воспитанника для успешного решения цели и задач воспитания; сочетание индивидуальных, групповых и массовых методов и форм воспитательной работы.**

Основополагающими ***принципами*** реализации программы являются:

– *системность* в планировании, организации, осуществлении и анализе воспитательной работы;

– *интеграция* внеаудиторной воспитательной работы, воспитательных аспектов учебного процесса и исследовательской деятельности;

– *мотивированность* участия обучающихся в различных формах воспитательной работы (аудиторной и внеаудиторной);

– *вариативность,* предусматривающая учет интересов и потребностей каждого обучающегося через свободный выбор альтернативных вариантов участия в направлениях воспитательной работы, ее форм и методов.

Реализация программы предусматривает использование следующих ***методов*** воспитания:

– методы формирования сознания личности (рассказ, беседа, лекция, диспут, метод примера);

– методы организации деятельности и приобретения опыта общественного поведения личности (создание воспитывающих ситуаций, педагогическое требование, инструктаж, иллюстрации, демонстрации);

– методы стимулирования и мотивации деятельности и поведения личности (соревнование, познавательная игра, дискуссия, эмоциональное воздействие, поощрение, наказание);

– методы контроля, самоконтроля и самооценки в воспитании.

При реализации программы используются следующие ***формы*** организации воспитательной работы:

– массовые формы – мероприятия на уровне университета, города, участие во всероссийских и международных фестивалях, конкурсах и т.д.;

– групповые формы – мероприятия внутри коллективов академических групп, студий творческого направления, клубов, секций, общественных студенческих объединений и др.;

– индивидуальные, личностно-ориентированные формы – индивидуальное консультирование преподавателями обучающихся по вопросам организации учебно-профессиональной и научно-исследовательской деятельности, личностного и профессионального самоопределения, выбора индивидуальной образовательной траектории и т.д.

3. Содержание воспитания

Практическая реализация цели и задач воспитания осуществляется в рамках следующих направлений воспитательной работы в вузе/на факультете:

1) духовно-нравственное воспитание;
2) гражданско-правовое воспитание;
3) патриотическое воспитание;
4) экологическое воспитание;
5) культурно-эстетическое воспитание;
6) физическое воспитание;
7) профессиональное воспитание.

3.1. Духовно-нравственное воспитание

– формирование нравственной позиции, в том нравственного сознания и поведения на основе усвоения общечеловеческих ценностей и нравственных чувств (чести, долга, справедливости, милосердия, добра, дружелюбия);

– развитие способности к сопереживанию и формированию позитивного отношения к людям, в том числе к лицам с ограниченными возможностями здоровья и инвалидам;

– формирование толерантного сознания и поведения в поликультурном мире, готовности и способности вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения;

– развитие способности к духовному развитию, реализации творческого потенциала в учебно-профессиональной деятельности на основе нравственных установок и моральных норм, непрерывного самообразования и самовоспитания;

– развитие способности к сотрудничеству с окружающими в образовательной, общественно полезной, проектной и других видах деятельности.

3.2. Гражданско-правовое воспитание

– выработка осознанной собственной позиции по отношению к общественно-политическим событиям прошлого и настоящего;

– формирование российской гражданской идентичности, гражданской позиции активного и ответственного члена российского общества, осознающего свои

конституционные права и обязанности, уважающего закон и правопорядок, обладающего чувством собственного достоинства, осознанно принимающего традиционные национальные и общечеловеческие гуманистические и демократические ценности;

– формирование установок личности, позволяющих противостоять идеологии экстремизма, национализма, ксенофобии, коррупции, дискриминации по социальным, религиозным, расовым, национальным признакам, другим негативным социальным явлениям;

– развитие студенческого самоуправления, совершенствование у обучающихся организаторских умений и навыков;

– расширение конструктивного участия обучающихся в принятии решений, затрагивающих их права и интересы, в том числе в различных формах общественной самоорганизации, самоуправления;

– поддержка инициатив студенческих объединений, развитие молодежного добровольчества и волонтерской деятельности;

– организация социально значимой общественной деятельности студенчества.

3.3. Патриотическое воспитание

– формирование чувств патриотизма, гражданственности, уважения к памяти защитников Отечества и подвигам Героев Отечества;

– формирование патриотического сознания, чувства верности своему Отечеству, стремления защищать интересы Родины и своего народа;

– формирование чувства гордости и уважения к достижениям и культуре своей Родины на основе изучения культурного наследия и традиций многонационального народа России, развитие желания сохранять ее уникальный характер и культурные особенности;

– развитие идентификации себя с другими представителями российского народа;

– вовлечение обучающихся в мероприятия военно-патриотической направленности;

– приобщение обучающихся к истории родного края, традициям вуза, развитие чувства гордости и уважения к выдающимся представителям университета;

– формирование социально значимых и патриотических качеств обучающихся.

3.4. Экологическое воспитание

– формирование экологической культуры;

– формирование бережного и ответственного отношения к своему здоровью (физическому и психологическому) и здоровью других людей, живой природе, окружающей среде;

– вовлечение обучающихся в экологические мероприятия;

– выработка умений и навыков разумного природопользования, нетерпимого отношения к действиям, приносящим вред экологии, приобретение опыта эколого-направленной деятельности;

– укрепление мотивации к физическому самосовершенствованию, занятию спортивно-оздоровительной деятельностью;

– развитие культуры безопасной жизнедеятельности, умений оказывать первую помощь;

– профилактика наркотической и алкогольной зависимости, табакокурения и других вредных привычек.

3.5. Культурно-эстетическое воспитание

– формирование эстетического отношения к миру, включая эстетику научного и технического творчества, спорта, общественных отношений и быта;

– приобщение обучающихся к истинным культурным ценностям;

– расширение знаний в области культуры, вовлечение в культурно-досуговые мероприятия;

– повышение интереса к культурной жизни региона; содействие его конкурентоспособности посредством участия во всероссийских конкурсах и фестивалях;

– создание социально-культурной среды вуза/факультета, популяризация студенческого творчества, формирование готовности и способности к самостоятельной, творческой деятельности;

– совершенствование культурного уровня и эстетических чувств обучающихся.

3.6. Физическое воспитание

– создание условий для занятий физической культурой и спортом, для развивающего отдыха и оздоровления обучающихся, включая студентов с ограниченными возможностями здоровья, студентов, находящихся в трудной жизненной ситуации, в том числе на основе развития спортивной инфраструктуры вуза/факультета и повышения эффективности ее использования;

– формирование мотивации к занятиям физической культурой и спортом, следованию здоровому образу жизни, в том числе путем пропаганды в студенческой среде необходимости участия в массовых спортивно-общественных мероприятиях, популяризации отечественного спорта и спортивных достижений страны/региона/города/вуза/факультета;

– вовлечение обучающихся в спортивные соревнования и турниры, межфакультетские и межвузовские состязания, встречи с известными спортсменами и победителями соревнований.

3.7. Профессиональное воспитание

– приобщение студентов к традициям и ценностям профессионального сообщества, нормам корпоративной этики;

– развитие профессионально значимых качеств личности будущего компетентного и ответственного специалиста в учебно-профессиональной, научно-исследовательской деятельности и внеучебной работе;

– формирование творческого подхода к самосовершенствованию в контексте будущей профессии;

– повышение мотивации профессионального самосовершенствования обучающихся средствами изучаемых учебных дисциплин, практик, научно-исследовательской и других видов деятельности;

– ориентация обучающихся на успех, лидерство и карьерный рост; формирование конкурентоспособных личностных качеств;

– освоение этических норм и профессиональной ответственности посредством организации взаимодействия обучающихся с мастерами профессионального труда.

4. Методические рекомендации по анализу воспитательной работы на факультете и проведению ее аттестации (по реализуемым направлениям подготовки/специальностям)

Ежегодно заместитель декана по воспитательной работе представляет на ученом совете факультета отчет, содержащий анализ воспитательной работы на факультете и итоги ее аттестации (по реализуемым направлениям подготовки / специальностям).

Анализ воспитательной работы на факультете проводится с ***целью*** выявления основных проблем воспитания и последующего их решения.

Основными ***принципами*** анализа воспитательного процесса являются:

– *принцип гуманистической направленности*, проявляющийся в уважительном отношении ко всем субъектам воспитательного процесса;

– *принцип приоритета анализа сущностных сторон воспитания*, ориентирующий на изучение не столько количественных его показателей, сколько качественных – таких как содержание и разнообразие деятельности, характер общения и отношений субъектов образовательного процесса и др.;

– *принцип развивающего характера осуществляемого анализа*, ориентирующий на использование его результатов для совершенствования воспитательной деятельности в вузе/на факультете: уточнения цели и задач воспитания, планирования воспитательной работы, адекватного подбора видов, форм и содержания совместной деятельности обучающихся и преподавателей;

– *принцип разделенной ответственности* за результаты профессионально-личностного развития обучающихся, ориентирующий на понимание того, что профессионально-личностное развитие – это результат влияния как социальных институтов воспитания, так и самовоспитания.

Примерная схема анализа воспитательной работы на факультете

1. Анализ целевых установок

1.1 Наличие рабочей программы воспитания по всем реализуемым на факультете ООП.

1.2 Наличие утвержденного комплексного календарного плана воспитательной работы.

2. Анализ информационного обеспечения организации и проведения воспитательной работы

2.1 Наличие доступных для обучающихся источников информации, содержащих план воспитательной работы, расписание работы студенческих клубов, кружков, секций, творческих коллективов и т.д.

3. Организация и проведение воспитательной работы

3.1 Основные направления воспитательной работы в отчетном году, использованные в ней формы и методы, степень активности обучающихся в проведении мероприятий воспитательной работы.

3.2 Проведение студенческих фестивалей, смотров, конкурсов и пр., их количество в отчетном учебном году и содержательная направленность.

3.3 Участие обучающихся и оценка степени их активности в фестивалях, конкурсах, смотрах, соревнованиях различного уровня.

3.4 Достижения обучающихся, участвовавших в фестивалях, конкурсах, смотрах, соревнованиях различного уровня (количество призовых мест, дипломов, грамот и пр.).

3.5 Количество обучающихся, участвовавших в работе студенческих клубов, творческих коллективов, кружков, секций и пр. в отчетном учебном году.

3.6 Количество обучающихся, задействованных в различных воспитательных мероприятиях в качестве организаторов и в качестве участников.

4. Итоги аттестации воспитательной работы факультета

4.1. Выполнение в отчетном году календарного плана воспитательной работы: выполнен полностью – перевыполнен (с приведением конкретных сведений о перевыполнении) – недовыполнен (с указанием причин невыполнения отдельных мероприятий).

4.2. Общее количество обучающихся, принявших участие в воспитательных мероприятиях в отчетном учебном году.

4.3. При наличии фактов пассивного отношения обучающихся к воспитательным мероприятиям: причины пассивности и предложения по ее устранению, активному вовлечению обучающихся в воспитательную работу.

4.4. Дополнительно в отчете могут быть представлены (по решению заместителя декана по воспитательной работе) сведения об инициативном участии обучающихся в воспитательных мероприятиях, не предусмотренных календарным планом воспитательной работы, о конкретных обучающихся, показавших наилучшие результаты участия в воспитательных мероприятиях и др.

Процедура аттестации воспитательной работы и выполнения календарного плана воспитательной работы

Оценочная шкала: «удовлетворительно» – «неудовлетворительно».

Оценочные критерии:

1. Количественный – участие обучающихся в мероприятиях календарного плана воспитательной работы (олимпиадах, конкурсах, фестивалях, соревнованиях и т.п.), участие обучающихся в работе клубов, секций, творческих, общественных студенческих объединений.

Воспитательная работа признается удовлетворительной при выполнении **одного из условий**:

Выполнение запланированных мероприятий по 6 из 7 направлений воспитательной работы
или
Участие не менее 80% обучающихся в мероприятиях по не менее 5 направлениям воспитательной работы
или
Охвачено 100% обучающихся по не менее 4 направлениям воспитательной работы
или
1. Охват не менее 50% обучающихся в мероприятиях по 7 направлениям воспитательной работы. 2. Наличие дополнительных достижений обучающихся (индивидуальных или групповых) в мероприятиях воспитательной направленности внутривузовского, городского, регионального, межрегионального, всероссийского или международного уровня.

2. Качественный – достижения обучающихся в различных воспитательных мероприятиях (уровень мероприятия – международный, всероссийский, региональный, университетский, факультетский; статус участия обучающихся – представители страны, области, вуза, факультета; характер участия обучающихся – организаторы, исполнители, зрители).

Способы получения информации для проведения аттестации: педагогическое наблюдение; анализ портфолио обучающихся и документации, подтверждающей их достижения (грамот, дипломов, благодарственных писем, сертификатов и пр.); беседы с обучающимися, студенческим активом факультета, преподавателями, принимающими участие в воспитательной работе, кураторами основных образовательных программ; анкетирование обучающихся (при необходимости); отчеты кураторов студенческих групп 1-2 курсов (по выбору заместителя декана по воспитательной работе и с учетом особенностей факультета).

Источники получения информации для проведения аттестации: устные, письменные, электронные (по выбору заместителя декана по воспитательной работе и с учетом особенностей факультета).

Фиксация результатов аттестации: отражаются в ежегодном отчете заместителя декана по воспитательной работе (по решению заместителя декана по воспитательной работе – в целом по факультету или отдельно по реализуемым направлениям подготовки / специальностям).

УТВЕРЖДАЮ

Декан
факультета компьютерных наук
_____ *А.А. Крыловецкий*
21.05.2025

КАЛЕНДАРНЫЙ ПЛАН ВОСПИТАТЕЛЬНОЙ РАБОТЫ
на 2025/2026 учебный год

№ п/п	Направление воспитательной работы	Мероприятие с указанием его целевой направленности	Сроки выполнения	Уровень мероприятия (федеральный, региональный, университетский, факультетский)	Исполнители
1.	2.	3.	4.	5.	6.
1.	Духовно-нравственное воспитание	День донора	Сентябрь, апрель	Региональный	Волонтерский центр ВГУ «Гравитация» Студсовет ФКН Зам. декана по восп. р-те
		Мероприятия по профилактике межнациональных конфликтов	Сентябрь	Университетский	Координационный центрСтудсовет ФКН Зам. декана по восп. р-те
		Акция «Снежный десант»	Январь	Региональный	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Мероприятия Клуба волонтеров ВГУ	В течение года	Региональный	Волонтерский центр ВГУ «Гравитация» Студсовет ФКН Зам. декана по восп. р-те
		Мероприятия волонтеров ФКН	В течение года	Региональный	Зам. декана по воспитательной работе, Студсовет ФКН Зам. декана по восп. р-те

1.		Курсы повышения квалификации ППС «Методика сохранения и укрепления традиционных российских духовно-нравственных ценностей и профилактики деструктивной идеологии»	Октябрь 2025	Университетский	Координационный центр
		Курсы повышения квалификации ППС «Современные подходы к укреплению общероссийской гражданской идентичности»	Ноябрь 2025	Университетский	Координационный центр
		Проведение интеллектуальных викторин	В течение года	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
2.	**Гражданско-правовое воспитание**	Мероприятия, посвященные Дню солидарности в борьбе с терроризмом	3 сентября	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Проведение комплекса круглых столов и лекций по противодействию экстремизму и терроризму	В течение года	Университетский	Управление по работе с молодежью, Координационный центр Студсовет ФКН Зам. декана по восп. р-те

1.	2.	3.	4.	5.	6.
		Дискуссионная площадка «Открытый диалог» по профилактике экстремизма среди молодежи со студентами	Октябрь 2025	Региональный	Координационный центр, факультет журналистики Студсовет ФКН Зам. декана по восп. р-те
		Проведение мероприятий (круглых столов, семинаров, лекций), направленных на формирование общероссийской гражданской идентичности в молодежной среде, в том числе из Календаря «100 дат российской идентичности»	В течение года	Университетский	Координационный центр Студсовет ФКН Зам. декана по восп. р-те
		Проведение мероприятий (круглых столов, семинаров, лекций, телемоста), направленных на гармонизацию межнациональных и межконфессиональных отношений в молодежной среде в рамках проекта «Наш общий дом – Россия»	В течение года	Университетский	Координационный центр Студсовет ФКН Зам. декана по восп. р-те
		Круглый стол "Безопасность в сети Интернет"	Март	Университетский	Управление по работе с молодежью, Координационный центр Студсовет ФКН Зам. декана по восп. р-те
		Секции Юридической клиники	Апрель	Университетский	Юридическая клиника ВГУ
3.	**Патриотическое воспитание**	Военно-спортивная игра для первокурсников «Впервые на Высоте 155»	Сентябрь	Университетский	Управление по работе с молодёжью
		Митинг, посвященный Дню освобождения г. Воронежа от немецко-фашистских захватчиков	25 января	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Гуманитарная помощь ветеранам	Май	Региональный	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Участие в акции "Бессмертный полк"	Май	Региональный	Управление по работе с молодежью Студсовет ФКН Зам. декана по восп. р-те

		Мероприятия, посвященные Дню Победы	Май	Региональный	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Военно-спортивная игра «Университетская Зарница»	Май	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
4.	**Экологическое воспитание**	Волонтерские акции	В течение года	Региональный	Волонтерский центр ВГУ «Гравитация» Студсовет ФКН Зам. декана по восп. р-те
		Участие в мероприятиях по благоустройству	В течение года	Региональный	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
5.	**Культурно-эстетическое воспитание**	Мероприятие в рамках адаптации первокурсников «Посвящение в студенты»	Сентябрь	Университетский	Студсовет ФКН Зам. декана по восп. р-те
		Цикл образовательных лекций для студентов в рамках подготовительной программы к фестивалю «Первокурсник – 2025»	Октябрь	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Фестиваль «Первокурсник – 2025»	Октябрь – ноябрь	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те

1.	2.	3.	4.	5.	6.
		Праздничный концерт, посвященный Дню студента	Ноябрь	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Праздничные мероприятия «Широкая масленица»	Март	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		«Мистер и Мисс студенческих отрядов ВГУ»	Март	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Творческий фестиваль студенческих отрядов ВГУ	Апрель	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Фестиваль «Университетская весна-2026»	Апрель	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Региональный фестиваль «Студенческая весна – творчество молодежи»	Апрель	Региональный	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Участие в федеральном мероприятии «Российская студенческая весна»	Май	Федеральный	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
6.	**Физическое воспитание**	Анкетирование студентов по видам спорта	Сентябрь	Университетский	Спортивный клуб, кафедра физического воспи тания и спорта Студсовет ФКН Зам. декана по восп. р-те
		Спартакиада первокурсников	Сентябрь - октябрь	Университетский	Спортивный клуб, кафедра физического воспитания и спорта
		Межфакультетская Универсиада	Февраль – май	Университетский	Спортивный клуб, кафедра физического воспитания и

					спорта Студсовет ФКН Зам. декана по восп. р-те
		Внутривузовский чемпионат АССК «Универлига»	Декабрь – март	Университетский	Управление по работе с молодёжью, спортивный клуб, кафедра физического воспитания и спорта Студсовет ФКН Зам. декана по восп. р-те
		Региональный чемпионат «Клубный турнир»	Март - апрель	Региональный	Управление по работе с молодёжью, спортивный клуб, кафедра физического воспитания и спорта Студсовет ФКН Зам. декана по восп. р-те
		Региональная Универсиада	Февраль - май	Региональный	Спортивный клуб, кафедра физического воспитания и спорта Студсовет ФКН Зам. декана по восп. р-те
		Участие в федеральном спортивном проекте «АССК.Фест»	Май	Федеральный	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те

1.	2.	3.	4.	5.	6.
7.	**Профессиональное воспитание**	Агитационная кампания по привлечению обучающихся в студенческие отряды	В течение года	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Турнир Трех Наук	Декабрь	Федеральный	Управление по инновациям
		Участие команд ФКН по спортивному программированию в олимпиадах федерального и международного уровней	В течение года	Международный	Декан, зам. декана по работе с одаренными студентами Студсовет ФКН Зам. декана по восп. р-те
		День российского студенчества	Январь	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Участие в организации и проведении межрегиональной олимпиады по информационной безопасности и программированию для студентов и школьников VrnCTF – 2026	Март	Федеральный	Зам. декана по воспитательной работе, зам. декана по работе с одаренными студентами
		Участие в организации и проведении межрегиональной олимпиады по информационной безопасности и программированию для студентов CenterCTF - 2026	Март	Федеральный	Зам. декана по воспитательной работе, зам. декана по работе с одаренными студентами
		День ФКН	Май	Университетский	Зам. декана по воспитательной работе
		«Домашняя целина» студенческих отрядов ВГУ	Май	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		Школа командных составов ВГУ	Май	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те
		«Авторская классика»	Сентябрь	Университетский	Управление по работе с молодёжью Студсовет ФКН Зам. декана по восп. р-те

Приложение 8

Аннотация рабочих программ дисциплин (модулей)

Б1.О.01 Философия

Общая трудоемкость дисциплины 3з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-1.1; УК-1.2; УК-1.3

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

− УК-1.1. Определяет пробелы в информации, необходимой для решения проблемной ситуации.

− УК-1.2. Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников.

− УК-1.3. Рассматривает возможные варианты решения задачи, оценивая достоинства и недостатки.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- формирование целостных представлений о зарождении и развитии философского знания;

- усвоение базовых понятий и категорий философской мысли, выработка умений системного изложения основных проблем теоретической философии, способствующих формированию мировоззренческой позиции

Задачи учебной дисциплины:

- развитие у студентов интереса к фундаментальным философским знаниям;

- усвоение студентами проблемного содержания основных философских концепций, направлений и школ, овладение философским категориальным аппаратом с целью развития мировоззренческих основ профессионального сознания;

- формирование у студентов знаний о современных философских проблемах бытия, познания, человека и общества;

- развитие у студентов способности использовать теоретические общефилософские знания в профессиональной практической деятельности.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.02 История России

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.

– УК-5.1. Анализирует историко-культурные традиции различных социальных групп, опираясь на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования).

– УК-5.2. Выделяет специфические черты и маркеры разных культур, религий, с последующим использованием полученных знаний в профессиональной деятельности и межкультурной коммуникации.

ОПК-17Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.

– ОПК-17.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире.

– ОПК-17.2. Знает ключевые события истории России и мира, выдающихся деятелей России.

– ОПК-17.3. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий.

– ОПК-17.4. Умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России, опираясь на принципы историзма и научной объективности.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- приобретение студентами научных и методических знаний в области истории,
- формирование теоретических представлений о закономерностях исторического процесса,
- овладение знаниями основных событий, происходящих в России и мире,
- приобретение навыков исторического анализа и синтеза.

Задачи учебной дисциплины:

- формирование у студентов научного мировоззрения, представлений о закономерностях исторического процесса;
- формирование у студентов исторического сознания, воспитания уважения к всемирной и отечественной истории, деяниям предков;
- развитие у студентов творческого мышления, выработка умений и навыков исторических исследований;
- выработка умений и навыков использования исторической информации при решении задач в практической профессиональной деятельности.

Форма(ы) промежуточной аттестации - зачет с оценкой

Б1.О.03 Иностранный язык

Общая трудоемкость дисциплины 9 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.

– УК-4.1. Выбирает на иностранном языке коммуникативно приемлемые стратегии академического и профессионального общения.

– УК-4.5. Владеет интегративными коммуникативными умениями в устной и письменной иноязычной речи в ситуациях академического и профессионального общения.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- повышение уровня владения ИЯ, достигнутого в средней школе, овладение иноязычной коммуникативной компетенцией на уровне А2+ для решения коммуникативных задач в социально-культурной, учебно-познавательной и деловой сферах иноязычного общения;

- обеспечение основ будущего профессионального общения и дальнейшего успешного самообразования.

Задачи учебной дисциплины:

Развитие умений:

- воспринимать на слух и понимать содержание аутентичных общественно-политических, публицистических (медийных) и прагматических текстов и выделять в них значимую/запрашиваемую информацию;

- понимать содержание аутентичных общественно-политических, публицистических, прагматических (информационных буклетов, брошюр/проспектов; блогов/веб-сайтов) и научно-популярных текстов; выделять значимую/запрашиваемую информацию из прагматических текстов справочно-информационного и рекламного характера

- начинать, вести/поддерживать и заканчивать диалог-расспрос об увиденном, прочитанном, диалог-обмен мнениями и диалог-интервью/собеседование при приеме на работу, соблюдая нормы речевого этикета, при необходимости используя стратегии восстановления сбоя в процессе коммуникации; расспрашивать собеседника, задавать вопросы и отвечать на них, высказывать свое мнение, просьбу, отвечать на предложение собеседника; делать сообщения и выстраивать монолог-описание, монолог-повествование и монолог-рассуждение

- заполнять формуляры и бланки прагматического характера; поддерживать контакты при помощи электронной почты; оформлять CurriculumVitae/Resume и сопроводительное письмо, необходимые при приеме на работу, выполнять письменные проектные задания.

Форма(ы) промежуточной аттестации - экзамен, зачет с оценкой.

Б1.О.04 Безопасность жизнедеятельности

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

- УК-8.1. Идентифицирует и анализирует опасные и вредные факторы элементов среды обитания и в рамках осуществляемой деятельности; знает основные вопросы безопасности жизнедеятельности.
- УК-8.2. Способен осуществлять действия по предотвращению возникновения чрезвычайных ситуаций природного, техногенного, социального (биолого-социального) происхождения; грамотно действовать в чрезвычайных ситуациях мирного и военного времени, создавать безопасные условия реализации профессиональной деятельности.
- УК-8.3. Готов принимать участие в оказании первой и экстренной допсихологической помощи при травмах и неотложных состояниях, в том числе в условиях чрезвычайных ситуаций в мирное и военное время.
- УК-8.4. Способен обеспечить безопасные и/или комфортные условия труда на рабочем месте, в том числе с помощью средств защиты; выявить и устранить проблемы, связанные с нарушениями техники безопасности на рабочем месте.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- приобретение знаний и умений, необходимых для сохранения своей жизни и здоровья, для обеспечения безопасности человека в современных экономических и социальных условиях;
- обучение студентов идентификации опасностей в современной техносфере;
- приобретение знаний в области защиты населения и территорий в чрезвычайных ситуациях как в мирное, так и в военное время,
- выбор соответствующих способов защиты в условиях различных ЧС;

Задачи учебной дисциплины:

- изучение основ культуры безопасности;
- формирование умения соблюдать нормативные требования по отношению к источникам опасностей, присутствующих в окружающей среде;
- сформировать навыки распознавания опасностей;

-освоить приемы оказания первой помощи;

- выработать алгоритм действий в условиях различных ЧС;

- психологическая готовность эффективного взаимодействия в условиях ЧС.

Форма(ы) промежуточной аттестации - зачет.

Б1.О.05 Физическая культура и спорт

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

– УК-7.1. Выбирает здоровьесберегающие технологии для поддержания здорового образа жизни с учетом физиологических особенностей организма.

– УК-7.2. Планирует свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности.

– УК-7.3. Соблюдает и пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- формирование физической культуры личности;

- приобретение способности целенаправленного использования средств физической культуры и спорта для сохранения и укрепления здоровья для обеспечения полноценной социальной и профессиональной деятельности.

Задачи учебной дисциплины:

- овладение знаниями теоретических и практических основ физической культуры и спорта и здорового образа жизни;

- формирование мотивационно-ценностного отношения к физической культуре, установки на здоровый стиль жизни, потребности в регулярных занятиях физическими упражнениями и в двигательной активности.

Форма(ы) промежуточной аттестации – зачет.

Б1.О.06 Коммуникативные технологии профессионального общения

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия.

− УК-4.2. Владеет культурой письменного и устного оформления профессионально ориентированного научного текста на государственном языке РФ.
− УК-4.3. Умеет вести устные деловые переговоры в процессе профессионального взаимодействия на государственном языке РФ.
− УК-4.4. Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ.
− УК-4.6. Выбирает на государственном языке коммуникативно приемлемые стратегии академического и профессионального общения.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины
Целями освоения учебной дисциплины являются:
изучение дисциплины является получение филологических знаний, необходимых для успешной профессиональной деятельности..

Задачи учебной дисциплины:
− применять методологию гуманитарной науки для решения профессиональных проблем;
− корректировать собственную профессиональную деятельность с учетом ориентиров и ограничений, налагаемых современной культурой;
− своить нормы русского литературного языка применительно к профессиональной деятельности;
− владеть коммуникативными технологиями профессиональной деятельности.

Форма(ы) промежуточной аттестации - зачет

Б1.О.07 Современные теории и технологии развития личности

Общая трудоемкость дисциплины 2 з.е.
Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

− УК-3.1. Вырабатывает конструктивные стратегии и на их основе формирует команду, распределяет в ней роли для достижения поставленной цели.
− УК-3.2. Планирует и корректирует работу команды с учетом интересов, особенностей поведения и мнений ее членов, распределяет поручения и делегирует полномочия членам команды для достижения поставленной цели.

– УК-3.3. Разрешает конфликты и противоречия при деловом общении в команде на основе учета интересов всех сторон.

УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни.

– УК-6.1. Оценивает свои личностные ресурсы, оптимально их использует для успешного выполнения порученного задания.

– УК-6.2. Самостоятельно выявляет мотивы и стимулы для саморазвития, определяет реалистичные цели и приоритеты профессионального роста, способы совершенствования собственной деятельности на основе самооценки по выбранным критериям.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- усвоение обучающимися системы знаний об современных теориях личности и технологиях ее развития как области психологической науки, о прикладном характере этих знаний в области их будущей профессиональной деятельности;
- формирование у студентов умений, навыков и компетенций, направленных на развитие и саморазвитие личности профессионала;
- укрепление у обучающихся интереса к глубокому и детальному изучению современных теорий личности и технологий ее развития, практическому применению полученных знаний, умений и навыков в целях собственного развития, профессиональной самореализации и самосовершенствования.

Задачи учебной дисциплины:

- проследить становление и развитие понятий «культура» и «цивилизация»;
- рассмотреть взгляды общества на место и роль культуры в социальном процессе;
- дать представление о типологии и классификации культур, внутри- и межкультурных коммуникациях;
- выделить доминирующие в той или иной культуре ценности, значения и смыслы, составляющие ее историко-культурное своеобразие.

Форма(ы) промежуточной аттестации – зачет с оценкой.

Б1.О.08 Правовые и организационные основы противодействия коррупции

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-10. Способен формировать нетерпимое отношение к коррупционному поведению.

– УК-10.1. Проявляет готовность добросовестно выполнять профессиональные обязанности на основе принципов законности.

– УК-10.2. Поддерживает высокий уровень личной и правовой культуры, соблюдает антикоррупционные стандарты поведения.

– УК-10.3. Даёт оценку и пресекает коррупционное поведение, выявляет коррупционные риски.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- получение знаний о системе и содержании правовых норм;
- обучение правильному пониманию правовых норм;
- привитие навыков толкования правовых норм.

Задачи учебной дисциплины:

- изучение основ теории права;
- изучение основ правовой системы Российской Федерации;
- анализ теоретических и практических правовых проблем.

Форма(ы) промежуточной аттестации – зачет.

Б1.О.09 Проектный менеджмент

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-2. Способен управлять проектом на всех этапах его жизненного цикла.

– УК-2.1. Формулирует конкретную, специфичную, измеримую во времени и пространстве цель, а также определяет дорожную карту движения к цели, исходя из имеющихся ресурсов и ограничений.

– УК-2.2. Проектирует решение конкретной задачи с учетом возможных ограничений действующих правовых норм. Составляет иерархическую структуру работ, распределяет по задачам финансовые и трудовые ресурсы, использует актуальное ПО.

– УК-2.3. Проектирует смету и бюджет проекта, оценивает эффективность результатов проекта

– УК-2.4. Составляет матрицу ответственности и матрицу коммуникаций проекта.

– УК-2.5. Использует гибкие технологии для реализации задач с изменяющимися во времени параметрами.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

- получение знаний о функциях и методах управления проектами;
- обучение инструментам управления проектами;

- расширение знаний и компетенций студентов по проблематике социального поведения, лидерства,

саморазвития, управления развитием команды.

Задачи учебной дисциплины:

- изучение основ водопадного и итеративного управления проектами;
- привитие навыков целеполагания, использования гибкого инструментария, оценки эффективности проекта;
- усвоение обучающимися различных инструментов управления проектами: иерархической структуры работ,

матриц ответственности и коммуникации, сметы и бюджета проекта, оценки эффективности проекта.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.10 Экономика и финансовая грамотность

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности.

- УК-9.1. Понимает базовые принципы функционирования экономики.
- УК-9.2. Понимает основные виды государственной социально-экономической политики и их влияние на индивида.
- УК-9.3. Использует финансовые инструменты для управления личными финансами (личным бюджетом).
- УК-9.4. Применяет методы личного экономического и финансового планирования для достижения поставленных целей.
- УК-9.5. Контролирует собственные экономические и финансовые риски.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- формирование у студентов базовых экономических знаний, умений и навыков, необходимых для анализа сложных экономических процессов, протекающих в современной рыночной экономике.

Задачи учебной дисциплины:

- ознакомление обучающихся с общими основами экономического развития, закономерностями функционирования рыночной экономики, методиками расчета экономических показателей, рассматриваемых в рамках курса,
- выработка навыков микроэкономического и макроэкономического анализа, способности работать с данными, необходимыми для расчета экономических и социально-экономических показателей,

- формирование умений использовать приобретённые теоретические знания в конкретной практической деятельности, принимая оптимальные организационно-управленческие решения.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.11 Введение в специальность

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

− ОПК-1.1. Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

− ОПК-5.2. Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Введение в специальность» является знакомство с положением, которое занимает специальность "Компьютерная безопасность" в общей системе высшего образования в РФ, с основными проблемами, стоящими в настоящее время в области информационной безопасности, с основными подходами к решению этих проблем, с особой ролью криптографических и математических методов в решении этих проблем. Дисциплина «Введение в специальность» базируется на знаниях, полученных в школе.

Форма(ы) промежуточной аттестации - зачет.

Б1.О.12 Основы российской государственности

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия.

− УК-5.3 Ориентируется в основных этапах развития истории и культуры России и ее достижениях, учитывает особенности российской цивилизации при взаимодействии с представителями различных культур, оценивая потенциальные вызовы и риски

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

овладение знаниями основных событий, происходящих в России и мире, приобретение навыков исторического анализа и синтеза.

Задачи учебной дисциплины: формирование у студентов системы знаний об основных этапах развития истории и культуры России и ее достижениях, понимание особенности российской цивилизации при взаимодействии с представителями различных культур, формирование способности оценивать потенциальные вызовы и риски.

Форма(ы) промежуточной аттестации - зачет.

Б1.О.13 Механика и оптика

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

- ОПК-4.1. Знает основные законы механики и оптики.
- ОПК-4.4. Знает основы теории колебаний и волн, оптики.
- ОПК-4.6. Умеет использовать математические модели физических явлений и процессов.
- ОПК-4.7. Умеет решать типовые прикладные физические задачи.
- ОПК-4.8. Владеет методами исследования физических явлений и процессов.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

изучение фундаментальных понятий и моделей механики и оптики, получение представлений о подходах к постановке и решению конкретных, с учётом особенностей специализации, физических и инженерных задач.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.14 Электричество и магнетизм

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

ОПК-4.3. Знает основные законы электричества и магнетизма.

ОПК-4.4. Знает основы теории колебаний и волн, оптики.

ОПК-4.6. Умеет использовать математические модели физических явлений и процессов.

ОПК-4.7. Умеет решать типовые прикладные физические задачи.

ОПК-4.8. Владеет методами исследования физических явлений и процессов.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

ознакомить студентов с основными положениями классической электродинамики и с приложениями этой теории, научить их использовать аппарат электродинамики для решения конкретных задач.

Главное внимание уделяется формулировке основных понятий и закономерностей поведения электромагнитного поля в вакууме и веществе. При изложении курса используются сведения из таких дисциплин, как «Векторный и тензорный анализ», «Математический анализ», «Теоретическая механика», «Методы математической физики». По завершению курса лекций студенты должны знать: систему уравнений электромагнитного поля Максвелла в вакууме, уравнения макроскопической электродинамики, законы сохранения, теорию распространения и излучения электромагнитных волн, основные представления электродинамики сплошных сред, уметь использовать эти знания при решении практических задач.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.15 Термодинамика

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

- ОПК-4.2. Знает основные законы термодинамики и молекулярной физики.
- ОПК-4.6. Умеет использовать математические модели физических явлений и процессов.
- ОПК-4.7. Умеет решать типовые прикладные физические задачи.
- ОПК-4.8. Владеет методами исследования физических явлений и процессов.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

систематическое изучение основных положений статистической физики и термодинамики.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.16 Квантовая теория

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

- ОПК-4.5. Знает основы квантовой физики.
- ОПК-4.6. Умеет использовать математические модели физических явлений и процессов.
- ОПК-4.7. Умеет решать типовые прикладные физические задачи.
- ОПК-4.8. Владеет методами исследования физических явлений и процессов.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью курса является ознакомление студентов с основными понятиями квантовой теории и ее математическим аппаратом. В результате изучения курса студенты научатся пользоваться понятиями и аппаратом теории для исследования квантовых информационных систем, а также для решения простейших задач квантовой теории информации.

Форма(ы) промежуточной аттестации - экзамен**.**

Б1.О.17 Электроника и схемотехника

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-4.9; ОПК-4.10; ОПК-4.11; ОПК-4.12; ОПК-4.13; ОПК-4.14; ОПК-4.15; ОПК-4.17

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

- ОПК-4.9. Знает принципы работы элементов и функциональных узлов электронной аппаратуры.
- ОПК-4.10. Знает методы анализа и синтеза электронных схем.

– ОПК-4.11. Знает типовые схемотехнические решения основных узлов и блоков электронной аппаратуры.

– ОПК-4.12. Умеет работать с современной элементной базой электронной аппаратуры.

– ОПК-4.13. Умеет использовать стандартные методы и средства проектирования цифровых узлов и устройств.

– ОПК-4.14. Владеет навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры.

– ОПК-4.15. Владеет навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации.

– ОПК-4.17. Умеет анализировать и синтезировать электронные схемы.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

изучение основных понятий и законов теории электрических цепей. Методы анализа линейных и нелинейных цепей в переходном и установившемся режимах, принцип действия и характеристики компонентов и узлов электронной аппаратуры, методы их расчета. Особенности аналоговой, силовой и цифровой электроники. Приобретение компетенций, необходимых для изучения специальных дисциплин, таких как электронные приборы и узлы ЭВМ, архитектура ЭВМ, телекоммуникационные технологии, методы и устройства передачи и обработки информации.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.18 Математический анализ

Общая трудоемкость дисциплины 9 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

- ОПК-3.38 знает основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных;
- ОПК-3.39 знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных;
- ОПК-3.40 знает основные методы интегрального исчисления функций одной и нескольких действительных переменных;
- ОПК-3.41 знает основные методы исследования числовых и функциональных рядов;
- ОПК-3.42 знает основные задачи теории функций комплексного переменного;
- ОПК-3.44 умеет обосновывать основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных;
- ОПК-3.45 умеет обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных переменных;

- ОПК-3.46 умеет обосновывать основные методы интегрального исчисления функций одной и нескольких действительных переменных;
- ОПК-3.47 умеет обосновывать основные методы исследования числовых и функциональных рядов;
- ОПК-3.48 владеет навыками использования справочных материалов по математическому анализу.

Цели и задачи учебной дисциплины:
Целью освоения дисциплины математического анализа является:

изучение основных математических понятий, их взаимосвязи и развития, а также отвечающих им математических методов, используемых для решения задач профессиональной деятельности.

Задачи учебной дисциплины:

- развитие алгоритмического и логического мышления студентов,
- выработка у студентов умения самостоятельно расширять свои математические знания,
- проводить математический анализ прикладных задач с использованием методов вычисления пределов и исследования непрерывности, отыскания производных функций, вычисления интегралов, нахождения сумм рядов.

Место учебной дисциплины в структуре ООП: Дисциплина «Математический анализ» (Б1.О.18) относится к обязательной части блока 1 «Дисциплины (модули)» учебного плана и изучается в 1 и 2 семестрах.

Краткое содержание (дидактические единицы) учебной дисциплины:

Множества. Метод математической индукции. Вещественные числа. Числовые множества. Числовые последовательности. Функции и их пределы. Непрерывность функции. Производная и дифференциал функции. Формула Тейлора. Применение дифференциального исчисления к исследованию функций. Первообразная функции и неопределенный интеграл. Определенный интеграл Римана. Несобственные интегралы. Числовые ряды. Степенные ряды. N-мерное евклидово пространство. Функции нескольких действительных переменных. Экстремум функции n переменных. Кратные интегралы. Криволинейные интегралы. Ряды Фурье.

Формы текущей аттестации (семестр): 2 контрольные работы (1 семестр); 2 контрольные работы (2 семестр);
Форма промежуточной аттестации: экзамен в 1 семестре, экзамен во 2 семестре

Б1.О.19 Геометрия

Общая трудоёмкость дисциплины: 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

ОПК-3.1 знает основные задачи векторной алгебры и аналитической геометрии;

ОПК-3.2 знает возможности координатного метода для исследования различных геометрических объектов;

ОПК-3.3 знает основные виды уравнений простейших геометрических объектов;

ОПК-3.5 умеет решать основные задачи аналитической геометрии на плоскости и в пространстве;

ОПК-3.6 владеет навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Форма промежуточной аттестации: зачет с оценкой.

Б1.О.20 Теория вероятностей и математическая статистика

Общая трудоемкость дисциплины 8 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

− ОПК-3.49. Знает основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства.

− ОПК-3.50. Знает классические предельные теоремы теории вероятностей.

− ОПК-3.51. Знает основные понятия теории случайных процессов.

− ОПК-3.52. Знает постановку задач и основные понятия математической статистики.

− ОПК-3.53. Знает стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений.

− ОПК-3.54. Знает стандартные методы проверки статистических гипотез.

− ОПК-3.55. Умеет обосновывать классические положения и стандартные методы теории вероятностей и случайных процессов.

− ОПК-3.56. Умеет обосновывать классические положения и стандартные методы математической статистики.

− ОПК-3.57. Умеет разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Теория вероятностей и математическая статистика» является овладение математическим аппаратом, используемым для описания массовых случайных явлений, и методами обработки статистических данных, необходимыми для построения вероятностных моделей; приобретение навыков решения задач математической статистики как аналитически, так и с помощью вычислительной техники.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.21 Алгебра

Общая трудоёмкость дисциплины: 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. *Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.*

– ОПК-3.7. Знает основные свойства важнейших алгебраических систем: групп, колец, полей;

– ОПК-3.8. Знает основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями;

– ОПК-3.9. Знает основные свойства колец многочленов над кольцами и полями;

– ОПК-3.10. Знает основные свойства отображений важнейших алгебраических систем;

– ОПК-3.11. Умеет производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ;

– ОПК-3.12. Умеет решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду;

– ОПК-3.13. Умеет производить оценку качества полученных решений прикладных задач;

– ОПК-3.14. Владеет методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах;

– ОПК-3.15. Владеет навыками решения типовых линейных уравнений над полем и кольцом вычетов;

– ОПК-3.16. Владеет навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований.

Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к обязательной части Блока 1.

Цели и задачи учебной дисциплины:

Цель изучения дисциплины: получение знаний об основных алгебраических структурах, освоение круга задач классической и современной алгебры, получение фундаментальных знаний, необходимых для последующего изучения смежных математических дисциплин.

Задачи учебной дисциплины: приобретение навыков работы с основными алгебраическими объектами: группами, кольцами, полями, комплексными числами, различными типами матриц и их числовыми характеристиками, полиномами, системами линейных алгебраических уравнений, матричными уравнениями.

Форма промежуточной аттестации – экзамен.

Б1.О.22 Аппаратные средства вычислительной техники

Общая трудоёмкость дисциплины: 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-2.1; ОПК-2.2; ОПК-2.3; ОПК-2.4; ОПК-4.16; ОПК-4.17; ОПК-4.18; ОПК-4.19; ОПК-15.1

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

− ОПК-2.1. Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере.

− ОПК-2.2. Знает логико-математические основы построения электронных цифровых устройств.

− ОПК-2.3. Знает состав, назначение аппаратных средств и программного обеспечения персонального компьютера.

− ОПК-2.4. Знает классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей.

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

− ОПК-4.16. Знает структуру и принципы работы современных и перспективных микропроцессоров.

− ОПК-4.17. Умеет анализировать и синтезировать электронные схемы.

− ОПК-4.18. Умеет определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств.

− ОПК-4.19. Владеет навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.

ОПК-15. Способен администрировать компьютерные сети и контролировать корректность их функционирования.

− ОПК-15.1. Знает архитектуру основных типов современных компьютерных систем.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Аппаратные средства вычислительной техники» является приобретение студентами знаний о принципах построения современных компьютеров, комплексов; основ организации информационных систем, ЭВМ, подсистем ЭВМ, их взаимодействия между собой.

Форма(ы) промежуточной аттестации - зачет.

Б1.О.23 Линейная алгебра

Общая трудоёмкость дисциплины: 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения: ОПК-3.4; ОПК-3.7; ОПК-3.8; ОПК-3.9; ОПК-3.10; ОПК-3.11; ОПК-3.12; ОПК-3.13; ОПК-3.14; ОПК-3.15; ОПК-3.16

ОПК-3. *Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.*

− ОПК 3.4 умеет решать основные задачи линейной алгебры;

− ОПК-3.7. Знает основные свойства важнейших алгебраических систем: групп, колец, полей;

− ОПК-3.8. Знает основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями;

− ОПК-3.9. Знает основные свойства колец многочленов над кольцами и полями;

− ОПК-3.10. Знает основные свойства отображений важнейших алгебраических систем;

− ОПК-3.11. Умеет производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ;

– ОПК-3.12. Умеет решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду;

– ОПК-3.13. Умеет производить оценку качества полученных решений прикладных задач;

– ОПК-3.14. Владеет методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах;

– ОПК-3.15. Владеет навыками решения типовых линейных уравнений над полем и кольцом вычетов;

– ОПК-3.16. Владеет навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований.

Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к обязательной части Блока 1.

Форма промежуточной аттестации – экзамен.

Б1.О.24 Математическая логика и теория алгоритмов

Общая трудоёмкость дисциплины: 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. *Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.*

– ОПК-3.17. Знает основные понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности;

– ОПК-3.18. Знает язык и средства современной математической логики и теории логических исчислений;

– ОПК-3.19. Знает основные способы задания булевых функций и функций многозначной логики формулами и их свойства;

– ОПК-3.20. Знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов;

– ОПК-3.21. Умеет производить основные логические операции в исчислении высказываний и исчислении предикатов;

– ОПК-3.22. Умеет находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах;

– ОПК-3.23. Умеет оценивать сложность алгоритмов и вычислений;

– ОПК-3.24. Умеет применять методы математической логики и теории алгоритмов к решению задач математической кибернетики;

– ОПК-3.25. Владеет навыками использования языка современной символической логики ;

– ОПК-3.26. Владеет навыками упрощения формул алгебры высказываний и алгебры предикатов;

– ОПК-3.27. Владеет навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.

Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к обязательной части Блока 1.

Цели и задачи учебной дисциплины:

Цель изучения дисциплины: ознакомление с основными понятиями и методами математической логики и теории алгоритмов с ориентацией на их использование в практической деятельности.

Задачи учебной дисциплины: знать основные понятия и методы математической логики и теории алгоритмов; уметь использовать знания для построения несложных логических моделей предметных областей, реализации логического вывода и оценки вычислительной сложности алгоритмов; иметь представление о направлениях развития данной дисциплины и перспективах ее использования в области обеспечения защиты данных и информационной безопасности.

Форма промежуточной аттестации – зачет.

Б1.О.25 Дискретная математика

Общая трудоемкость дисциплины 8 з. е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

–ОПК-3.28 - знает свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур;

–ОПК-3.29 - знает основные понятия и методы теории графов;

–ОПК-3.30 - знает основные понятия и методы теории конечных автоматов;

–ОПК-3.31 - знает основные понятия и методы комбинаторного анализа;

–ОПК-3.32 - умеет решать задачи периодичности и эквивалентности для линейных рекуррентных последовательностей и конечных автоматов;

–ОПК-3.33 - умеет применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач

–ОПК-3.34 - умеет решать оптимизационные задачи на графах;

–ОПК-3.35 - умеет применять стандартные методы дискретной математики для решения профессиональных задач;

–ОПК-3.36 - владеет навыками решения типовых комбинаторных и теоретико-графовых задач;

–ОПК-3.37 - владеет навыками применения языка и средств дискретной математики при решении профессиональных задач.

Место учебной дисциплины в структуре ОПОП: дисциплина Дискретная математика относится к обязательной части блока Б1.

Цели и задачи учебной дисциплины

Цели изучения дисциплины:

Цель изучения дисциплины: изучение и практическое освоение основных разделов дискретной математики – дисциплины, которая является базовой для формирования математической культуры современного специалиста в области моделирования и информационных технологий.

Основными задачами учебной дисциплины являются:

- формирование терминологической базы, а также представления об алгоритмических основах дискретной математики;
- ознакомление с важнейшими разделами дискретной математики и ее применением для представления информации и решения задач теоретической информатики;

- ознакомление студентов с методами дискретной математики, которые используются для построения моделей и конструирования алгоритмов некоторых классов практических задач.

Форма промежуточной аттестации – экзамен.

Б1.О.26 Дифференциальные уравнения

Общая трудоёмкость дисциплины: 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. *Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.*

– ОПК-3.43. Знает основные типы обыкновенных дифференциальных уравнений и методы их решения;

– ОПК-3.58. Владеет навыками решения основных типов обыкновенных дифференциальных уравнений.

Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к обязательной части Блока 1.

Цели и задачи учебной дисциплины:

Цель изучения дисциплины: сформировать у студентов современные теоретические знания в области обыкновенных дифференциальных уравнений и практические навыки в решении и исследовании основных типов обыкновенных дифференциальных уравнений, познакомить студентов с начальными навыками математического моделирования.

Задачи учебной дисциплины: обучение студентов применению на практике методов построения математических моделей в виде дифференциальных уравнений; освоение основных методов решения дифференциальных уравнений; обучение основным положениям теории: устойчивость, существование решений, качественные свойства решений.

Форма промежуточной аттестации – зачет с оценкой.

Б1.О.27 Методы вычислений

Общая трудоёмкость дисциплины: 5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3. *Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.*

– ОПК-3.11. Умеет производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ;

– ОПК-3.13. Умеет производить оценку качества полученных решений прикладных задач;

– ОПК-3.20 знает различные подходы к определению понятия алгоритма, методы доказа-тельства алгоритмической неразрешимости и методы построения эффективных алгоритмов

Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к обязательной части Блока 1.

Форма промежуточной аттестации – зачет.

Б1.О.28 Методы оптимизации

Общая трудоёмкость дисциплины: 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-7. *Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.*

– ОПК-7.12. Знает необходимые и достаточные условия оптимальности задачи математического программирования;

– ОПК-7.13. Умеет применять методы одномерной оптимизации при решении прикладных задач;

– ОПК-7.14. Умеет использовать методы многомерной безусловной оптимизации при решении профессиональных задач;

– ОПК-7.15. Знает методы условной оптимизации при решении прикладных задач;

– ОПК-7.16. Знает задачи вариационного исчисления, оптимального управления и линейного программирования.

Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к обязательной части Блока 1.

Цели и задачи учебной дисциплины:

Цель изучения дисциплины: изучение основ теории экстремальных задач, получение необходимых концептуальных представлений, достаточных для понимания, оценки существующих алгоритмов решения оптимизационных задач и, если необходимо, разработки новых методов и подходов решения новых типов таких задач.

Задачи учебной дисциплины: дать студентам общее представление о прикладных задачах оптимизации; ознакомить с основными теоретическими фактами; изучить основные классы методов; обучить использованию методов решения прикладных задач оптимизации.

Форма промежуточной аттестации – зачет с оценкой.

Б1.О.29 Теория информации

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

− ОПК-10.21. Знает фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации.

– ОПК-10.22. Знает основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума.

– ОПК-10.23. Знает основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга).

– ОПК-10.24. Знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования.

– ОПК-10.25. Умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность).

– ОПК-10.26. Умеет решать типовые задачи кодирования и декодирования.

– ОПК-10.27. Владеет основами построения математических моделей текстовой информации и моделей систем передачи информации.

– ОПК-10.28. Владеет навыками применения математического аппарата для решения прикладных теоретико-информационных задач.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

дисциплина ориентирована на формирование у студентов основополагающих представлений об использовании количественной меры информации для характеристики источников и каналов передачи информации, а также их потенциальных характеристик; задачи дисциплины - сформировать представление о современном состоянии теории информации, представить фундаментальные положения теории информации, различные аспекты количественной меры информации источников с дискретным и непрерывным множеством состояний, информационные характеристики источников информации и каналов связи, рассмотреть вопросы оценки пропускной способности канала связи без шума и с шумом, методы кодирования информации.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.30 Технологии обработки информации

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;.

– ОПК-8.12. Знает современные методы обработки информации и машинного обучения.

– ОПК-8.13. Умеет применять методы машинного обучения при проведении разработок в области обеспечения безопасности компьютерных систем.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение теоретических основ и овладение практическими навыками применения методов и средств обработки информации в интересах сопровождения и проектирования информационных, информационно-измерительных и управляющих систем различного назначения; получение профессиональных компетенций в области современных технологий обработки информации.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных технологий обработки информации;
- обучение студентов базовым методам машинного обучения и алгоритмам обработки информации в рамках структурно-статистического, структурно-геометрического, нейросетевого подходов;
- овладение практическими навыками разработки алгоритмов обработки информации с использованием современных программных средств и технологий;
- раскрытие принципов построения и эксплуатации информационных, информационно-измерительных и управляющих систем с точки зрения решения базовых задач обработки информации.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.31 Информатика

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

- ОПК-2.1. Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере.
- ОПК-2.5. Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет.
- ОПК-2.6. Умеет составлять документы, используя прикладные программы офисного назначения.
- ОПК-2.7. Владеет средствами управления пользовательскими интерфейсами операционных систем.

ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

- ОПК-3.20. Знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов.

ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

− ОПК-10.21. Знает фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации.

− ОПК-10.22. Знает основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума.

− ОПК-10.23. Знает основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга).

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

введение студентов первого курса в круг основных фактов, концепций, принципов и теоретических проблем, а также практических задач и приложений, основных методов и технологий, относящихся к сфере информатики.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.32 Операционные системы

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности

ОПК-2.7 Владеет средствами управления пользовательскими интерфейсами операционных систем.

ОПК-2.8 знает основные принципы конфигурирования и администрирования операци-онных систем

ОПК-2.9 умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями;;

ОПК-2.10 умеет применять основные методы программирования в выбранной операционной среде;

ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;

ОПК-12.1 знает принципы построения современных операционных систем и особенности их применения;

ОПК-12.2 знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей.;

ОПК-12.3 знает основные принципы конфигурирования и администрирования операционных систем;

ОПК-12.4 владеет навыками системного программирования;

ОПК-12.5 Умеет осуществлять администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отечественного производства.;

ОПК-12.6 Знает методы восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.33 Сети и системы передачи информации

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

- ОПК-9.5. Знает основные характеристики сигналов электросвязи, спектры и виды модуляции.
- ОПК-9.6. Знает принципы построения и функционирования систем и сетей передачи информации.
- способы передачи и распределения информации в телекоммуникационных системах и сетях.
- ОПК-9.7. Знает основные телекоммуникационные протоколы.
- ОПК-9.8. Умеет анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

формирование у студентов основополагающих представлений о принципах построения и алгоритмах функционирования систем и сетей передачи информации; моделировании и анализе процессов передачи информации в сетях и системах связи; задачи дисциплины - сформировать представление о современном состоянии систем и сетей передачи информации, основных принципах работы их элементов.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.34 Компьютерные сети

Общая трудоёмкость дисциплины: 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-15. Способен администрировать компьютерные сети и контролировать корректность их функционирования;

–ОПК-15.1 знает архитектуру основных типов современных компьютерных систем;

–ОПК-15.2 знает основы организации и построения компьютерных сетей;

–ОПК-15.3 знает эталонную модель взаимодействия открытых систем;

–ОПК-15.4 знает функции, принципы действия и алгоритмы работы сетевого оборудования;

–ОПК-15.5 умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах;

–ОПК-15.6 умеет осуществлять проектирование и оптимизацию функционирования компьютерных сетей;

–ОПК-15.7 владеет навыками администрирования компьютерных сетей;

–ОПК-15.8 владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением;

Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к обязательной части Блока 1.

Цели и задачи учебной дисциплины:

Цель изучения дисциплины: получение студентами фундаментальных знаний по основам аппаратного и программного обеспечения компьютерных сетей и базовых сетевых протоколов, а также практических навыков по разработке и администрированию сетей.

Задачи учебной дисциплины: ознакомить студентов с принципами построения сетей передачи данных, сетевыми моделями и протоколами, работой основных сетевых приложений и протоколов прикладного уровня, алгоритмами передачи данных, маршрутизации, и протоколами, реализующие эти алгоритмы.

Форма промежуточной аттестации – экзамен.

Б1.О.35 Объектно-ориентированное программирование

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

− ОПК-2.9. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями.

− ОПК-2.10. Умеет применять основные методы программирования в выбранной операционной среде.

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

– ОПК-7.1. Знает общие принципы построения, области и особенности применения языков программирования высокого уровня.

– ОПК-7.2. Знает язык программирования высокого уровня (объектно-ориентированное программирование).

– ОПК-7.3. Знает язык ассемблера персонального компьютера.

– ОПК-7.4. Умеет работать с интегрированной средой разработки программного обеспечения.

– ОПК-7.5. Умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач.

– ОПК-7.6. Владеет навыками разработки, документирования, тестирования и отладки программ.

– ОПК-7.7. Знает базовые структуры данных.

– ОПК-7.8. Знает основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы.

– ОПК-7.9. Знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения.

– ОПК-7.10. Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.

– ОПК-7.11. Владеет навыками разработки алгоритмов решения типовых профессиональных задач.

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

– ОПК-13.4. Знает язык программирования высокого уровня (объектно-ориентированное программирование).

– ОПК-13.7. Владеет навыками использования инструментальных средств отладки и дизассемблирования программного кода.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

изучение современных объектно-ориентированных подходов и технологий в разработки ПО (обобщенное программирование, паттерны проектирования, компонентная разработка); углубленное изучение языка C# и знакомство с библиотекой .NET FCL; формирование практических навыков объектно-ориентированного программирования и проектирования ПО.

Форма(ы) промежуточной аттестации – экзамен.

Б1.О.36 Введение в программирование

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

– ОПК-2.9. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями.

– ОПК-2.10. Умеет применять основные методы программирования в выбранной операционной среде.

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

– ОПК-7.1. Знает общие принципы построения, области и особенности применения языков программирования высокого уровня.

– ОПК-7.2. Знает язык программирования высокого уровня (объектно-ориентированное программирование).

– ОПК-7.3. Знает язык ассемблера персонального компьютера.

– ОПК-7.4. Умеет работать с интегрированной средой разработки программного обеспечения.

– ОПК-7.5. Умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач.

– ОПК-7.6. Владеет навыками разработки, документирования, тестирования и отладки программ.

– ОПК-7.7. Знает базовые структуры данных.

– ОПК-7.8. Знает основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы.

– ОПК-7.9. Знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения.

– ОПК-7.10. Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.

– ОПК-7.11. Владеет навыками разработки алгоритмов решения типовых профессиональных задач.

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

– ОПК-13.3. Знает общие принципы построения и использования современных языков программирования высокого уровня.

– ОПК-13.5. Умеет работать с интегрированными средами разработки программного обеспечения.

– ОПК-13.7. Владеет навыками использования инструментальных средств отладки и дизассемблирования программного кода.

– ОПК-13.8. Знает современные технологии программирования.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

формирование теоретических и практических навыков в области создания надежного и качественного программного обеспечения с применением современных технологий программирования, методов и средств коллективной разработки.

Задачи учебной дисциплины:

– освоение теоретических основ и современных технологий анализа, проектирования и разработки программного обеспечения;

– овладение практическими навыками проектирования и разработки различных видов программного обеспечения на основе объектно-ориентированного подхода;

– приобретение опыта разработки программных средств средней сложности;

– знакомство с библиотеками классов и инструментальными средствами, используемыми при разработке программного обеспечения.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.37 Методы программирования

Общая трудоемкость дисциплины 6 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

− ОПК-2.9. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями.

− ОПК-2.10. Умеет применять основные методы программирования в выбранной операционной среде.

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

− ОПК-7.1. Знает общие принципы построения, области и особенности применения языков программирования высокого уровня.

− ОПК-7.3. Знает язык ассемблера персонального компьютера.

− ОПК-7.4. Умеет работать с интегрированной средой разработки программного обеспечения.

− ОПК-7.5. Умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач.

– ОПК-7.6. Владеет навыками разработки, документирования, тестирования и отладки программ.

– ОПК-7.7. Знает базовые структуры данных.

– ОПК-7.8. Знает основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы.

– ОПК-7.9. Знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения.

– ОПК-7.10. Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.

– ОПК-7.11. Владеет навыками разработки алгоритмов решения типовых профессиональных задач.

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

– ОПК-13.3. Знает общие принципы построения и использования современных языков программирования высокого уровня.

– ОПК-13.4. Знает язык программирования высокого уровня (объектно-ориентированное программирование).

– ОПК-13.5. Умеет работать с интегрированными средами разработки программного обеспечения.

– ОПК-13.6. Владеет навыками разработки, отладки, документирования и тестирования программ.

– ОПК-13.7. Владеет навыками использования инструментальных средств отладки и дизассемблирования программного кода.

– ОПК-13.8. Знает современные технологии программирования.

– ОПК-13.9. Знает показатели качества программного обеспечения.

– ОПК-13.10. Знает базовые структуры данных.

– ОПК-13.11. Знает основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности.

– ОПК-13.12. Умеет формализовать поставленную задачу.

– ОПК-13.13. Умеет разрабатывать эффективные алгоритмы и программы.

– ОПК-13.14. Умеет проводить оценку вычислительной сложности алгоритма.

– ОПК-13.15. Умеет планировать разработку сложного программного обеспечения.

– ОПК-13.16. Владеет методами оценки качества готового программного обеспечения.

– ОПК-13.17. Владеет навыками разработки алгоритмов для решения типовых профессиональных задач.

–

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

формирование теоретических и практических навыков в области создания надежного и качественного программного обеспечения с применением современных технологий программирования, методов и средств коллективной разработки.

Задачи учебной дисциплины:

– освоение теоретических основ и современных технологий анализа, проектирования и разработки программного обеспечения;

– овладение практическими навыками проектирования и разработки различных видов программного обеспечения на основе объектно-ориентированного подхода;

– приобретение опыта разработки программных средств средней сложности;

– знакомство с библиотеками классов и инструментальными средствами, используемыми при разработке программного обеспечения.

Форма(ы) промежуточной аттестации - зачет с оценкой, экзамен.

Б1.О.38 Системы управления базами данных

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-14.1; ОПК-14.2; ОПК-14.3; ОПК-14.4; ОПК-14.5; ОПК-14.6; ОПК-14.9; ОПК-14.10; ОПК-14.11; ОПК-14.14

ОПК-14Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации;

ОПК-14.1. Знает характеристики и типы систем баз данных.

ОПК-14.2. Знает основные языки запросов.

ОПК-14.3. Знает физическую организацию баз данных и принципы (основы) их защиты.

ОПК-14.4. Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных.

ОПК-14.5. Умеет настраивать и применять современные системы управления базами данных.

ОПК-14.6. Владеет методикой и навыками составления запросов для поиска информации в базах данных.

ОПК-14.9. Знает особенности применения криптографической защиты в СУБД.

ОПК-14.10. Знает этапы проектирования системы защиты в СУБД.

ОПК-14.11. Умеет пользоваться средствами защиты, предоставляемыми СУБД.

ОПК-14.14. Владеет методикой и навыками использования средств защиты, предоставляемых СУБД.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.39 Основы информационной безопасности

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

– ОПК-1.1. Знает основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

– ОПК-1.2. Знает классификацию защищаемой информации по видам тайны и степеням конфиденциальности.

– ОПК-1.3. Знает классификацию и основные угрозы информационной безопасности для объекта информатизации.

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

– ОПК-5.1. Знает источники и классификацию угроз информационной безопасности.

– ОПК-5.2. Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России.

– ОПК-5.3. Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.

– ОПК-5.4. Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение теоретических основ и принципов построения защищенных систем обработки информации, стандартов информационной безопасности, критериев и классов защищенности автоматизированных систем и средств вычислительной техники, формальных моделей безопасности, методов обоснования требований и оценки защищенности систем обработки информации, архитектуры защищенных операционных систем, порядка проведения сертификации защищенных систем обработки информации, вопросов использования инструментальных интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям стандартов информационной безопасности и руководящих документов Гостехкомиссии России (ФСТЭК России) в области защиты от НСД автоматизированных систем и средств вычислительной техники;
- обучение студентов формальным моделям для дискреционной, мандатной и ролевой политик безопасности и их расширений;

- обучение студентов базовым методам обоснования требований и оценки защищенности систем обработки информации;
- овладение практическими навыками использования инструментальных интеллектуальных систем обоснования требований и оценки защищенности систем обработки информации;
- овладение практическими навыками проведения сертификации защищенных систем обработки информации.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.40 Модели безопасности компьютерных систем

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

- ОПК-6.4. Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа.
- ОПК-6.5. Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем.
- ОПК-6.6. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем.
- ОПК-6.8. Умеет определить политику контроля доступа работников к информации ограниченного доступа.
- ОПК-6.10. Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

- ОПК-8.10. Умеет разрабатывать модели безопасности компьютерных систем с использованием необходимого математического аппарата и средств компьютерного моделирования.
- ОПК-8.11. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.

ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

– ОПК-11.1. Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем.

– ОПК-11.2. Знает основные виды политик управления доступом и информационными потоками в компьютерных системах.

– ОПК-11.3. Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков.

– ОПК-11.4. Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.

– ОПК-11.5. Умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.41 Защита в операционных системах

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами

данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

– ОПК-9.11. Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных.

– ОПК-9.12. Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных.

ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

– ОПК-11.6. Знает средства и методы хранения и передачи аутентификационной информации.

– ОПК-11.7. Знает основные требования к подсистеме аудита и политике аудита.

– ОПК-11.8. Знает защитные механизмы и средства обеспечения безопасности операционных систем.

– ОПК-11.9. Умеет формулировать и настраивать политику безопасности основных операционных систем.

– ОПК-11.10. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.

ОПК-12 Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения.

– ОПК-12.2. Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей.

– ОПК-12.4. Владеет навыками системного программирования.

ОПК-13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

– ОПК-13.1. Умеет формулировать и настраивать политику безопасности основных операционных систем.

– ОПК-13.2. Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки

безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.42 Основы построения защищенных компьютерных сетей

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

– ОПК-8.11. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

– ОПК-9.9. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем.

– ОПК-9.11. Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных.

– ОПК-9.12. Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных.

ОПК-11 Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации.

– ОПК-11.10. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.

ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования.

– ОПК-15.7. Владеет навыками администрирования компьютерных сетей.

– ОПК-15.8. Владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением.

ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

– ОПК-16.1. Знает средства и методы хранения и передачи аутентификационной информации в компьютерных системах и сетях.

– ОПК-16.2. Знает механизмы реализации атак в сетях TCP/IP.

– ОПК-16.3. Знает основные протоколы идентификации и аутентификации абонентов сети.

– ОПК-16.4. Знает защитные механизмы и средства обеспечения сетевой безопасности.

– ОПК-16.5. Знает средства и методы предотвращения и обнаружения вторжений.

– ОПК-16.6. Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе.

– ОПК-16.7. Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях.

– ОПК-16.8. Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

– ОПК-16.9. Владеет навыками настройки межсетевых экранов.

– ОПК-16.10. Владеет методиками анализа сетевого трафика.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение принципов и методов оценки безопасности компьютерных систем на основе комплексного подхода к определению актуальных угроз безопасности в таких системах в рамках обеспечения безопасности информационных систем и технологий в целом, изучение математических основ моделирования процессов оценки безопасности компьютерных систем, получение профессиональных компетенций в области современных технологий оценки безопасности компьютерных систем.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных методов оценки безопасности компьютерных систем;
- обучение студентов базовым методам оценки безопасности компьютерных систем;
- овладение практическими навыками применения методов оценки безопасности компьютерных систем;
- раскрытие физической сущности построения и эксплуатации компьютерных систем с точки зрения определения актуальных угроз безопасности в таких системах

с целью корректного решения задач по применению методов оценки безопасности компьютерных систем.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.43 Основы построения защищенных баз данных

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

− ОПК-8.11. Владеет способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

− ОПК-9.10. Знает общие и специфические угрозы безопасности баз данных.

− ОПК-9.11. Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных.

− ОПК-9.12. Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных.

ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации.

− ОПК-14.7. Знает основные критерии защищенности баз данных и методы оценивания механизмов защиты.

− ОПК-14.8. Знает механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных.

− ОПК-14.9. Знает особенности применения криптографической защиты в СУБД.

− ОПК-14.10. Знает этапы проектирования системы защиты в СУБД.

− ОПК-14.11. Умеет пользоваться средствами защиты, предоставляемыми СУБД.

− ОПК-14.12. Умеет создавать дополнительные средства защиты баз данных.

− ОПК-14.13. Умеет проводить анализ и оценивание механизмов защиты баз данных.

− ОПК-14.14. Владеет методикой и навыками использования средств защиты, предоставляемых СУБД.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Основы построения защищенных баз данных» является формирование у студентов совокупности профессиональных качеств, обеспечивающих решение проблем, связанных с использованием и проектированием баз данных под управлением современных систем управления базами данных (СУБД), а также связанных с обеспечением безопасности информации в автоматизированных информационных системах (АИС), основу которых составляют базы данных (БД), навыкам работы со встроенными в системы управления базами данных (СУБД) средствами защиты. Задачи дисциплины – обучение принципам работы современных систем управления базами данных, изучение моделей и механизмов защиты в СУБД, приобретение

практических навыков организации защиты БД, обучение проведению обоснования и выбора рационального решения по защите.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.44 Защита программ и данных

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

− ОПК-5.14. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.

− ОПК-5.15. Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации.

− ОПК-5.16. Знает возможности технических средств перехвата информации.

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

− ОПК-7.5. Умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач.

− ОПК-7.6. Владеет навыками разработки, документирования, тестирования и отладки программ.

− ОПК-7.9. Знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения.

− ОПК-7.10. Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

− ОПК-13.18. Умеет применять средства и методы анализа программного обеспечения для выявления закладок.

− ОПК-13.19. Умеет применять методы анализа проектных решений для обеспечения защищенности компьютерных систем.

− ОПК-13.20. Знает программные методы предотвращения несанкционированного доступа к данным.

− ОПК-13.21. Уметь применять современные средства обеспечения информационной безопасности программ и данных.

− ОПК-13.22. Знает основные программные методы защиты данных от несанкционированного доступа.

− ОПК-13.23. Умеет проводить анализ программных средств, применяемых для контроля и защиты информации.

− ОПК-13.24. Умеет проводить аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.

ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

− ОПК-16.11. Знает основные виды деструктивных воздействий на программные продукты.

− ОПК-16.12. Умеет выявлять действие вредоносных программ, и определять характер их воздействия.

− ОПК-16.13. Знает современные методы анализа программных решений по обеспечению защищенности компьютерных систем.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Защита программ и данных» является теоретическая и практическая подготовка специалистов к деятельности, связанной с применением современных технологий анализа программных реализаций, защиты программ и программных систем от анализа и вредоносных программных воздействий.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.45 Методы и средства криптографической защиты информации

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

− ОПК-10.1. Знает основные задачи, решаемые криптографическими методами.

− ОПК-10.2. Знает математические модели шифров, подходы к оценке их стойкости.

− ОПК-10.3. Знает зарубежные и российские криптографические стандарты.

− ОПК-10.4. Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами.

− ОПК-10.5. Умеет применять математические методы при исследовании криптографических алгоритмов.

− ОПК-10.6. Владеет навыками использования типовых криптографических алгоритмов.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Методы и средства криптографической защиты информации» является изложение основополагающих принципов защиты информации с помощью криптографических методов и средств, а также примеров реализации этих методов на практике. Задачи дисциплины - дать основы: системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; принципов разработки шифров; математических методов, используемых в криптографии.

Форма(ы) промежуточной аттестации – зачет с оценкой.

Б1.О.46 Криптографические протоколы

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

− ОПК-10.7. Знает типовые криптопротоколы, используемые в сетях связи.

− ОПК-10.8. Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем.

− ОПК-10.9. Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.

− ОПК-10.10. Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств.

− ОПК-10.11. Владеет подходами к разработке и анализу безопасности криптографических протоколов.

− ОПК-10.20. Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Криптографические протоколы» является теоретическая и практическая подготовка специалистов к деятельности, связанной с анализом и синтезом криптографических протоколов. Задачи освоения дисциплины: изучение основных свойств, характеризующих защищенность криптографических протоколов, и основных механизмов, применяемых для обеспечения выполнения того или иного свойства безопасности протокола; приобретение навыков поиска уязвимостей протоколов.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.47 Теоретико-числовые методы в криптографии

Общая трудоемкость дисциплины 5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

− ОПК-8.1. Знает строение мультипликативной группы колец вычетов.

− ОПК-8.2. Знает способы представления действительных чисел цепными дробями.

− ОПК-8.3. Знает основные свойства символов Лежандра и Якоби.

− ОПК-8.4. Знает критерии простоты и их использование для факторизации натуральных чисел.

− ОПК-8.5. Знает алгоритмы проверки чисел на простоту; построения больших простых чисел.

− ОПК-8.6. Умеет строить большие простые числа.

− ОПК-8.7. Умеет применять алгоритмы проверки чисел на простоту; построения больших простых чисел.

− ОПК-8.8. Умеет применять алгоритмы разложения чисел на множители.

− ОПК-8.9. Владеет навыками применения теории чисел в криптографии и других дисциплинах.

ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

− ОПК-10.12. Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах.

− ОПК-10.13. Знает базовые понятия теории эллиптических кривых.

− ОПК-10.14. Умеет эффективно производить операции с большими числами, а также в кольцах вычетов, кольцах многочленов и конечных полях.

− ОПК-10.15. Умеет исследовать и решать сравнения в кольцах вычетов.

− ОПК-10.16. Умеет использовать достаточные условия простоты для построения больших простых чисел.

− ОПК-10.17. Умеет оценивать теоретическую сложность применяемых алгоритмов.

− ОПК-10.18. Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.

− ОПК-10.19. Владеет методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Теоретико-числовые методы в криптографии» является освоение студентом математического аппарата теории чисел для последующего успешного использования основных методов теории чисел в профессиональной деятельности. Задачами дисциплины являются: развитие у студентов соответствующих общекультурных, профессиональных и профессионально-специализированных компетенций; ознакомление с основами классической и современной теории чисел и численными– алгоритмами, имеющими практические приложения в криптографии; формирование умения строгой оценки эффективности применяемых алгоритмов с – математической точки зрения; формирование четкого осознания необходимости и важности математической подготовки для специалиста по компьютерной безопасности. Цели образовательного процесса достигаются посредством применения инновационных образовательных технологий в обеспечении компетентностного подхода.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.48 Управление ресурсами в системах информационной безопасности

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;

ОПК-5.4 Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;

ОПК-6.3 Знает систему организационных мер, направленных на защиту информации ограниченного доступа.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Основы управленческой деятельности» является ознакомление обучаемых с основными понятиями и методами управленческой деятельности, обеспечить теоретическую и практическую подготовку специалистов к деятельности, связанной с планированием и принятием управленческих решений, организацией выполнения задач, контроля и оценки эффективности действий персонала в процессе обеспечения информационной безопасности в условиях существования угроз в информационной сфере. Задача дисциплины – привить обучаемым навыки использования теории и практики управленческой деятельности в профессиональной деятельности и воспитать у обучаемых высокую культуру мышления.

Форма(ы) промежуточной аттестации - зачет.

Б1.О.49 Организационное и правовое обеспечение информационной безопасности

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

- ОПК-5.3. Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.
- ОПК-5.5. Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации.
- ОПК-5.6. Знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации.
- ОПК-5.7. Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации.
- ОПК-5.8. Знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности.
- ОПК-5.9. Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав.
- ОПК-5.10. Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.
- ОПК-5.11. Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации.
- ОПК-5.12. Умеет формулировать основные требования информационной безопасности при эксплуатации компьютерной системы.
- ОПК-5.13. Умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

− ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

− ОПК-6.2. Знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях.

− ОПК-6.3. Знает систему организационных мер, направленных на защиту информации ограниченного доступа.

− ОПК-6.4. Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа.

− ОПК-6.5. Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем.

− ОПК-6.6. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем.

− ОПК-6.7. Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации.

− ОПК-6.8. Умеет определить политику контроля доступа работников к информации ограниченного доступа.

− ОПК-6.9. Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации.

− ОПК-6.10. Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

овладение основами использования нормативно-правовых актов для разработки организационно-распорядительной документации, организации и планирования деятельности по защите информационных ресурсов.

Задачи учебной дисциплины:

формирование у студентов знаний о многообразии возможных способов и средств обеспечения информационной безопасности; знаний, умений и навыков по оцениванию эффективности систем защиты информации в компьютерных системах, подбору, изучению и обобщению научно-технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.50 Инсталляция и настройка программного обеспечения

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

− ОПК-2.3. Знает состав, назначение аппаратных средств и программного обеспечения персонального компьютера.

− ОПК-2.5. Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет.

− ОПК-2.6. Умеет составлять документы, используя прикладные программы офисного назначения.

− ОПК-2.7. Владеет средствами управления пользовательскими интерфейсами операционных систем.

− ОПК-2.8. Знает основные принципы конфигурирования и администрирования операционных систем.

− ОПК-2.11. Знает характерные особенности современного программного обеспечения специального назначения.

− ОПК-2.12. Умеет производить установку, наладку, тестирование и обслуживание программного обеспечения, включая решения отечественного производства.

− ОПК-2.13. Умеет производить установку, наладку, тестирование и обслуживание сетевого программного обеспечения, включая решения отечественного производства.

− ОПК-2.14. Умеет производить установку, наладку, тестирование и обслуживание современных программных средств обеспечения информационной безопасности.

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

− ОПК-4.19. Владеет навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.

ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения.

− ОПК-12.1. Знает принципы построения современных операционных систем и особенности их применения.

− ОПК-12.5. Умеет осуществлять администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отечественного производства.

− ОПК-12.6. Знает методы восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций.

− ОПК-12.7. Умеет восстанавливать работоспособность программ специального назначения при возникновении нештатных ситуаций.

ОПК-15. Способен администрировать компьютерные сети и контролировать корректность их функционирования.

− ОПК-15.8. Владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением.

ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

− ОПК-16.8. Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

− ОПК-16.9. Владеет навыками настройки межсетевых экранов.

− ОПК-16.10. Владеет методиками анализа сетевого трафика.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целью изучения дисциплины «Инсталляция и настройка программного обеспечения» является обучение студентов практическим навыкам по установке и настройке общесистемного и прикладного ПО. Основные задачи дисциплины – обучение студентов базовым принципам способов и современных средств инсталляции и настройки ПО, практическим навыкам применения способов и средствам ЗИ, при эксплуатации информационных, информационно-измерительных и управляющих систем данных с точки зрения решения базовых задач обработки информации.

Форма(ы) промежуточной аттестации - зачет.

Б1.О.51 Защита информации от утечки по техническим каналам

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.

− ОПК-5.14. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.

− ОПК-5.15. Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации.

− ОПК-5.16. Знает возможности технических средств перехвата информации.

− ОПК-5.17. Умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам.

− ОПК-5.18. Знает нормативные документами в области технической защиты информации.

− ОПК-5.19. Владеет методами и средствами технической защиты информации.

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

− ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

– ОПК-6.2. Знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях.

– ОПК-6.3. Знает систему организационных мер, направленных на защиту информации ограниченного доступа.

– ОПК-6.4. Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа.

– ОПК-6.5. Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем.

– ОПК-6.6. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем.

– ОПК-6.7. Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации.

– ОПК-6.8. Умеет определить политику контроля доступа работников к информации ограниченного доступа.

– ОПК-6.9. Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации.

– ОПК-6.10. Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.

ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

– ОПК-9.1. Знает технические каналы утечки информации.

– ОПК-9.2. Знает возможности технических средств перехвата информации.

– ОПК-9.3. Умеет организовать защиту информации от утечки по техническим каналам на объектах информатизации.

– ОПК-9.4. Умеет пользоваться нормативными документами в области технической защиты информации.

– ОПК-9.13. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.

– ОПК-9.14. Знает основы физической защиты объектов информатизации.

– ОПК-9.15. Умеет анализировать и оценивать угрозы информационной безопасности объекта.

– ОПК-9.16. Владеет методами и средствами технической защиты информации.

– ОПК-9.17. Владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение основ и принципов организации и технологии защиты информации (ЗИ) от утечки по техническим каналам с применением способов и средств ЗИ в рамках комплексного обеспечения безопасности информационных систем и технологий, изучение математических основ моделирования процессов защиты информации, получение профессиональных компетенций в области современных технологий защиты информации.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных способов и средств ЗИ;
- обучение студентов базовым методам ЗИ;
- овладение практическими навыками применения способов и средств ЗИ;
- раскрытие физической сущности построения и эксплуатации информационных, информационно-измерительных и управляющих систем данных с точки зрения решения базовых задач обработки информации.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.52 Теория радиотехнических систем

Общая трудоемкость дисциплины 5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности.

– ОПК-4.4. Знает основы теории колебаний и волн, оптики.

– ОПК-4.6. Умеет использовать математические модели физических явлений и процессов.

– ОПК-4.7. Умеет решать типовые прикладные физические задачи.

– ОПК-4.8. Владеет методами исследования физических явлений и процессов.

– ОПК-4.9. Знает принципы работы элементов и функциональных узлов электронной аппаратуры.

– ОПК-4.10. Знает методы анализа и синтеза электронных схем.

– ОПК-4.11. Знает типовые схемотехнические решения основных узлов и блоков электронной аппаратуры.

– ОПК-4.12. Умеет работать с современной элементной базой электронной аппаратуры.

– ОПК-4.13. Умеет использовать стандартные методы и средства проектирования цифровых узлов и устройств.

– ОПК-4.14. Владеет навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры.

– ОПК-4.15. Владеет навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации.

– ОПК-4.17. Умеет анализировать и синтезировать электронные схемы.

– ОПК-4.20. Знает фундаментальные закономерности, связанные с получением сигналов и их передачей по каналам связи.

– ОПК-4.21. Знает фундаментальные закономерности, связанные с обработкой и преобразованием сигналов в информационных системах.

– ОПК-4.22. Знает функциональное назначение и принципы работы основных блоков современных средств защиты информации.

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

− ОПК-9.5. Знает основные характеристики сигналов электросвязи, спектры и виды модуляции.

− ОПК-9.8. Умеет анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи.

ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.

− ОПК-10.22. Знает основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума.

− ОПК-10.23. Знает основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга).

− ОПК-10.24. Знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования.

ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.

− ОПК-16.14. Умеет производить оценку технического состояния аппаратных средств защиты информации.

− ОПК-16.15. Знает методологию применения технических средств диагностики состояния устройств защиты информации.

− ОПК-16.16. Умеет выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Цель изучения дисциплины «Введение в специальность» заключается в изложении математических основ теории радиотехнических систем, методов их синтеза и анализа, подготовке студентов к применению данных методов для моделирования различных телекоммуникационных систем.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.53 Уравнения математической физики

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-3.43 Знает основные типы обыкновенных дифференциальных уравнений и методы их решения.

ОПК-3.58 Владеет навыками решения основных типов обыкновенных дифференциальных уравнений

ОПК-4 Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять

основные физические законы и модели для решения задач профессиональной деятельности;

ОПК-4.6 Умеет использовать математические модели физических явлений и процессов.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Форма(ы) промежуточной аттестации – зачет.

Б1.О.54 Комплексный анализ

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;

ОПК-3.42 Знает основные задачи теории функций комплексного переменного.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Форма(ы) промежуточной аттестации – зачет.

Б1.О.55 Дисциплины специализации

Общая трудоемкость дисциплины 22 з.е.

Б1.О.53.01 Методы верификации

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-1.3. Способен проводить тестирование и использовать средства верификации механизмов защиты информации.

–ОПК-1.3.1. Знает основные способы и средства верификации программ.

–ОПК-1.3.2. Знает основные способы тестирования средств защиты информации с использованием средств верификации программ.

–ОПК-1.3.3. Умеет применять основные методы верификации программ и алгоритмов на предмет соответствия требованиям защиты информации.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

ознакомление с предметом верификации программного обеспечения, обзор существующих методов и подходов, освещение преимуществ и ограничений, присущих методам верификации. Изучение способов спецификации свойств

программ, методов и приемов исследования свойств программ, анализа и доказательства корректности программ.

Задачи учебной дисциплины:

- формирование базовых знаний в области обеспечения качества программного обеспечения, как неотъемлемой части теории и практики разработки верификации программного обеспечения;
- изучение основ жизненного цикла программного обеспечения и задач верификации, возникающих в ходе разработки, внедрения и эксплуатации верификации программного обеспечения;
- изучение методов тестирования, применяемых в различных сценариях разработки верификации программного обеспечения;
- изучение базовых методов анализа корректности программ.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.53.02 Алгоритмы кодирования и сжатия информации

Общая трудоемкость дисциплины 5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-1.2. Способен оценивать корректность программных реализаций алгоритмов защиты информации.

–ОПК-1.2.2. Знает теоретические основы устранения избыточности данных.

–ОПК-1.2.3. Знает основные алгоритмы кодирования данных и сжатия текстовой, графической, аудио- и видеоинформации.

–ОПК-1.2.4. Умеет проводить анализ программ и алгоритмов сжатия данных на предмет соответствия требованиям защиты информации.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

углубление знаний в области теории информации, в частности теории кодирования и сжатия информации, а также в получении навыков разработки и применения соответствующих технологий в задачах передачи, преобразования и хранения информации.

Задачи учебной дисциплины:

- овладение фундаментальными знаниями по теории кодирования и сжатия информации;
- овладение технологиями кодирования и сжатия, восстановления и хранения информации;
- приобретение практических навыков работы при реализации кодирующих и декодирующих алгоритмов, а также алгоритмов сжатия.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.53.03 Методы и стандарты оценки защищенности компьютерных систем

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-1.1. Способен проводить анализ защищенности и находить уязвимости компьютерной системы.

–ОПК-1.1.1. Знает принципы построения защищенных компьютерных систем и сетей.

–ОПК-1.1.2. Знает требования основных стандартов по оценке защищенности компьютерных систем и сетей.

–ОПК-1.1.3. Умеет определять уровень защищенности и доверия программно-аппаратных средств защиты информации.

–ОПК-1.1.4. Умеет классифицировать информационные системы по требованиям защиты информации.

–ОПК-1.1.5. Умеет определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе.

–ОПК-1.1.6. Умеет выполнять анализ компьютерной системы с целью определения уровня защищенности и доверия.

–ОПК-1.1.7. Умеет проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

Изучение теоретических основ и принципов построения защищенных систем обработки информации, стандартов информационной безопасности, критериев и классов защищенности средств вычислительной техники и автоматизированных систем, формальных моделей безопасности, методов и средств проектирования технологически безопасного программного обеспечения, порядка проведения сертификации защищенных систем обработки информации, вопросов использования интеллектуальных систем для обоснования требований и оценки защищенности систем обработки информации.

Основные задачи дисциплины:

- обучение студентов базовым понятиям стандартов информационной безопасности и руководящих документов Гостехкомиссии России (ФСТЭК России) в области защиты от НСД автоматизированных систем и средств вычислительной техники;
- обучение студентов формальным моделям безопасности для дискреционной, мандатной и ролевой политик безопасности и их расширений;
- обучение студентов базовым методам и алгоритмам проектирования технологически безопасного программного обеспечения;

- овладение практическими навыками проектирования технологически безопасного программного обеспечения и интеллектуальных систем обоснования требований и оценки защищенности систем обработки информации;

- овладение практическими навыками проведения сертификации защищенных систем обработки информации.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.О.53.04 Интеллектуальные системы обработки информации

Общая трудоемкость дисциплины 5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

–ОПК-7.4. Умеет работать с интегрированной средой разработки программного обеспечения.

–ОПК-7.6. Владеет навыками разработки, документирования, тестирования и отладки программ.

–ОПК-7.10. Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.

–ОПК-7.11. Владеет навыками разработки алгоритмов решения типовых профессиональных задач.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- изучение теоретических основ и принципов построения информационных систем, основанных на представлении, хранении и обработки знаний, реализующих интеллектуальны вывод на знаниях;

- получение практических навыков разработки интеллектуальных информационных программных систем;

- получение профессиональных компетенций в области современных технологий разработки систем искусственного интеллекта.

Задачи учебной дисциплины:

- обучение студентов методам формального представления и описания знаний и принципам реализации интеллектуального вывода;

- освоение современных теорий построения систем искусственного интеллекта, реализующих нечеткий вывод на неполных и ненадежных знаниях;

- обучение студентов методам и алгоритмам, применяемым для построения систем поддержки принятия решений, экспертных систем, систем обработки естественно-языковой информации;

- овладение практическими навыками разработки и применения интеллектуальных информационных технологий.

Форма(ы) промежуточной аттестации - экзамен.

Б1.О.53.05 Алгоритмы и структуры данных

Общая трудоемкость дисциплины 5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ.

–ОПК-7.7. Знает базовые структуры данных.

–ОПК-7.8. Знает основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы.

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности.

–ОПК-13.10. Знает базовые структуры данных.

–ОПК-13.11. Знает основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности.

–ОПК-13.12. Умеет формализовать поставленную задачу.

–ОПК-13.13. Умеет разрабатывать эффективные алгоритмы и программы.

–ОПК-13.14. Умеет проводить оценку вычислительной сложности алгоритма.

–ОПК-13.15. Умеет планировать разработку сложного программного обеспечения.

–ОПК-13.16. Владеет методами оценки качества готового программного обеспечения.

–ОПК-13.17. Владеет навыками разработки алгоритмов для решения типовых профессиональных задач.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

познакомить студентов с различными способами представления данных в памяти ЭВМ, с различными классами задач и типами алгоритмов, встречающихся при решении задач на современных ЭВМ.

Задачи учебной дисциплины:

Изучение структур данных и алгоритмов их обработки, знакомство с фундаментальными принципами построения эффективных и надежных программ. Курс ориентирован на становление математика-программиста, должен способствовать повышению культуры мышления. Курс предназначен для овладения компьютерными методами обработки информации путем развития

профессиональных навыков разработки, выбора и преобразования алгоритмов, что является важной составляющей эффективной реализации программного продукта.

Форма(ы) промежуточной аттестации – экзамен.

Б1.В.01 Стеганография и цифровые водяные знаки

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

ПК-3. Способен проводить анализ безопасности программных средств в компьютерных системах.

–ПК-3.2. Знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования.

–ПК-3.4. Умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение основ стеганографического скрытия информации, вопросов выявления скрытых стеганографическим способом данных – стегоанализа, защиты информации от несанкционированного доступа, обеспечения конфиденциальности обмена информацией в информационно-вычислительных системах, вопросов защиты авторских прав с применением современных технологий создания цифровых водяных знаков; получение профессиональных компетенций в области современных технологий защиты информации.

Задачи учебной дисциплины:

–обучение студентов основным теоретическим и практическим аспектам стеганографического скрытия информации, включая базовые принципы организации скрытых каналов передачи информации и принципы защиты авторских прав на цифровые объекты интеллектуальной собственности с использованием технологий создания цифровых водяных знаков;

–ознакомление студентов с современными мерами противодействия стеганографическому скрытию, принципами стегоанализа;

–овладение практическими навыками применения на практике теоретических знаний для реализации стеганографического скрытия информации в файлы распространенных форматов.

Форма(ы) промежуточной аттестации - экзамен.

Б1.В.02 Моделирование систем

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

ПК-2. Способен проводить исследования на всех этапах жизненного цикла программных средств в профессиональной деятельности.

–ПК-2.1. Знает методы и средства планирования и организации исследований и разработок.

–ПК-2.2. Знает методы проведения экспериментов и наблюдений, обобщения и обработки информации, полученной в ходе исследований.

–ПК-2.3. Планирует стадии исследования или разработки в рамках поставленной задачи, выбирает или формирует программную среду для компьютерного моделирования и проведения экспериментов.

–ПК-2.4. Использует стандартное и оригинальное программное обеспечение, проводит компьютерный эксперимент, составляет его описание и формулирует выводы.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение теоретических основ и овладение практическими навыками компьютерного моделирования систем в интересах анализа информационных, информационно-измерительных и управляющих систем различного назначения.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современной методологии и технологий моделирования систем различного назначения;
- обучение студентов базовым методам и подходам компьютерного имитационного моделирования систем;
- овладение практическими навыками применения средств компьютерного моделирования систем.

Форма(ы) промежуточной аттестации - экзамен.

Б1.В.03 Технологии защищенного документооборота и блокчейн

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

ПК-3. Способен проводить анализ безопасности программных средств в компьютерных системах.

–ПК-3.2. Знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования.

–ПК-3.4. Умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение теоретических основ и овладение практическими навыками применения методов и средств электронной подписи,технологий блокчейн для организации защищенного документооборота, в интересах обеспечения мер защиты информации при разработке, сопровождении и проектировании информационных систем различного назначения; получение профессиональных компетенций в области современных технологий обработки и защиты информации.

Задачи учебной дисциплины:

- обучение студентов базовым понятиям современных технологий обработки информации с использованием электронной подписи;
- освоение студентами положений и требований, современных нормативнометодических документов регламентирующих использование электронной подписи;
- освоение студентами положений инфраструктуры открытых ключей (англ. PKI
- Public Key Infrastructure) для поддержки криптозадач на основе закрытого и открытого ключей;
- освоение технологии формирования квалифицированных сертификатов ключей проверки электронной подписи и освоение практических решений применения

технологий защищённого документооборота;

- овладение практическими навыками применения алгоритмов обработки информации с использованием электронной подписи;

- формирование представления об угрозах безопасности информации при использовании электронной подписи и основных требованиях к удостоверяющим центрам, средствам электронной подписи и квалифицированным сертификатам проверки электронной подписи;

- овладение практическими навыками применения алгоритмов обработки информации с использованием электронной подписи;

- формирование представления о технологиях блокчейн.

Форма(ы) промежуточной аттестации - зачет.

Б1.В.04 Методология экспериментальных исследований и испытаний

Общая трудоемкость дисциплины 4 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-2. Способен проводить исследования на всех этапах жизненного цикла программных средств в профессиональной деятельности.

–ПК-2.1. Знает методы и средства планирования и организации исследований и разработок.

–ПК-2.2. Знает методы проведения экспериментов и наблюдений, обобщения и обработки информации, полученной в ходе исследований.

–ПК-2.3. Планирует стадии исследования или разработки в рамках поставленной задачи, выбирает или формирует программную среду для компьютерного моделирования и проведения экспериментов.

–ПК-2.4. Использует стандартное и оригинальное программное обеспечение, проводит компьютерный эксперимент, составляет его описание и формулирует выводы.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение теоретических основ и овладение практическими навыками применения методов и средств экспериментальных исследований, измерений и испытаний в процессе разработки, создания и эксплуатации информационных, информационно-измерительных и управляющих систем различного назначения; получение профессиональных компетенций в области современных технологий организации, проведения и обработки результатов экспериментальный исследований и испытаний на различных этапах жизненного цикла информационных, информационно-измерительных и управляющих систем.

Задачи учебной дисциплины:

- обучение базовым понятиям теорий измерения, контроля, испытаний и технической диагностики;

- обучение базовым методам и приемам организации и проведения экспериментальных исследований в процессе испытаний информационных, информационно-измерительных и управляющих систем, контроля их состояния и технической диагностики;

- раскрытие принципов построения и применения организационно-технических (технических) систем экспериментальных исследований (измерений, контроля, испытаний, технической диагностики).

- овладение практическими навыками разработки методик экспериментальных исследований с использованием современных технических и программных средств и технологий;

- овладение практическими навыками разработки итоговых документов по результатам экспериментальных исследований (отчетов, актов, протоколов) в соответствии с действующими стандартами и нормативно-техническими документами.

Форма(ы) промежуточной аттестации - экзамен.

Б1.В.05 Анализ уязвимостей и защита программного обеспечения

Общая трудоемкость дисциплины 3 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-3. Способен проводить анализ безопасности программных средств в компьютерных системах.

–ПК-3.1. Знает основные типы уязвимостей программного обеспечения и возможные пути их устранения.

–ПК-3.3. Умеет анализировать программные средства на наличия уязвимостей.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

ознакомление студентов с теоретическими и практическими аспектами анализа уязвимостей программного обеспечения (ПО) для повышения безопасности разработки и эксплуатации информационных систем различного назначения.

Задачи учебной дисциплины:

- ознакомление студентов с причинами возникновения уязвимостей в программном коде, классификация уязвимостей, изучение практических примеров уязвимостей в программном коде;
- изучение принципов анализа кода, внутреннего представления программы для анализа, ознакомление с принципами работы статистических и динамических анализаторов кода;
- изучение приемов обфускции, вопросов защиты исходных и байт кодов программ;

- овладение практическими навыками формирования комплекса мер для повышения качества разработки ПО.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.В.06 Дисциплины военного модуля

Общая трудоемкость дисциплины 38 з.е.

Форма(ы) промежуточной аттестации - экзамен.

Б1.В.07 Элективные дисциплины по физической культуре и спорту

Общая трудоемкость дисциплины 21 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-7 Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

– УК-7.4. Понимает роль физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

– УК-7.5. Использует методику самоконтроля для определения уровня здоровья и физической подготовленности в соответствии с нормативными требованиями и условиями будущей профессиональной деятельности.

– УК-7.6. Поддерживает должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности, регулярно занимаясь физическими упражнениями.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

формирование физической культуры личности и способности направленного использования методов и средств физической культуры и спорта для обеспечения полноценной социальной и профессиональной деятельности.

Задачи учебной дисциплины:

- обеспечение понимания роли физической культуры в развитии личности и подготовке ее к профессиональной деятельности.

- формирование мотивационно-ценностного отношения к физической культуре, установки на здоровый стиль жизни, потребности в регулярных занятиях физическими упражнениями и спортом.

- способствование адаптации организма к воздействию умственных и физических нагрузок, а также расширению функциональных возможностей физиологических систем, повышению сопротивляемости защитных сил организма.

- овладение методикой формирования и выполнения комплекса упражнений оздоровительной направленности для самостоятельных занятий, способами самоконтроля при выполнении физических нагрузок различного характера, правилами личной гигиены, рационального режима труда и отдыха.

Форма(ы) промежуточной аттестации - зачет.

Б1.В.ДВ.01.01 Язык программирования Java

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

изучение основных конструкций и структур языка программирования Java, а также принципов разработки приложений для персональных компьютеров на данной платформе; приобретение навыков построения пользовательского интерфейса приложений; приобретение навыков работы в наиболее популярных языковых средах разработки для языка программирования Java (NetBeans IDE, IntelliJ IDEA, Eclipse IDE).

Форма(ы) промежуточной аттестации - зачет.

Б1.В.ДВ.01.02 Язык программирования C#

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

изучение основных конструкций и структур языка программирования С++, а также принципов разработки приложений для персональных компьютеров на данной платформе; приобретение навыков построения пользовательского интерфейса приложений; приобретение навыков работы в наиболее популярных языковых средах разработки для языка программирования С++.

Форма(ы) промежуточной аттестации - зачет.

Б1.В.ДВ.01.03 Правовые и организационные основы добровольческой (волонтерской) деятельности

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

УК-3.2 Вырабатывает конструктивную командную стратегию для достижения поставленной цели

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

Задачи учебной дисциплины:

Форма(ы) промежуточной аттестации - зачет.

Б1.В.ДВ.01.04 Основы конструктивного взаимодействия лиц с ограниченными возможностями здоровья в образовательном процессе

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

–УК-3.3. Эффективно взаимодействует с участниками образовательного процесса, соблюдая психологически обоснованные правила и нормы общения.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

теоретическая и практическая подготовка обучающихся с ОВЗ в области коммуникативной компетентности.

Задачи учебной дисциплины:

1) изучение техник и приемов эффективного общения;

2) формирование у обучающихся навыков активного слушания, установления доверительного контакта;

3) преодоление возможных коммуникативных барьеров, формирование умений и навыков использования различных каналов для передачи информации в процессе общения;

4) развитие творческих способностей будущих психологов в процессе тренинга общения.

Форма(ы) промежуточной аттестации - зачет.

Б1.В.ДВ.01.05 Общественный проект "Обучение служением"

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-5. Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

–УК-5.4.1 Осознает свою гражданскую идентичность как принадлежность к государству, обществу, культурному наследию страны, ответственность за будущее страны; проявляет активную гражданскую позицию.

Место учебной дисциплины в структуре ОПОП: дисциплина «Общественный проект “Обучение служением”» относится к Блоку Б.1 «Дисциплины (модули)», включена в часть, формируемую участниками образовательных отношений, и является курсом по выбору.

Цели и задачи учебной дисциплины

Цели изучения дисциплины:

Целью реализации Общественного проекта “Обучение служением” выступает развитие у обучающихся гражданственности, формирование чувства ответственности за свою страну и её будущее в процессе решения социально значимой практической задачи.

Задачи учебной дисциплины:

- совершенствовать навыки проектной деятельности на всех этапах разработки и реализации проекта, а также умение определять свою роль в коллективе, навыки командного взаимодействия;

- развить профессиональные умения и навыки обучающихся в ходе разработки и реализации социального проекта;

- способствовать формированию активной гражданской позиции обучающихся через практическое взаимодействие с социальными и профессиональными партнёрами.

- создать условия для приобщения обучающихся к традиционным ценностям гражданской солидарности, патриотизма, сотрудничества, добровольчества, социальной ответственности.

Форма промежуточной аттестации – зачет.

Б1.В.ДВ.02.01 Языки программирования

Общая трудоемкость дисциплины 2.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

знакомство студентов с различными подходами, приемами и парадигмами программирования, различными языками программирования и представления данных, современными приемами разработки ПО; изучение на примере языка C# и среды программирования Visual Studio принципов объектно-ориентированного программирования и разработки ПО; изучение основ UML (диаграммы классов, объектов, взаимодействия); овладение эффективными приемами работы в современных средах программирования (в том числе отладка, тестирование, рефакторинг кода).

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.В.ДВ.02.02 Алгоритмы машинной графики

Общая трудоемкость дисциплины 2.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

понимание основных принципов обработки графической информации в компьютерных системах

Задачи учебной дисциплины:

- представление об основных технологиях в области компьютерной графики;
- владение методами конструирования 2D и 3D графических объектов;
- навыки использования графических библиотек;
- знание основных алгоритмов обработки графической информации;
- научить студентов профессионально проектировать программные приложения .NET; использовать современные технологии разработки программ, с учетом требований предметной области и потребностей пользователей;
- выработать практические навыки применения полученных знаний.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.В.ДВ.02.03 Психолого-педагогическое сопровождение лиц с ограниченными возможностями здоровья

Общая трудоемкость дисциплины 2.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

–УК-3.3. Эффективно взаимодействует с участниками образовательного процесса, соблюдая психологически обоснованные правила и нормы общения.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

теоретическая и практическая подготовка обучающихся с ОВЗ в области коммуникативной компетентности.

Задачи учебной дисциплины:

1) изучение техник и приемов эффективного общения;
2) формирование у обучающихся навыков активного слушания, установления доверительного контакта;
3) преодоление возможных коммуникативных барьеров, формирование умений и навыков использования различных каналов для передачи информации в процессе общения;
4) развитие творческих способностей будущих психологов в процессе тренинга общения.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.В.ДВ.03.01 Биометрические методы идентификации личности

Общая трудоемкость дисциплины 4.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

изучение студентами совокупности автоматизированных методов и средств идентификации человека, основанных на его физиологической или поведенческой характеристике, представленных в виде статистических данных.

Задачи учебной дисциплины:

- изучение методов биометрической идентификации (статистических и динамических) и их характеристики;
- исследование существующих биометрических систем безопасности;
- изучение структуры и компонентов биометрических систем;
- изучение биометрических методов компьютерной безопасности;
- исследование возможных перспектив биометрических систем безопасности;
- формирование практических навыков идентификации личности.

Форма(ы) промежуточной аттестации - экзамен.

Б1.В.ДВ.03.02 Язык HTML

Общая трудоемкость дисциплины 4.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

ознакомление студентов с технологиями разработки и создания WWW-сайтов, изучение языка гипертекстовой разметки (HTML) и применение интернет технологий в учебной и профессиональной деятельности/

Форма(ы) промежуточной аттестации - экзамен.

Б1.В.ДВ.04.01 Параллельные алгоритмы обработки данных

Общая трудоемкость дисциплины 2.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

изучение наиболее общих принципов построения параллельных алгоритмов и связанных вопросов классификации их реализующих параллельных вычислительных систем, практических приемов их применения для решения вычислительных задач и при реализации параллельных приложений.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.В.ДВ.04.02 Технологии интернет вещей

Общая трудоемкость дисциплины 2.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: обязательная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

- изучение инструментария управления и оптимизации процессов, происходящих в современном информационном обществе. Сформировать основные понятия и объяснить терминологию, при разработке конкретных проектов в сфере «Интернета вещей». Освоить основные технологии интернета вещей: операционные системы реального времени, базы данных, клиент-серверные технологии, промышленный интернет вещей (SCADA).

Задачи учебной дисциплины:

–формирование основополагающих представлений о вычислительной сети физических объектов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека;

–формирование навыков оценки основных характеристик способов и устройств адресации, а также технологии идентификации этих предметов («вещей»). Методы и средства, применяемые для автоматической идентификации: оптически распознаваемые идентификаторы (штрих коды, Data Matrix, QR-коды), средства определения местонахождения в режиме реального времени.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.В.ДВ.05.01 Разработка приложений на C++

Общая трудоемкость дисциплины 2.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются:

приобретение базовых знаний и навыков по алгоритмизации, разработке, отладке и тестированию программ на языке C++, проектированию и разработке приложений с применением объектно-ориентированного подхода.

Задачи учебной дисциплины:

- изучение технологии программирования на языке С++;
- раскрытие принципов объектно-ориентированного подхода при проектировании и разработке приложений;
- овладение средствами объектно-ориентированного и обобщенного программирования языка С++, средствами стандартной библиотеки STL.
- изучение методов отладки и тестирования программ на С++.

Форма(ы) промежуточной аттестации - зачет с оценкой.

Б1.В.ДВ.05.02 Обработка изображений

Общая трудоемкость дисциплины 2.5 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения.

–ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.

–ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.

–ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Цели и задачи учебной дисциплины

Форма(ы) промежуточной аттестации - зачет с оценкой.

ФТД.01 Защита персональных данных

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

– *ПК-3. Способен проводить анализ безопасности программных средств в компьютерных системах*

– ПК-3.2 знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от несанкционированного использования

– ПК-3.4 умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента

Место учебной дисциплины в структуре ОПОП: учебная дисциплина "Защита персональных данных" относится к вариативной части Блока ФТД.

Форма промежуточной аттестации – зачет.

ФТД.02 Реляционные системы управления базами данных

Общая трудоемкость дисциплины 2 з.е.

Дисциплина направлена на формирование следующих компетенций и индикаторов их достижения:

– *ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности;*

– ОПК-2.3 Знает состав, назначение аппаратных средств и программного обеспечения персонального компьютера,

Место учебной дисциплины в структуре ОПОП: учебная дисциплина "Реляционные системы управления базами данных" относится к вариативной части Блока ФТД.

Форма промежуточной аттестации – зачет.

Приложение 9

Аннотация программы учебной и производственной практик Б2.О.01(У) Учебная практика, экспериментально-исследовательская

Общая трудоемкость практики 3 з.е.

Практика направлена на формирование следующих компетенций с указанием кодов индикаторов их достижения:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1.1)

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели (УК-3.1 - УК-3.3)

ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2.1 - ОПК-2.14)

ОПК-4. Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности (ОПК-4.18 - ОПК-4.19)

Место практики в структуре ОПОП: обязательная часть блока Б2

Целями учебной практики, экспериментально-исследовательской являются:

ознакомление студентов со спецификой получаемой специальности, с объектами будущей работы;

подготовка студентов к осознанному и углубленному изучению общепрофессиональных и специальных дисциплин для последующего освоения компетенций по направлению специализированной подготовки в области защиты информации;

формирование первичных профессиональных умений и навыков исследования и формализации прикладных задач по защите информации на базе учебных задач.

Задачами учебной практики, экспериментально-исследовательской являются:

получение студентами первичных сведений по обеспечению комплексной защиты информации в различных типах организаций, знакомство с правовым регулированием обеспечения информационной безопасности, с технологиями информационной защиты, применяемыми в автоматизированной информационной системе (АИС) ВГУ и на рабочих местах пользователей.

Тип практики: учебная экспериментально-исследовательская.

Способ проведения практики: стационарная.

Форма проведения практики: *дискретная.*

Разделы (этапы) практики:

Учебно-исследовательский этап: определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор современных информационных технологий, специального программного обеспечения и

оборудования, для решения поставленной задачи по анализу защищенности объекта информатизации;

Экспериментально-исследовательский этап: проведение самостоятельного решения учебной исследовательской задачи, выполнение типовых расчетов и моделирование датчиков псевдослучайных числовых последовательностей с применением компьютерной техники, проведение экспериментальных исследований системы защиты информации.

Оформление отчёта по итогам практики: составление итогового отчета и защита проекта, описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

Форма промежуточной аттестации – зачет.

Б2.О.02(У) Учебный сбор

Общая трудоемкость практики 3 з.е.

Форма промежуточной аттестации – зачет с оценкой.

Б2.О.03(Н) Производственная практика, научно-исследовательская работа

Общая трудоемкость практики 11 з.е.

Практика направлена на формирование следующих компетенций с указанием кодов индикаторов их достижения:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1.1- УК-1.2)

ОПК-7. Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ (ОПК-7.1 - ОПК-7.16)

ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей (ОПК-8.10, ОПК-8.11, ОПК-8.13, ОПК-8.15)

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации (ОПК-9.15 - ОПК-9.17)

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13.1, ОПК-13.2, ОПК-13.5-ОПК-13.7, ОПК-13.12-ОПК-13.19, ОПК-13.21, ОПК-13.23, ОПК-13.24)

Целью производственной практики, научно-исследовательской работы является:

развитие профессиональных знаний и компетенций студентов, получение профессиональных умений и опыта профессиональной деятельности на базе практических задач, для решения которых необходимо использовать современные информационные технологии обработки и защиты информации.

Задачами производственной практики, научно-исследовательской работы являются:

проведение анализа исходных данных для проектирования компонентов подсистем и средств обеспечения информационной безопасности;

разработка отдельных компонентов программных и программно-аппаратных средств защиты информации в компьютерных системах;

проведение анализа и экспериментальных исследований их безопасности;

получение навыков самостоятельного применения методов научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей.

Место практики в структуре ОПОП: обязательная часть блока Б2

Способ проведения практики: стационарная.

Форма проведения практики: *непрерывная.*

Разделы (этапы) практики:

Проектно-технологический этап: анализ исходных данных для проектирования компонентов подсистем и средств обеспечения информационной безопасности и разработка отдельных компонентов программных и программно-аппаратных средств защиты информации в компьютерных системах;

Экспериментально-исследовательский этап: анализ и проведение экспериментальных исследований компонентов подсистем защиты информации с целью получения навыков самостоятельного решения исследовательских задач.

Оформление отчёта по итогам практики: составление итогового отчета и защита проекта, описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

Форма промежуточной аттестации – зачет с оценкой.

Б2.О.04 (Пд) Производственная практика, преддипломная

Общая трудоемкость практики 7 з.е.

Практика направлена на формирование следующих компетенций с указанием кодов индикаторов их достижения:

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

(УК-1.1 - УК-1.3)

УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни (УК-6.1, УК-6.3, УК-6.4)

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации (ОПК-9.13-ОПК-9.17)

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13.1-ОПК-13.24)

Место практики в структуре ОПОП: обязательная часть блока Б2

Целями производственной практики, преддипломной являются:
проведение систематизации, расширения, закрепление и углубления теоретических профессиональных знаний, полученных в результате изучения дисциплин направления и специальных дисциплин профильной программы подготовки.

Задачами производственной практики преддипломной являются:
формирование у студентов навыков ведения самостоятельной научной работы, исследования и экспериментирования, приобретение опыта в исследовании актуальной научной проблемы, а также подбор необходимых материалов для выполнения выпускной квалификационной работы.

Тип практики: производственная преддипломная.

Способ проведения практики: стационарная.

Форма проведения практики: *дискретная.*

Разделы (этапы) практики:
Подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ.
Научно-исследовательский этап: выбор темы исследования; определение проблемы, объекта и предмета исследования; формулирование цели и задач исследования; теоретический анализ литературы и исследований по проблеме, подбор необходимых источников по теме (патентные материалы, научные отчеты, техническая документация и др.); составление библиографии; формулирование рабочей гипотезы.
Этап выполнения исследовательских работ по индивидуальному плану: определение проблемы, объекта и предмета исследования, формулирование цели и задач исследования, теоретический анализ литературы и исследований по проблеме, проведение обзора и выбор современных информационных технологий, специального программного обеспечения и оборудования для решения поставленной задачи по анализу защищенности объекта информатизации; проведение самостоятельного решения учебной научной задачи, исследований и экспериментов.
Этап оформления отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

Форма промежуточной аттестации – зачет с оценкой.

Б2.О.05(П) Войсковая стажировка

Общая трудоемкость практики 6 з.е.
Форма промежуточной аттестации – зачет с оценкой.

Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности

Общая трудоемкость практики 6 з.е.

Практика направлена на формирование следующих компетенций с указанием кодов индикаторов их достижения:

ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах (ОПК-1.1.1-ОПК-1.1.7)

ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях (ОПК-1.2.1-ОПК-1.2.7)

ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям (ОПК-1.3.1-ОПК-1.3.3)

ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации (ОПК-5.3, ОПК-5.4, ОПК-5.9-ОПК-5.13, ОПК-5.17, ОПК-5.19)

ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6.6, ОПК-6.7, ОПК-6.9, ОПК-6.10)

ОПК-9. Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации (ОПК-9.3, ОПК-9.4, ОПК-9.9, ОПК-9.16, ОПК-9.17)

ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10.4-ОПК-10.6, ОПК-10.9, ОПК-10.10, ОПК-10.14-ОПК-10.20, ОПК-10.25- ОПК-10.28)

ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации (ОПК-11.4, ОПК-11.5, ОПК-11.9, ОПК-11.10)

ОПК-12. Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения (ОПК-12.4, ОПК-12.5)

ОПК-13. Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13.1, ОПК-13.2, ОПК-13.5-ОПК-13.7, ОПК-13.12-ОПК-13.19, ОПК-13.21, ОПК-13.23, ОПК-13.24)

ОПК-14. Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации (ОПК-14.4-ОПК-14.6, ОПК-14.11- ОПК-14.14)

ОПК-15. Способен администрировать компьютерные сети и контролировать корректность их функционирования (ОПК-15.5-ОПК-15.8)

ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях (ОПК-16.6-ОПК-16.10, ОПК-16.12, ОПК-16.14, ОПК-16.16)

Место практики в структуре ОПОП: обязательная часть блока Б2

Целью производственной практики по получению профессиональных умений и навыков в области профессиональной деятельности является:

развитие профессиональных знаний и компетенций студентов, получение профессиональных умений и опыта профессиональной деятельности на базе практических задач, для решения которых необходимо использовать современные информационные технологии обработки и защиты информации, а также приобщение студентов к среде предприятия (организации) с целью приобретения социально-личностных и профессиональных компетенций.

Задачами производственной практики по получению профессиональных умений и навыков в области профессиональной деятельности являются:

формирование у студентов умений и навыков: проведения технического обследования объекта информационной защиты; сбора экспериментального и экспертного материала и его теоретического обобщения; настройки, эксплуатации и поддержании в работоспособном состоянии компонентов систем обеспечения информационной безопасности;

обучение студентов методикам работы с измерительной аппаратурой для контроля и изучения отдельных характеристик процессов, приборов, устройств, программного обеспечения информационных систем для решения задач обеспечения информационной безопасности.

Тип практики: производственная, по получению профессиональных умений и навыков в области профессиональной деятельности.

Способ проведения практики: стационарная.

Форма проведения практики: *дискретная.*

Разделы (этапы) практики:

Подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ, ознакомление студентов с организационной структурой профильной организации, применяемой аппаратурой и программным обеспечением, нормативными актами и инструкциями.

Эксплуатационный этап: изучение нормативных документов по защите информации и методиками проверки защищенности объекта информатизации; ознакомление с принципами формирования политики информационной безопасности в корпоративной информационной системе; оценка информационных рисков в информационной системе;

ознакомление с применяемыми в организации принципами технического, программного и информационного обеспечения защищенных информационных систем; разработка предложений по совершенствованию системы управления информационной безопасностью.

Оформление отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

Форма промежуточной аттестации – зачет с оценкой.

Б2.В.01(П) Производственная практика, технологическая

Общая трудоемкость практики 5 з.е.

Практика направлена на формирование следующих компетенций с указанием кодов индикаторов их достижения:

ПК-1. Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения (ПК-1.1- ПК-1.3)

ПК-2. Способен проводить исследования на всех этапах жизненного цикла программных средств в профессиональной деятельности (ПК-2.1- ПК-2.4)

ПК-3. Способен проводить анализ безопасности программных средств в компьютерных системах (ПК-3.1- ПК-3.4)

Место практики в структуре ОПОП: Вариативная часть блока Б2

Целями производственной практики, технологической являются:

закрепление и расширение теоретических знаний студентов, получение студентами практического профессионального опыта, приобретение более глубоких практических навыков по направлению будущей работы;

практическое освоение методов и средств защиты информации на объектах информатизации.

Задачами производственной практики, технологической являются:

развитие профессиональных знаний и компетенций студентов, получение профессиональных умений и опыта профессиональной деятельности на базе практических производственных задач, для решения которых необходимо использовать современные информационные технологии обработки и защиты информации.

Тип практики: производственная технологическая.

Способ проведения практики: стационарная.

Форма проведения практики: *дискретная.*

Разделы (этапы) практики:

Подготовительный этап: инструктаж по общим вопросам, по технике безопасности, составление плана работ, ознакомление студентов с организационной структурой профильной организации, применяемой аппаратурой и программным обеспечением, нормативными актами и инструкциями.

Технологический этап: изучить нормативные документы по защите информации и методиками проверки защищенности объекта информатизации; ознакомиться с принципами формирования политики информационной безопасности в корпоративной информационной системе;

ознакомиться с применяемыми в организации технологиями технического, программного и информационного обеспечения защищенных информационных систем, методами и средствами обеспечения сетевой безопасности, безопасности операционных систем, безопасности в СУБД; разработать предложения по совершенствованию системы управления информационной безопасностью.

Оформление отчёта по итогам практики: описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.

Форма промежуточной аттестации – зачет с оценкой.

Приложение 10

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

основной профессиональной образовательной программы высшего образования

10.05.01 Компьютерная безопасность

Профиль – Анализ безопасности компьютерных систем

В результате освоения программы у выпускника должны быть сформированы следующие компетенции:

— универсальные компетенции:

Категория универсальных компетенций	Код	Формулировка компетенции	Код и формулировка индикатора достижения универсальной компетенции	Планируемые результаты освоения соответствующих дисциплин (модулей), практик[1]	
				Дисциплина	Результаты
Системное и критическое мышление	УК-1	Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1 Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними	Б1.О.01 Философия	Знать: сущность и основы философии как науки, основное содержание философских понятий и категорий, основные направления в философии; Уметь: применять системный подход для решения поставленных задач, оценивать надежность источников информации; Владеть: навыками критического анализа проблемных ситуаций, навыками использования логико□ методологического инструментария в процессе философского осмысления мира, приемами организации общения и совместной работы в группах и коллективах, учета социальных, этнических, конфессиональных и культурных различий входящих в них индивидов
				Б2.О.01(У) Учебная практика (экспериментальн о-	Знать: - цели, задачи, принципы и ос□ новные направления обеспече□ ния информационной безопасно□ сти; - основные

[1] Заполняются в соответствии с рабочими программами дисциплин (модулей), практик (без учета элективных и факультативных дисциплин (модулей))

				исследовательская)	термины по пробле□ мам информационной безопас□ ности;- роль и место информационной безопасности в системе нацио□ нальной безопасности страны; - угрозы информационной без□ опасности государства. Уметь: - проводить сбор, обработку, анализ и систематизацию научно-технической информа□ ции; - пользоваться современной научно-технической информа□ цией по исследуемым пробле□ мам и задачам; - оценивать информационные риски в информационных систе□ мах. Владеть:- методами обработки и анализа научно-технической информа□ цией по исследуемым пробле□ мам и задачам; - методами оценки информаци□ онных рисков.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - цели, задачи, принципы и основ□ ные направления обеспечения ин□ формационной безопасности; - основные термины по проблемам информационной безопасности; - роль и место информационной безопасности в системе нацио□ нальной безопасности страны; - угрозы информационной безопас□ ности государства. Уметь: - проводить сбор, обработку, ана□ лиз и систематизацию научно-тех□ нической информации; - пользоваться современной научно-технической информацией по исследуемым проблемам и за□ дачам; - оценивать информационные риски в информационных систе□ мах. Владеть:- методами обработки и анализа научно-технической информацией по исследуемым проблемам и за□ дачам; - методами оценки информацион□ ных рисков
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - цели, задачи, принципы и ос□ новные направления обеспе□ чения информационной без□ опасности; - основные термины по про□ блемам информационной без□ опасности;- роль и место информацион□ ной безопасности в системе национальной безопасности страны; - угрозы информационной без□ опасности государства. Уметь: - проводить сбор, обработку, анализ и систематизацию научно-технической информа□ ции; - пользоваться современной научно-технической информа□ цией по исследуемым пробле□ мам и задачам; - оценивать информационные риски в информационных си□ стемах. Владеть:-

					методами обработки и ана□лиза научно-технической ин□формацией по исследуемым проблемам и задачам; - методами оценки информа□ционных рисков.
			УК-1.2 Используя логико-методологический инструментарий, критически оценивает надежность источников информации, анализирует классические и современные философские концепции, определяет возможности их применения для выработки стратегии и разрешения проблемных ситуаций	Б1.О.01 Философия	Знать: сущность и основы философии как науки, основное содержание философских понятий и категорий, основные направления в философии; Уметь: применять системный подход для решения поставленных задач, оценивать надежность источников информации; Владеть: навыками критического анализа проблемных ситуаций, навыками использования логико□методологического инструментария в процессе философского осмысления мира, приемами организации общения и совместной работы в группах и коллективах, учета социальных, этнических, конфессиональных и культурных различий входящих в них индивидов
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - цели, задачи, принципы и основ□ные направления обеспечения ин□формационной безопасности; - основные термины по проблемам информационной безопасности; - роль и место информационной безопасности в системе нацио□нальной безопасности страны; - угрозы информационной безопас□ности государства. Уметь: - проводить сбор, обработку, ана□лиз и систематизацию научно-тех□нической информации; - пользоваться современной научно-технической информацией по исследуемым проблемам и за□дачам; - оценивать информационные риски в информационных систе□мах. Владеть: - методами обработки и анализа научно-технической информацией по исследуемым проблемам и за□дачам; - методами оценки информацион□ных рисков
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - цели, задачи, принципы и ос□новные направления обеспе□чения информационной без□опасности; - основные термины по про□блемам информационной без□опасности;- роль и место информацион□ной безопасности в системе национальной безопасности страны; - угрозы информационной без□опасности государства. Уметь: - проводить сбор, обработку, анализ и систематизацию научно-технической информа□ции; -

					пользоваться современной научно-технической информа□ цией по исследуемым пробле□ мам и задачам; - оценивать информационные риски в информационных си□ стемах. Владеть: - методами обработки и ана□ лиза научно-технической ин□ формацией по исследуемым проблемам и задачам; - методами оценки информа□ ционных рисков.
			УК-1.3 Анализирует возможные варианты разрешения проблемной ситуации, критически оценивая их достоинства и недостатки	Б1.О.01 Философия	Знать: сущность и основы философии как науки, основное содержание философских понятий и категорий, основные направления в философии; Уметь: применять системный подход для решения поставленных задач, оценивать надежность источников информации; Владеть: навыками критического анализа проблемных ситуаций, навыками использования логико□ методологического инструментария в процессе философского осмысления мира, приемами организации общения и совместной работы в группах и коллективах, учета социальных, этнических, конфессиональных и культурных различий входящих в них индивидов
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - цели, задачи, принципы и ос□ новные направления обеспе□ чения информационной без□ опасности; - основные термины по про□ блемам информационной без□ опасности; - роль и место информацион□ ной безопасности в системе национальной безопасности страны; - угрозы информационной без□ опасности государства. Уметь: - проводить сбор, обработку, анализ и систематизацию научно-технической информа□ ции; - пользоваться современной научно-технической информа□ цией по исследуемым пробле□ мам и задачам; - оценивать информационные риски в информационных си□ стемах. Владеть: - методами обработки и ана□ лиза научно-технической ин□ формацией по исследуемым проблемам и задачам; - методами оценки информа□ ционных рисков.
Разработка и реализация проектов	УК-2	Способен управлять проектом на всех этапах его жизненного	УК-2.1. Формулирует конкретную, специфичную, измеримую во времени и пространстве цель, а	Б1.О.09 Проектный менеджмент	Знание истории и основ организации деятельности предприятий, теории менеджмента, концепций мотивации, основ контроля и управления производством и коллективом Умение организовывать коллектив, рабочую группу и управлять им, используя принципы

		цикла	также определяет дорожную карту движения к цели, исходя из имеющихся ресурсов и ограничений.		мотивации, контроля, учитывая особенности организации Владение экономическими,организационно□ административными методы и социально-психологическими методами управления
			УК-2.2. Проектирует решение конкретной задачи с учетом возможных ограничений действующих правовых норм. Составляет иерархическую структуру работ, распределяет по задачам финансовые и трудовые ресурсы, использует актуальное ПО.	Б1.О.09 Проектный менеджмент	Знание истории и основ организации деятельности предприятий, теории менеджмента, концепций мотивации, основ контроля и управления производством и коллективом Умение организовывать коллектив, рабочую группу и управлять им, используя принципы мотивации, контроля, учитывая особенности организации Владение экономическими,организационно□ административными методы и социально-психологическими методами управления
			УК-2.3. Проектирует смету и бюджет проекта, оценивает эффективность результатов проекта	Б1.О.09 Проектный менеджмент	Знание истории и основ организации деятельности предприятий, теории менеджмента, концепций мотивации, основ контроля и управления производством и коллективом Умение организовывать коллектив, рабочую группу и управлять им, используя принципы мотивации, контроля, учитывая особенности организации Владение экономическими,организационно□ административными методы и социально-психологическими методами управления
			УК-2.4. Составляет матрицу ответственности и матрицу коммуникаций проекта.	Б1.О.09 Проектный менеджмент	Знание истории и основ организации деятельности предприятий, теории менеджмента, концепций мотивации, основ контроля и управления производством и коллективом Умение организовывать коллектив, рабочую группу и управлять им, используя принципы мотивации, контроля, учитывая особенности организации Владение экономическими,организационно□ административными методы и социально-психологическими методами управления
			УК-2.5. Использует гибкие технологии для реализации задач с изменяющимися во времени параметрами.	Б1.О.09 Проектный менеджмент	Знание истории и основ организации деятельности предприятий, теории менеджмента, концепций мотивации, основ контроля и управления производством и коллективом Умение организовывать коллектив, рабочую группу и управлять им, используя принципы мотивации, контроля, учитывая особенности организации Владение экономическими,организационно□ административными

					методы и социально-психологическими методами управления
Командная работа и лидерство	УК-3	Способен организовывать и руководить работой команды,вырабатывая для достижения поставленной цели	УК-3.1. Планирует организацию работы команды и руководство ею с учетом индивидуально-психологических особенностей каждого ее члена.	Б1.О.07 Современные теории и технологии развития личности	Знать: теоретико-психологические основы командной работы и руководства ею, основные командные стратегии и способы их выработки, ведущие командные роли, в том числе лидерские; Уметь: понимать, анализировать, объяснять и интерпретировать с позиций психологических теорий и концепций принципы и особенности руководства работой команды; выявлять интересы, особенности поведения и личности членов команды для правильного распределения командных ролей, в том числе лидерских; вырабатывать конструктивные стратегии взаимодействия и на их основе формировать команду; Владеть: навыками применения знаний психологических теорий и концепций для научного объяснения принципов и особенностей руководства работой команды; использования психодиагностических методов, методик и психотехнологий в соответствии с целями командной работы, распределения командных ролей, в том числе лидерских; проведения дискуссий по заданной теме; целеполагания и формирования командной стратегии для достижения поставленной цели.в на основе учета интересов всех сторон
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - законы и принципы эффектив□ ного общения с разными типами аудиторий и собеседников; - основные категории и понятия речевого воздействия; - общую схему речевого воздей□ ствия, законы эффективной ком□ муникации;- причины неэффективной ком□ муникации. Уметь:- вырабатывать умения и навыки решения в различных коммуни□ кативных задачах; - достигать коммуникативной цели и оценивать результаты своей речевой деятельности; - реализовать обмен информа□ цией в устной и письменной фор□ мах; - использовать язык для установ□ ления адекватных межличност□ ных и конвенциальных отноше□ ний в профессиональной среде; - логически верно, аргументиро□ ванно и ясно строить устную и письменную речь;- эффективно общаться в устной и письменной формах с

					соблю□дением норм культуры речи. Владеть:- навыками общения в професси□ональной деятельности и работы с технической документацией; - практическими навыками эф□фективной коммуникации; - навыками подготовки текста в соответствии с требованиями ри□торики; - приемами эффективного вер□бального и невербального взаи□модействия с партнерами для решения задач межличностного и межкультурного взаимодей□ствия
			УК-3.2. Вырабатывает конструктивную командную стратегию для достижения поставленной цели.	Б1.О.07 Современные теории и технологии развития личности	Знать: теоретико-психологические основы командной работы и руководства ею, основные командные стратегии и способы их выработки, ведущие командные роли, в том числе лидерские; Уметь: понимать, анализировать, объяснять и интерпретировать с позиций психологических теорий и концепций принципы и особенности руководства работой команды; выявлять интересы, особенности поведения и личности членов команды для правильного распределения командных ролей, в том числе лидерских; вырабатывать конструктивные стратегии взаимодействия и на их основе формировать команду; Владеть: навыками применения знаний психологических теорий и концепций для научного объяснения принципов и особенностей руководства работой команды; использования психодиагностических методов, методик и психотехнологий в соответствии с целями командной работы, распределения командных ролей, в том числе лидерских; проведения дискуссий по заданной теме; целеполагания и формирования командной стратегии для достижения поставленной цели.в на основе учета интересов всех сторон
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - законы и принципы эффектив□ного общения с разными типами аудиторий и собеседников; - основные категории и понятия речевого воздействия; - общую схему речевого воздей□ствия, законы эффективной ком□муникации;- причины неэффективной ком□муникации. Уметь:- вырабатывать умения и навыки решения в различных коммуни□кативных задачах; - достигать коммуникативной цели и оценивать результаты своей

					речевой деятельности; - реализовать обмен информа□цией в устной и письменной фор□мах; - использовать язык для установ□ления адекватных межличност□ных и конвенциальных отноше□ний в профессиональной среде; - логически верно, аргументиро□ванно и ясно строить устную и письменную речь; - эффективно общаться в устной и письменной формах с соблю□дением норм культуры речи. Владеть:- навыками общения в професси□ональной деятельности и работы с технической документацией; - практическими навыками эф□фективной коммуникации; - навыками подготовки текста в соответствии с требованиями ри□торики; - приемами эффективного вер□бального и невербаљного взаи□модействия с партнерами для решения задач межличностного и межкультурного взаимодей□ствия
			УК-3.3. Эффективно взаимодействует с участниками образовательного процесса, соблюдая психологически обоснованные правила и нормы общения.	Б1.О.07 Современные теории и технологии развития личности	Знать: теоретико-психологические основы командной работы и руководства ею, основные командные стратегии и способы их выработки, ведущие командные роли, в том числе лидерские; Уметь: понимать, анализировать, объяснять и интерпретировать с позиций психологических теорий и концепций принципы и особенности руководства работой команды; выявлять интересы, особенности поведения и личности членов команды для правильного распределения командных ролей, в том числе лидерских; вырабатывать конструктивные стратегии взаимодействия и на их основе формировать команду; Владеть: навыками применения знаний психологических теорий и концепций для научного объяснения принципов и особенностей руководства работой команды; использования психодиагностических методов, методик и психотехнологий в соответствии с целями командной работы, распределения командных ролей, в том числе лидерских; проведения дискуссий по заданной теме; целеполагания и формирования командной стратегии для достижения поставленной цели.в на основе учета интересов всех сторон
				Б2.О.01(У) Учебная практика	Знать: - законы и принципы эффектив□ного общения с разными

				(экспериментальн о-исследовательска я)	типами аудиторий и собеседников; - основные категории и понятия речевого воздействия; - общую схему речевого воздей□ствия, законы эффективной ком□ муникации;- причины неэффективной ком□ муникации. Уметь:- вырабатывать умения и навыки решения в различных коммуни□ кативных задачах; - достигать коммуникативной цели и оценивать результаты своей речевой деятельности; - реализовать обмен информа□ цией в устной и письменной фор□ мах; - использовать язык для установ□ ления адекватных межличност□ ных и конвенциальных отноше□ ний в профессиональной среде; - логически верно, аргументиро□ ванно и ясно строить устную и письменную речь; - эффективно общаться в устной и письменной формах с соблю□ дением норм культуры речи. Владеть:- навыками общения в професси□ ональной деятельности и работы с технической документацией; - практическими навыками эф□ фективной коммуникации; - навыками подготовки текста в соответствии с требованиями ри□ торики; - приемами эффективного вер□ бального и невербального взаи□ модействия с партнерами для решения задач межличностного и межкультурного взаимодей□ ствия
Коммуникация	УК-4	Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1. Выбирает на иностранном языке коммуникативно приемлемые стратегии академического и профессионального общения.	Б1.О.03 Иностранный язык	Знать: различия в стилях речи (разговорный, нейтральный, официально-деловой) Уметь: оформлять речевое высказывание в соответствии с нормами стиля, определяемыми конкретной ситуацией иноязычного общения Владеть: умениями вербального и невербального иноязычного общения в деловой (академической) сфере
			УК-4.2. Владеет культурой письменного и устного оформления профессионально ориентированного научного текста на государственном языке РФ.	Б1.О.06 Коммуникативные технологии профессионального общения	Знать требования, предъявляемые к письменной и устной речи в деловой и научной сферах, правила оформления профессионально ори□ ентированного научного текста на государственном языке РФ Уметь создавать и редактировать профессионально ориентированные и академические тексты Владеть культурой письменного и устного оформления профессионально ориентированного научного текста на государственном языке РФ

			УК-4.3. Умеет вести устные деловые переговоры в процессе профессионального взаимодействия на государственном языке РФ.	Б1.О.06 Коммуникативные технологии профессионального общения	Знать специфику подготовки и проведения деловых переговоров, вербальные и невербальные особенности коммуникативного поведения Уметь моделировать сценарии переговоров, выстраивать эффективную коммуникацию для достижения целей переговорного процесса Владеть технологиями и приемами проведения деловых переговоров
			УК-4.4. Аргументировано и конструктивно отстаивает свои позиции и идеи в академических и профессиональных дискуссиях на государственном языке РФ.	Б1.О.06 Коммуникативные технологии профессионального общения	Знать специфику деловой коммуникации, технологий речевого воздействия, особенности эффективного общения, коммуникативные законы, правила поведения в конфликтных ситуациях Уметь устранять коммуникативные барьеры, аргументированно и конструктивно отстаивать свои идеи и позиции в академических и про□ фессиональных дискуссиях. Владеть коммуникативными стратегиями, тактиками и навыками речевого воздействия в академических и профессиональных дискуссиях
			УК-4.5. Владеет интегративными коммуникативными умениями в устной и письменной иноязычной речи в ситуациях академического и профессионального общения.	Б1.О.03 Иностранный язык	Знать: особенности устной и письменной иноязычной речи Уметь: оформлять речевое высказывание в соответствии с фонетическими, лексико□ грамматическими и др. языковыми нормами Владеть: умениями осуществлять информационный поиск и использовать его результаты для решения конкретной коммуникативной задачи, строить монологические высказывания разных типов, поддерживать диалогическое взаимодействие
			УК-4.6. Выбирает на государственном языке коммуникативно приемлемые стратегии академического и профессионального общения.	Б1.О.06 Коммуникативные технологии профессионального общения	Знать: нормы русского литературного языка, правила речевого воздействия, принятые в сферах академического и профес□ сионального общения Уметь: выбирать коммуникативно приемлемые стратегии академического и профе□ ссионального общения; выбирать стиль делового общения, применять вербальные и невербальные средства при взаимодействии с партнерами Владеть: коммуникативными приемами, принятыми в сферах академического и профессионального общения

Межкультурное взаимодействие	УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	УК-5.1. Анализирует историко-культурные традиции различных социальных групп, опираясь на знание этапов исторического развития России (включая основные события, основных исторических деятелей) в контексте мировой истории и ряда культурных традиций мира (в зависимости от среды и задач образования).	Б1.О.02 История России	Владеть навыками анализа причинно-следственных связей в развитии российского государства и общества, места человека в историческом процессе и политической организации общества, навыками уважительного и бережного отношения к историческому наследию и культурным традициям России
			УК-5.2. Выделяет специфические черты и маркеры разных культур, религий, с последующим использованием полученных знаний в профессиональной деятельности и межкультурной коммуникации.	Б1.О.02 История России	Владеть навыками анализа причинно-следственных связей в развитии российского государства и общества, места человека в историческом процессе и политической организации общества, навыками уважительного и бережного отношения к историческому наследию и культурным традициям России
			УК-5.3. Ориентируется в основных этапах развития истории и культуры России и ее достижениях, учитывает особенности российской цивилизации при взаимодействии с представителями различных культур, оценивая потенциальные вызовы и риски.	Б1.О.12 Основы российской государственности	Владеть навыками анализа причинно-следственных связей в развитии российского государства и общества, места человека в историческом процессе и политической организации общества, навыками уважительного и бережного отношения к историческому наследию и культурным традициям России

			УК-5.4.1 Осознает свою гражданскую идентичность как принадлежность к государству, обществу, культурному наследию страны, ответственность за будущее страны; проявляет активную гражданскую позицию	Б1.В.ДВ.01.05 Общественный проект «Обучение служением»	
Самоорганизация и саморазвитие (в том числе здоровьесбережение)	УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки и образования в течение всей жизни	УК-6.1. Оценивает свои личностные ресурсы на основе самодиагностики, самооценки и принципов образования в течение всей жизни	Б1.О.07 Современные теории и технологии развития личности	Знать: теоретико-психологические основы развития и саморазвития личности; методические процедуры тестирования; критерии подбора психодиагностических методов и методик для определения самооценки, выбора адекватных психотехнологий самоорганизации и саморазвития; Уметь: понимать, анализировать, объяснять и интерпретировать с позиций психологических теорий и концепций механизмы развития и саморазвития личности; выявлять психологические особенности личности, ее черт, познавательной сферы, самосознания; планировать, организовывать и проводить психологическое обследование (самообследование) для последующего саморазвития, адекватно представлять полученные данные в психодиагностическом заключении; Владеть: навыками применения знаний психологических теорий и концепций для научного объяснения принципов развития и саморазвития личности; использования психодиагностических методов, методик и психотехнологий для определения временно́й перспективы, самооценки личностного потенциала и его коррекции; целеполагания на основе определения приоритетов профессиональной деятельности, самоорганизации и саморазвития, корректировки планов с учетом имеющихся ресурсов
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - закономерности усвоения че□ ловеком социального опыта и его активного воспроизводства и саморазвития через форми□ рование систем установок и ценностей;- психологические основы управления временем; - инструменты и методы

					управления временем; - этапы, порядок проведения работ оп обеспечению инфор□мационной безопасности объ□ектов и систем; - модели жизненного цикла проекта. Уметь - ориентироваться в условиях избытка информации, выде□лять ключевые приоритеты и следовать им; - проводить анализ поставлен□ных задач для декомпозиции на более простые подзадачи. - оценивать актуальность соб□ственных знаний и навыков с точки зрения требований рынка труда. Владеть: - методиками саморазвития, самостоятельного приобрете□ния и освоения новых знаний; - навыками критической оценки своих достоинств и не□достатков; - опытом выбора средств и возможностей развития досто□инств и устранения недостат□ков; - навыками планирования и распределения времени и дру□гих ресурсов при решении по□ставленных задач.
			УК-6.2. Определяет и реализовывает приоритеты своей деятельности и способы ее совершенствования	Б1.О.07 Современные теории и технологии развития личности	Знать: теоретико-психологические основы развития и саморазвития личности; методические процедуры тестирования; критерии подбора психодиагностических методов и методик для определения самооценки, выбора адекватных психотехнологий самоорганизации и саморазвития; Уметь: понимать, анализировать, объяснять и интерпретировать с позиций психологических теорий и концепций механизмы развития и саморазвития личности; выявлять психологические особенности личности, ее черт, познавательной сферы, самосознания; планировать, организовывать и проводить психологическое обследование (самообследование) для последующего саморазвития, адекватно представлять полученные данные в психодиагностическом заключении; Владеть: навыками применения знаний психологических теорий и концепций для научного объяснения принципов развития и саморазвития личности; использования психодиагностических методов, методик и психотехнологий для определения временно́й перспективы, самооценки личностного потенциала и его коррекции; целеполагания на основе определения приоритетов профессиональной деятельности, самоорганизации и

					саморазвития, корректировки планов с учетом имеющихся ресурсов
	УК-7	Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Выбирает здоровьесберегающие технологии для поддержания здорового образа жизни с учетом физиологических особенностей организма.	Б1.О.05 Физическая культура и спорт	Знать: научно-практические основы физической культуры и здорового образа жизни Уметь: творчески использовать средства и методы физического воспитания для поддержания должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры для успешной социальной и профессиональной деятельности
			УК-7.2. Планирует свое рабочее и свободное время для оптимального сочетания физической и умственной нагрузки и обеспечения работоспособности.	Б1.О.05 Физическая культура и спорт	Знать: научно-практические основы физической культуры и здорового образа жизни Уметь: творчески использовать средства и методы физического воспитания для поддержания должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры для успешной социальной и профессиональной деятельности
			УК-7.3. Соблюдает и пропагандирует нормы здорового образа жизни в различных жизненных ситуациях и в профессиональной деятельности.	Б1.О.05 Физическая культура и спорт	Знать: научно-практические основы физической культуры и здорового образа жизни Уметь: творчески использовать средства и методы физического воспитания для поддержания должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры для успешной социальной и профессиональной деятельности

			УК-7.4. Осуществляет выбор вида спорта или системы физических упражнений для физического самосовершенствования, развития профессионально важных психофизических качеств и способностей в соответствии со своими индивидуальными способностями и будущей профессиональной деятельностью	Б1.В.07 **Элективные дисциплины по физической культуре и спорту (модуль)**	Знать: научно-практические основы физической культуры и здорового образа жизни Уметь: творчески использовать средства и методы физического воспитания для поддержания должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры для успешной социальной и профессиональной деятельности
			УК-7.5. Использует методику самоконтроля для определения уровня здоровья и физической подготовленности в соответствии с нормативными требованиями и условиями будущей профессиональной деятельности.	Б1.В.07 **Элективные дисциплины по физической культуре и спорту (модуль)**	Знать: научно-практические основы физической культуры и здорового образа жизни Уметь: творчески использовать средства и методы физического воспитания для поддержания должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры для успешной социальной и профессиональной деятельности
			УК-7.6. Приобретает личный опыт повышения двигательных и функциональных возможностей организма, обеспечивающий специальную физическую подготовленность в профессиональной деятельности.	Б1.В.07 **Элективные дисциплины по физической культуре и спорту (модуль)**	Знать: научно-практические основы физической культуры и здорового образа жизни Уметь: творчески использовать средства и методы физического воспитания для поддержания должного уровня физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности Владеть: средствами и методами укрепления индивидуального здоровья, физического самосовершенствования, ценностями физической культуры для успешной социальной и профессиональной деятельности

Безопасность жизнедеятельности	УК-8	Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.1. Идентифицирует и анализирует опасные и вредные факторы элементов среды обитания и в рамках осуществляемой деятельности; знает основные вопросы безопасности жизнедеятельности.	Б1.О.04 Безопасность жизнедеятельности	знать: основные подходы к оп□ределению, изучению и понима□ нию содержания, роли и значе□ ния здоровья издоровом образе жизни, способах обеспечения техносферной, информационной и психологической безопасности личности; государственной сис□ теме защиты населения и её правовых рамках; уметь: выявлять важные компо□ ненты обеспечения безопасно сти жизнедеятельности; форму□ лировать требования, предъяв□ ляемые к безопасности общест□ ва и среды обучения (прожива□ ния) в большом городе; верифи□ цировать полученную информа□ цию и обрабатывать ее, ком□ плексно оценивая проблемные ситуации или процессы, соблю□ дать адекватные нормы и пра□ вила безопасности при осущест□ влении последующей профес□ сиональной деятельности; рас□ познавать и оценивать опасные для жизни и общества ситуации и риски; владеть (иметь навык(и)): раз□ витие черт личности, необходи□ мых для безопасного поведения, как в чрезвычайных ситуациях, так и повседневной жизни в большом городе; соблюдения здорового образа жизни;
			УК-8.2. Способен осуществлять действия по предотвращению возникновения чрезвычайных ситуаций природного, техногенного, социального (биолого-социального) происхождения; грамотно действовать в чрезвычайных ситуациях мирного и военного времени, создавать безопасные условия реализации профессиональной деятельности.	Б1.О.04 Безопасность жизнедеятельности	знать: классификацию ЧС, ос□ новные правила безопасного поведения человека в чрезвы□ чайных ситуациях природного, техногенного, социального и биолого-социального характера мирного и военного времени; уметь: грамотно действовать при различных ЧС и использо□ вать средства индивидуальной и коллективной защиты; владеть (иметь навык(и)): раз□ витие черт личности, необходи□ мых для безопасного поведения, как в чрезвычайных ситуациях, так и повседневной жизни в большом городе;

			УК-8.3. Готов принимать участие в оказании первой и экстренной допсихологической помощи при травмах и неотложных состояниях, в том числе в условиях чрезвычайных ситуаций в мирное и военное время.	Б1.О.04 Безопасность жизнедеятельности	знать: универсальный алгоритм оказания первой помощи, основ□ ные приемы и правила оказания первой помощи при неотложных состояниях; приемы экстренной допсихологической помощи; уметь: действовать и использо□ вать средства индивидуальной и коллективной защиты; оценить состояние пораженных и оче□ редность оказания помощи; владеть (иметь навык(и)): навы□ ками самостоятельно применять меры помощи пострадавшим при неотложных состояниях в экс□ тремальных ситуациях; пра□ вильно использовать табельные медицинские средства индиви□ дуальной защиты; способностью участвовать в спасательных ме□ роприятиях в случае возникно вения чрезвычайных ситуаций;
			УК-8.4. Способен обеспечить безопасные и/или комфортные условия труда на рабочем месте, в том числе с помощью средств защиты; выявить и устранить проблемы, связанные с нарушениями техники безопасности на рабочем месте.	Б1.О.04 Безопасность жизнедеятельности	знать: правила по охране труда, основы трудового законодатель□ ства РФ; основные подходы к определению, изучению и пони□ манию содержания, роли и зна□ чения безопасного поведения человека; уметь: создавать и поддержи□ вать безопасные условия жизне□ деятельности; соблюдать адек□ ватные нормы и правила безо□ пасности при осуществлении последующей профессиональ□ ной деятельности; использовать средства индивидуальной и кол□ лективной защиты; владеть (иметь навык(и)): соз□ дания и поддержки безопасных условий жизнедеятельности: основными правилами и мето□ дами обеспечения техники безо□ пасности
Экономическая культура, в том числе финансовая грамотность	УК-9	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Понимает базовые принципы функционирования экономики.	Б1.О.10 Экономика и финансовая грамотность	Знает: • базовые экономические понятия: экономические ресурсы, товары и услуги, спрос, предложение, доходы, расходы, цена, деньги, прибыль, процент, риск, собственность, рынок, фирма, домохозяйство, государство, налоги, трансферы, инфляция, валовой внутренний продукт, экономический рост, сбережения, инвестиции и др.); • базовые принципы функционирования экономики (законы спроса и предложения, принципы ценообразования, принцип альтернативных издержек, принцип изменения ценности денег во времени и др.); • предпосылки поведения экономических агентов: теоретические принципы рационального выбора (максимизация полезности) и отклонения

					от рационального поведения (ограниченная рациональность, поведенческие эффекты, эвристики, и систематические ошибки, с ними связанные). Умеет: • воспринимать и анализировать информацию, необходимую для принятия обоснованных решений в сфере личных финансов.
			УК-9.2. Понимает основные виды государственной социально-экономической политики и их влияние на индивида.	Б1.О.10 Экономика и финансовая грамотность	Знает: • цели, задачи, инструменты и эффекты экономической политики государства, понятие и факторы экономического роста; • базовые принципы и инструменты бюджетной, налоговой, денежно-кредитной, антимонопольной, конкурентной, социальной, пенсионной политики государства, осознает ее влияние на индивида (права, обязанности, риски, влияние на доходы и расходы); Умеет: • пользоваться налоговыми и социальными льготами, формировать личные пенсионные накопления
			УК-9.3. Использует финансовые инструменты для управления личными финансами (личным бюджетом).	Б1.О.10 Экономика и финансовая грамотность	Знает: • основные финансовые институты (Банк России, Агентство по страхованию вкладов, Пенсионный фонд России, коммерческий банк, страховая организация, брокер, биржа, негосударственный пенсионный фонд, паевой инвестиционный фонд, микрофинансовая организация, кредитный потребительский кооператив, ломбард, и др.) и принципы взаимодействия индивида с ними; • основные инструменты управления личными финансами (банковский вклад, кредит (заём), ценные бумаги, инвестиционные фонды, драгоценности, недвижимость, валюта), способы определения их доходности, надежности, ликвидности, влияние на доходы и расходы индивида; • источники информации об инструментах управления личными финансами, правах и обязанностях потребителя финансовых услуг; • о существовании недобросовестных практик на рынке финансовых услуг (мошенничество, обман и др.) и способах защиты от них. Умеет: • пользоваться основными расчётными инструментами (наличные, безналичные, электронные денежные средства), предотвращать возможное мошенничество; • выбирать инструменты управления личными финансами для достижения поставленных финансовых целей, сравнивать их по критериям доходности, надежности и

					ликвидности
			УК-9.4. Применяет методы личного экономического и финансового планирования для достижения поставленных целей.	Б1.О.10 Экономика и финансовая грамотность	Знает: • основные виды личных доходов (оплата труда, доходы от предпринимательской деятельности, от собственности, владения финансовыми инструментами, заимствования, наследство и др.), механизмы их получения и увеличения; • основные виды расходов, механизмы их снижения, способы формирования сбережений; • принципы и технологии ведения личного бюджета. Умеет: • решать типичные задачи в сфере личного экономического и финансового планирования, возникающие на всех этапах жизненного цикла индивида (выбрать товар или услугу с учетом реальных финансовых возможностей, найти работу и согласовать с работодателем условия контракта, рассчитать процентные ставки, определить целесообразность взятия кредита, определить способ хранения или инвестирования временно свободных денежных средств, определить целесообразность страхования и др.); • вести личный бюджет, используя существующие программные продукты.
			УК-9.5. Контролирует собственные экономические и финансовые риски.	Б1.О.10 Экономика и финансовая грамотность	Знает: – понятия риск и неопределенность, осознает неизбежность риска и неопределенности в экономической и финансовой сфере; – виды и источники возникновения экономических и финансовых рисков для индивида, способы их оценки и снижения; – основные виды страхования и ключевые параметры страховых договоров. Умеет: • оценивать индивидуальные риски, связанные с экономической деятельностью и использованием инструментов управления личными финансами • использовать способы снижения индивидуальных рисков; • анализировать предложения страховых компаний.
Гражданская позиция	УК-10	Способен формировать нетерпимое отношение к коррупционном	УК-10.1. Соблюдает антикоррупционные стандарты поведения, выявляет коррупционные риски, противодействует	Б1.О.08 Правовые и организационные основы противодействия противоправному поведению	Знать: понятие коррупции, признаки и виды коррупционного поведения; требования антикоррупционного законодательства. Уметь: выявлять и оценивать коррупционное поведение, коррупционные риски в профессиональной деятельности,

		у поведению	коррупционному поведению в профессиональной деятельности.		принимать решения в соответствии с требованием антикоррупционного законодательства. Владеть: навыками по пресечению коррупционного поведения в профессиональной деятельности в соответствии с требованиями антикоррупционного законодательства
			УК-10.2. Поддерживает высокий уровень личной и правовой культуры, выявляет проявления экстремистской идеологии и противодействует им в профессиональной деятельности..	Б1.О.08 Правовые и организационные основы противодействия противоправному поведению	Знать: понятие коррупции, признаки и виды коррупционного поведения; требования антикоррупционного законодательства. Уметь: выявлять и оценивать коррупционное поведение, коррупционные риски в профессиональной деятельности, принимать решения в соответствии с требованием антикоррупционного законодательства. Владеть: навыками по пресечению коррупционного поведения в профессиональной деятельности в соответствии с требованиями антикоррупционного законодательства
			УК-10.3. Идентифицирует правонарушения террористической направленности, противодействует проявлениям терроризма в профессиональной деятельности.	Б1.О.08 Правовые и организационные основы противодействия противоправному поведению	Знать: понятие коррупции, признаки и виды коррупционного поведения; требования антикоррупционного законодательства. Уметь: выявлять и оценивать коррупционное поведение, коррупционные риски в профессиональной деятельности, принимать решения в соответствии с требованием антикоррупционного законодательства. Владеть: навыками по пресечению коррупционного поведения в профессиональной деятельности в соответствии с требованиями антикоррупционного законодательства

— общепрофессиональные компетенции:

Категория компетенций	**Код**	**Формулировка компетенции**	**Код и формулировка индикатора достижения компетенции**	**Планируемые результаты освоения соответствующих дисциплин (модулей), практик[2]**	
				Дисциплина	**Результаты**
	ОПК-1	Способен оценивать роль информации,	ОПК-1.1. Знает основные средства и способы обеспечения	Б1.О.11 Введение в специальность	Знает основные понятия об информации как предмете защиты. Знает принципы и модели взаимодействия «открытых» систем, информационно□ вычислительных систем. Знает основные угрозы

[2] Заполняются в соответствии с рабочими программами дисциплин (модулей), практик (без учета элективных и факультативных дисциплин (модулей))

		информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	информационной безопасности, принципы построения систем защиты информации.		безопасности информации, обрабатываемой в компьютерных системах. Знает методы и средства защиты информации. Имеет представление о технических каналах утечки информации; каналах перехвата при передаче информации системами связи; каналы утечки акустической и видовой информации; компьютерные методы съёма информации. Знает технические, правовые и организационные методы и средства защиты информации. Знает стандарты шифрования, хэширования, и цифровой подписи
				Б1.О.39 Основы информационной безопасности	знать: сущность и понятие информацион□ ной безопасности, характеристику ее со□ ставляющих; уметь: классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; владеть: навыками определения основ□ ных угроз безопасности информации
			ОПК-1.2. Знает классификацию защищаемой информации по видам тайны и степеням конфиденциальности.	Б1.О.39 Основы информационной безопасности	знать: место информационной безопас□ ности в системе национальной безопас□ ности страны; источники угроз информа□ ционной безопасности и меры по их предотвращению; уметь: определять основные угрозы национальной безопасности, связанные с информационной безопасностью; владеть: основами государственной ин□ формационной политики
			ОПК-1.3. Знает классификацию и основные угрозы информационной безопасности для объекта информатизации.	Б1.О.39 Основы информационной безопасности	знать: основные источники угроз без□ опасности информации; уметь: анализировать возможные источ□ ники угроз безопасности информации; владеть: практическими навыками клас□ сификации потенциально опасных угроз информационной безопасности.
	ОПК-2	Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства,	ОПК-2.1. Знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере.	Б1.О.22 Аппаратные средства вычислительной техники	Имеет представление о структурах вычислительных систем. Знает общие принципы построения и архитектуры ВТ. Знает архитектуру ВТ различного уровня. Знает особенности архитектур вычислительной техники и отдельных аппаратных средств (CISC, RISC, ARM), их применение в современных вычислительных машинах. Знает алгоритмы перевода чисел в различные системы счисления. Знает формы и форматы представления чисел в ЭВМ. Знает особенности представления в ЭВМ графической и звуковой информации. Знает принципы кодирования текстовой и числовой

		для решения задач профессиональной деятельности;			информации в ЭВМ, виды кодов. Арифметико-логические операции в ЭВМ.
				Б1.О.31 Информатика	Знает: • формы и способы представления данных в ЭВМ; • особенности машинного представления целых чисел со знаком и без знака, вещественных чисел; • особенности машинной арифметики для целых и вещественных чисел.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тическ-го и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах

					аналитической и численной оценки основных показателей эффективности алгоритмов ана□лиза данных и машинного обуче□ния;- проводить разработку простей□ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ления базами данных; - использовать основные плат□формы, технологии и инструмен□тальные программно-аппарат□ные средства для реализации информационных систем; - применять защищенные прото□колы, межсетевые экраны и средства обнаружения вторже□ний для защиты информации в сетях. Владеть: - практическими навыками при□менения специализированных программных средств, предна□значенных для обеспечения без□опасности и целостности дан□ных;- навыками составления запро□сов к базе данных;- практическими навыками разра□ботки и применения в професси□ональной деятельности крипто□графических и стеганографиче□ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ализации технических процессов жизненного цикла систем, а также соответствующим про□граммным обеспечением; - практическими навыками разра□ботки и применения алгоритмов и технологий обработки инфор□мации в части анализа данных и машинного обучения; - навыками разработки и модели□рования алгоритмов обработки информации в современных ин□струментальных средах, навы□ками проведения компьютерного эксперимента по оценке эффек□тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□терных моделей алгоритмов об□работки информации; - специализированными про□граммными средствами для реа□лизации

					стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.2. Знает логико-математические основы построения электронных цифровых устройств.	Б1.О.22 Аппаратные средства вычислительной техники	Имеет представление о видах и схемной реализации типовых узлов комбинационного и накапливающего типа. Знает назначение, виды и обозначение шифраторов, дешифраторов, сумматоров, схем сравнения, мультиплексоров. Знает основы построения и функционирования устройств с памятью, особенности анализа и синтеза элементов с памятью.
				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов

					обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□ лиза данных и машинного обуче□ ния;- проводить разработку простей□ ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных;- навыками составления запро□ сов к базе данных;- практическими навыками разра□ ботки и применения в професси□ ональной деятельности крипто□ графических и стеганографиче□ ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей

					алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.3. Знает состав, назначение аппаратных средств и программного обеспечения персонального компьютера.	Б1.О.22 Аппаратные средства вычислительной техники	Знает конструктивные и функциональные модули ЭВМ. Знает иерархическую структуру запоминающих устройств. Имеет представление об аппаратной реализации внутренней и внешней памяти, организации доступа к данным. Знает состав и назначение периферийных устройств, устройств ввода-вывода информации. Имеет представление о видах и назначении портов ПЭВМ
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками

					обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□ лиза данных и машинного обуче□ ния; - проводить разработку простей□ ших компьютерных

					моделей; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных;- навыками составления запро□ сов к базе данных;- практическими навыками разра□ ботки и применения в професси□ ональной деятельности крипто□ графических и стеганографи□ ческих алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков

			ОПК-2.4. Знает классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей.	Б1.О.22 Аппаратные средства вычислительной техники	Знает направления и средства развития АСВТ. Знает классификацию ПЭВМ. Знает обобщенную структуру ПЭВМ, технико□ экономические параметры ПЭВМ различных классов. Знает принципы построения систем контроля данных. Знает типовые структуры и принципы организации систем и сете передачи данных.
				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах

					аналитической и численной оценки основных показателей эффективности алгоритмов ана□лиза данных и машинного обуче□ния;- проводить разработку простей□ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ления базами данных; - использовать основные плат□формы, технологии и инструмен□тальные программно-аппарат□ные средства для реализации информационных систем; - применять защищенные прото□колы, межсетевые экраны и средства обнаружения вторже□ний для защиты информации в сетях. Владеть: - практическими навыками при□менения специализированных программных средств, предна□значенных для обеспечения без□опасности и целостности дан□ных; - навыками составления запро□сов к базе данных;- практическими навыками разра□ботки и применения в професси□ональной деятельности крипто□графических и стеганографиче□ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ализации технических процессов жизненного цикла систем, а также соответствующим про□граммным обеспечением; - практическими навыками разра□ботки и применения алгоритмов и технологий обработки инфор□мации в части анализа данных и машинного обучения; - навыками разработки и модели□рования алгоритмов обработки информации в современных ин□струментальных средах, навы□ками проведения компьютерного эксперимента по оценке эффек□тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□терных моделей алгоритмов об□работки информации; - специализированными про□граммными средствами для реа□лизации

					стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.5. Умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети Интернет.	Б1.О.31 Информатика	Умеет: применять типовые программные средства сервисного назначения и информационного поиска при работа на компьютере.
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б1.О.55 Дисциплины специализации	Умеет: использовать программные средства сервисного назначения для сети WWW: ping, tracert, telnet-, ssh-, ftp клиенты, web-браузер

				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□ лиза данных и машинного обуче□ ния; - проводить разработку простей□ ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; -

					формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных;- навыками составления запро□ сов к базе данных;- практическими навыками разра□ ботки и применения в професси□ ональной деятельности крипто□ графических и стеганографиче□ ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.6. Умеет составлять документы, используя прикладные программы офисного	Б1.О.31 Информатика	Умеет: работать с документами в программах Word и Excel.
				Б1.О.50 Инсталляция и настройка	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления

			назначения.	программного обеспечения	базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного

					моде□лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ных технологий, роль и место проектировщика и разработчика информационных систем в про□цессе создания сложных систем; - стандарты описания архитек□туры программного обеспечения; - основные платформы, техноло□гии и инструментальные про□граммно-аппаратные средства для реализации информацион□ных систем; - цели и задачи моделирования информационных систем с ис□пользованием современных ин□формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□печение для проведения иссле□дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□вать рекомендации по принци□пам построения и параметрам алгоритмов в области професси□ональной деятельности; - проводить синтез и анализ ал□горитмов обработки информации для решения конкретных практи□ческих задач, использовать ма□тематические методы в интере□сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□лиза данных и машинного обуче□ния; - проводить разработку простей□ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ления базами данных; - использовать основные плат□формы, технологии и инструмен□тальные программно-аппарат□ные средства для реализации информационных систем; - применять защищенные прото□колы, межсетевые экраны и средства обнаружения вторже□ний для защиты информации в сетях. Владеть: -

					практическими навыками при□менения специализированных программных средств, предна□значенных для обеспечения без□опасности и целостности дан□ных;- навыками составления запро□сов к базе данных;- практическими навыками разра□ботки и применения в професси□ональной деятельности крипто□графических и стеганографиче□ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ализации технических процессов жизненного цикла систем, а также соответствующим про□граммным обеспечением; - практическими навыками разра□ботки и применения алгоритмов и технологий обработки инфор□мации в части анализа данных и машинного обучения; - навыками разработки и модели□рования алгоритмов обработки информации в современных ин□струментальных средах, навы□ками проведения компьютерного эксперимента по оценке эффек□тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□терных моделей алгоритмов об□работки информации; - специализированными про□граммными средствами для реа□лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.7. Владеет средствами управления пользовательскими интерфейсами операционных систем.	Б1.О.31 Информатика	Имеет навыки: настройки пользовательского интерфейса при работе с ОС Windows.
				Б1.О.32 Операционные системы	Владеет средствами управления пользовательскими интерфейсами операционных систем
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные

					системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии

					и инструментальные про□граммно-аппаратные средства для реализации информацион□ных систем; - цели и задачи моделирования информационных систем с ис□пользованием современных ин□формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□печение для проведения иссле□дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□вать рекомендации по принци□пам построения и параметрам алгоритмов в области професси□ональной деятельности; - проводить синтез и анализ ал□горитмов обработки информации для решения конкретных практи□ческих задач, использовать ма□тематические методы в интере□сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□лиза данных и машинного обуче□ния; - проводить разработку простей□ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ления базами данных; - использовать основные плат□формы, технологии и инструмен□тальные программно-аппарат□ные средства для реализации информационных систем; - применять защищенные прото□колы, межсетевые экраны и средства обнаружения вторже□ний для защиты информации в сетях. Владеть: - практическими навыками при□менения специализированных программных средств, предна□значенных для обеспечения без□опасности и целостности дан□ных; - навыками составления запро□сов к базе данных; - практическими навыками разра□ботки и применения в професси□ональной деятельности крипто□графических и стеганографиче□ских алгоритмов; - навыками конфигурирования и администрирования ОС; -

					современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.8. Знает основные принципы конфигурирования и администрирования операционных систем.	Б1.О.32 Операционные системы	Знает основные принципы конфигурирования и администрирования операционных систем
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального

					назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной

					деятельности; - проводить синтез и анализ ал□горитмов обработки информации для решения конкретных практи□ческих задач, использовать ма□тематические методы в интере□сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□лиза данных и машинного обуче□ния; - проводить разработку простей□ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ления базами данных; - использовать основные плат□формы, технологии и инструмен□тальные программно-аппарат□ные средства для реализации информационных систем; - применять защищенные прото□колы, межсетевые экраны и средства обнаружения вторже□ний для защиты информации в сетях. Владеть: - практическими навыками при□менения специализированных программных средств, предна□значенных для обеспечения без□опасности и целостности дан□ных;- навыками составления запро□сов к базе данных;- практическими навыками разра□ботки и применения в професси□ональной деятельности крипто□графических и стеганографиче□ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ализации технических процессов жизненного цикла систем, а также соответствующим про□граммным обеспечением; - практическими навыками разра□ботки и применения алгоритмов и технологий обработки инфор□мации в части анализа данных и машинного обучения; - навыками разработки и модели□рования алгоритмов обработки информации в современных ин□струментальных средах, навы□ками проведения компьютерного эксперимента по оценке эффек□тивности алгоритмов анализа данных и машинного

					обучения, навыками тестирования компью□терных моделей алгоритмов об□работки информации; - специализированными про□граммными средствами для реа□лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.9. Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями.	Б1.О.32 Операционные системы	Умеет разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями
				Б1.О.35 Объектно-ориентированное программирование	Уметь: разрабатывать программы сложных информационных систем с использованием технологии объектно-ориентированного программирования
				Б1.О.36 Введение в программирование	Уметь: разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями
				Б1.О.37 Методы программирования	Уметь: разрабатывать системное и прикладное программное обеспечение для многозадачных, многопользовательских и многопроцессорных сред, а также для сред с интерфейсом, управляемым сообщениями.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - базовые понятия методов обра□ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□министского подходов; - технологии организации и про□ведения статистического компь□ютерного моделирования алго□ритмов обработки информации, возможности современных про□граммных сред для реализации исследований и разработок в об□ласти алгоритмов анализа дан□ных и машинного обучения;- роль и место средств матема□тического и имитационного моде□лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ных технологий, роль и место проектировщика и разработчика информационных систем в про□цессе создания

					сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□ лиза данных и машинного обуче□ ния; - проводить разработку простей□ ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных;- навыками составления запро□ сов к базе данных;- практическими навыками разра□ ботки и применения в професси□ ональной деятельности

					крипто□ графических и стеганографиче□ ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.10. Умеет применять основные методы программирования в выбранной операционной среде.	Б1.О.32 Операционные системы	Умеет применять основные методы программирования в выбранной операционной среде
				Б1.О.35 Объектно-ориентированное программировани е	Уметь: применять объектно□ ориентированное программирование для разработки системных программ.
				Б1.О.36 Введение в программировани е	Уметь: применять основные методы программирования в выбранной операционной среде
				Б1.О.37 Методы программировани я	Уметь: применять основные методы программирования в выбранной операционной среде.
				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;-

					роль и место средств матема□тического и имитационного моде□лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ных технологий, роль и место проектировщика и разработчика информационных систем в про□цессе создания сложных систем; - стандарты описания архитек□туры программного обеспечения; - основные платформы, техноло□гии и инструментальные про□граммно-аппаратные средства для реализации информацион□ных систем; - цели и задачи моделирования информационных систем с ис□пользованием современных ин□формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□печение для проведения иссле□дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□вать рекомендации по принци□пам построения и параметрам алгоритмов в области професси□ональной деятельности; - проводить синтез и анализ ал□горитмов обработки информации для решения конкретных практи□ческих задач, использовать ма□тематические методы в интере□сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□лиза данных и машинного обуче□ния; - проводить разработку простей□ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ногоподхода, в том числе при□менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ления базами данных; - использовать основные плат□формы, технологии и инструмен□тальные программно-аппарат□ные средства для реализации информационных систем; - применять защищенные прото□колы, межсетевые экраны и средства обнаружения

					вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных;- навыками составления запро□ сов к базе данных;- практическими навыками разра□ ботки и применения в професси□ ональной деятельности крипто□ графических и стеганографиче□ ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.11. Знает характерные особенности современного программного обеспечения специального назначения.	Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное

					обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием

					современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□ лиза данных и машинного обуче□ ния; - проводить разработку простей□ ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационньм системам; - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных;- навыками составления запро□ сов к базе данных;- практическими навыками разра□ ботки и применения в професси□ ональной деятельности крипто□ графических и стеганографиче□ ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками

					разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.12. Умеет производить установку, наладку, тестирование и обслуживание программного обеспечения, включая решения отечественного производства.	Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при

					возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ пам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□ лиза данных и машинного

					обуче□ ния; - проводить разработку простей□ ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных;- навыками составления запро□ сов к базе данных;- практическими навыками разра□ ботки и применения в професси□ ональной деятельности крипто□ графических и стеганографиче□ ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ ализации технических процессов жизненного цикла систем, а также соответствующим про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков

			ОПК-2.13. Умеет производить установку, наладку, тестирование и обслуживание сетевого программного обеспечения, включая решения отечественного производства.	Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в

					об□ ласти алгоритмов анализа дан□ ных и машинного обучения;- роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи моделирования информационных систем с ис□ пользованием современных ин□ формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□ печение для проведения иссле□ дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□ вать рекомендации по принци□ ам построения и параметрам алгоритмов в области професси□ ональной деятельности; - проводить синтез и анализ ал□ горитмов обработки информации для решения конкретных практи□ ческих задач, использовать ма□ тематические методы в интере□ сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□ лиза данных и машинного обуче□ ния;- проводить разработку простей□ ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, втом числе при□ менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ ного продукта в рамках систем□ ного подхода, в том числе при□ менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные

					прото□колы, межсетевые экраны и средства обнаружения вторже□ний для защиты информации в сетях. Владеть: - практическими навыками при□менения специализированных программных средств, предна□значенных для обеспечения без□опасности и целостности дан□ных;- навыками составления запро□сов к базе данных;- практическими навыками разра□ботки и применения в професси□ональной деятельности крипто□графических и стеганографиче□ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ализации технических процессов жизненного цикла систем, а также соответствующим про□граммным обеспечением; - практическими навыками разра□ботки и применения алгоритмов и технологий обработки инфор□мации в части анализа данных и машинного обучения; - навыками разработки и модели□рования алгоритмов обработки информации в современных ин□струментальных средах, навы□ками проведения компьютерного эксперимента по оценке эффек□тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□терных моделей алгоритмов об□работки информации; - специализированными про□граммными средствами для реа□лизации стеганографического скрытия информации и создания цифровых водяных знаков
			ОПК-2.14. Умеет производить установку, наладку, тестирование и обслуживание современных программных средств обеспечения информационной безопасности.	Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы,

					системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа данных и машинного обучения в рамках статистического и детер□ министского подходов; - технологии организации и про□ ведения статистического компь□ ютерного моделирования алго□ ритмов обработки информации, возможности современных про□ граммных сред для реализации исследований и разработок в об□ ласти алгоритмов анализа дан□ ных и машинного обучения; - роль и место средств матема□ тического и имитационного моде□ лирования при проектировании сложных систем, применяемые при этом технологии структурно - функционального и объектного визуального моделирования; - цели и задачи информацион□ ных технологий, роль и место проектировщика и разработчика информационных систем в про□ цессе создания сложных систем; - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем; - цели и задачи

					моделирования информационных систем с ис□пользованием современных ин□формационных технологий. Уметь: - использовать стандартное и оригинальное программное обес□печение для проведения иссле□дований и разработок в области алгоритмов анализа данных и машинного обучения, формиро□вать рекомендации по принци□пам построения и параметрам алгоритмов в области професси□ональной деятельности; - проводить синтез и анализ ал□горитмов обработки информации для решения конкретных практи□ческих задач, использовать ма□тематические методы в интере□сах аналитической и численной оценки основных показателей эффективности алгоритмов ана□лиза данных и машинного обуче□ния; - проводить разработку простей□ших компьютерных моделей; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - формулировать и развивать концепцию создания произволь□ного продукта в рамках систем□ного подхода, в том числе при□менительно к информационным системам; - использовать средства защиты, представляемые систем управ□ления базами данных; - использовать основные плат□формы, технологии и инструмен□тальные программно-аппарат□ные средства для реализации информационных систем; - применять защищенные прото□колы, межсетевые экраны и средства обнаружения вторже□ний для защиты информации в сетях. Владеть: - практическими навыками при□менения специализированных программных средств, предна□значенных для обеспечения без□опасности и целостности дан□ных; - навыками составления запро□сов к базе данных; - практическими навыками разра□ботки и применения в професси□ональной деятельности крипто□графических и стеганографиче□ских алгоритмов; - навыками конфигурирования и администрирования ОС; - современными подходами к ре□ализации технических процессов жизненного цикла систем, а также соответствующим

					про□ граммным обеспечением; - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки инфор□ мации в части анализа данных и машинного обучения; - навыками разработки и модели□ рования алгоритмов обработки информации в современных ин□ струментальных средах, навы□ ками проведения компьютерного эксперимента по оценке эффек□ тивности алгоритмов анализа данных и машинного обучения, навыками тестирования компью□ терных моделей алгоритмов об□ работки информации; - специализированными про□ граммными средствами для реа□ лизации стеганографического скрытия информации и создания цифровых водяных знаков
	ОПК-3	Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;	ОПК-3.1. Знает основные задачи векторной алгебры и аналитической геометрии.	Б1.О.19 Геометрия	Знать: основные задачи векторной алгебры и аналитической геометрии Уметь: решать основные задачи векторной алгебры и аналитической геометрии Владеть: основными инструментами и подходами к решению основных задач векторной алгебры и аналитической геометрии
			ОПК-3.2. Знает возможности координатного метода для исследования различных геометрических объектов.	Б1.О.19 Геометрия	Знать: возможности координатного метода для исследования различных геометрических объектов Уметь: применять на практике координатный метод для исследования различных геометрических объектов Владеть: навыками исследования различных геометрических объектов
			ОПК-3.3. Знает основные виды уравнений простейших геометрических объектов.	Б1.О.19 Геометрия	Знать: основные виды уравнений простейших геометрических объектов Уметь: получать уравнения простейших геометрических объектов, находить значения их основных параметров Владеть: навыками построения простейших геометрических объектов
			ОПК-3.4. Умеет решать основные задачи линейной алгебры.	Б1.О.23 Линейная алгебра	Знать: основные задачи линейной алгебры Уметь: решать основные задачи линейной алгебры Владеть: основными инструментами и подходами к решению основных задач линейной алгебры

			ОПК-3.5. Умеет решать основные задачи аналитической геометрии на плоскости и в пространстве.	Б1.О.19 Геометрия	Знать: основные подходы к решению задач аналитической геометрии на плоскости и в пространстве Уметь: решать основные задачи аналитической геометрии на плоскости и в пространстве Владеть: базовыми инструментами для решения задачи аналитической геометрии на плоскости и в пространстве
			ОПК-3.6. Владеет навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике.	Б1.О.19 Геометрия	Знать: основные подходы к решению задач аналитической геометрии и векторной алгебры в смежных дисциплинах Уметь: решать задачи аналитической геометрии и векторной алгебры в смежных дисциплинах и физике Владеть: навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике
			ОПК-3.7. Знает основные свойства важнейших алгебраических систем: групп, колец, полей.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные свойства важнейших алгебраических систем:

					групп, колец, полей Уметь: применять на практике основные свойства важнейших алгебраических систем Владеть: навыками работы с важнейшими алгебраическими системами: группами, кольцами, полями
			ОПК-3.8. Знает основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основы линейной алгебры и важнейшие свойства векторных пространств над произвольными полями Уметь: применять на практике важнейшие свойства векторных пространств над произвольными полями Владеть: базовыми инструментами линейной алгебры
			ОПК-3.9. Знает основные свойства колец многочленов над	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и

			кольцами и полями.		действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные свойства колец многочленов над кольцами и полями Уметь: применять на практике основные свойства колец многочленов Владеть: базовыми инструментами для работы с кольцами многочленов
			ОПК-3.10. Знает основные свойства отображений важнейших алгебраических систем.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные

					действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные свойства отображений важнейших алгебраических систем Уметь: применять на практике основные свойства отображений Владеть: навыками использования основных свойств отображений важнейших алгебраических систем
			ОПК-3.11. Умеет производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих

					уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные алгебраические операции в основных числовых и конечных полях, кольцах, алгебру многочленов и матриц Уметь: производить стандартные алгебраические операции в основных числовых и конечных полях, кольцах, а также оперировать с подстановками, многочленами, матрицами, в том числе с использованием компьютерных программ Владеть: базовыми инструментами для работы с многочленами, подстановками и матрицами
				Б1.О.27 Методы вычислений	
			ОПК-3.12. Умеет решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы;

					ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные подходы к решению систем линейных уравнений, приведению матрицы и квадратичные формы к каноническому виду Уметь: решать системы линейных уравнений над полями, приводить матрицы и квадратичные формы к каноническому виду Владеть: базовыми подходами к решению систем линейных уравнений
			ОПК-3.13. Умеет производить оценку качества полученных решений прикладных задач.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные принципы оценки качества полученных решений прикладных задач Уметь: производить оценку качества полученных решений прикладных задач Владеть: навыками

					оценки качества полученных решений
				Б1.О.27 Методы вычислений	
			ОПК-3.14. Владеет методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные методы решения стандартных алгебраических, матричных, подстановочных уравнений Уметь: применять на практике методы решения стандартных алгебраических, матричных, подстановочных уравнений Владеть: методами решения стандартных алгебраических, матричных, подстановочных уравнений в алгебраических структурах
			ОПК-3.15. Владеет навыками решения типовых линейных	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и

			уравнений над полем и кольцом вычетов.		действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь: производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные методы решения типовых линейных уравнений над полем и кольцом вычетов Уметь: применять на практике методы решения типовых линейных уравнений над полем и кольцом вычетов Владеть: навыками решения типовых линейных уравнений над полем и кольцом вычетов
			ОПК-3.16. Владеет навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований.	Б1.О.21 Алгебра	Знать: роль и место алгебры в си□ стеме математического знания; основные алгебраические структуры – группа, кольцо, поле, линейное пространство; основы матричной ал□ гебры: матрицы и действия над ни□ ми, матричные и матрично-вектор□ ные уравнения; комплексные числа, действия над ними, формулы Эйле□ ра и Муавра, области применения комплексных чисел; системы линей□ ных алгебраических уравнений, за□ дачи, приводящие к СЛАУ, методы точного и приближенного решения СЛАУ; полиномы от одной перемен□ ной и методы их исследования; спектральные характеристики мат□ риц. Уметь:

					производить преобразования матриц, осуществлять стандартные действия с матрицами: сложение, умножение, возведение в степень; находить различные числовые ха□ рактеристики матриц: след, опреде□ литель, норма, спектральный ради□ ус, спектр; строить обратные матри□ цы методами присоединенной мат□ рицы и преобразований Жордана; выполнять действия с комплексны□ ми числами, решать уравнения с комплексными коэффициентами; ре□ шать системы линейных алгебраи□ ческих уравнений методами Краме□ ра, Гаусса, обратной матрицы; ре□ шать матричные уравнения; решать алгебраические уравнения высоких степеней. Владеть: навыками применения раз□ личных методов алгебры для реше□ ния поставленной за
				Б1.О.23 Линейная алгебра	Знать: основные методы решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований Уметь: применять на практике стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований Владеть: навыками решения стандартных задач в векторных пространствах и методами нахождения канонических форм линейных преобразований
			ОПК-3.17. Знает основные понятия математической логики, теории дискретных функций и теории алгоритмов, а также возможности применения общих логических принципов в математике и профессиональной деятельности.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□ мов: вычислимость, разрешимость; важ□ нейшие понятия классической логики: ло□ гические исчисления, истинность и дока□ зуемость (выводимость) формул; альтер□ нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ ской логики и теории алгоритмов для ре□ шения практических задач; использовать язык математической логики для пред□ ставления знаний о предметных обла□ стях; Владеть: навыками использования логи□ ческих законов; способностью и готовно□ стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□ тиями теории вычислимых функций

			ОПК-3.18. Знает язык и средства современной математической логики и теории логических исчислений.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□ мов: вычислимость, разрешимость; важ□ нейшие понятия классической логики: ло□ гические исчисления, истинность и дока□ зуемость (выводимость) формул; альтер□ нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ ской логики и теории алгоритмов для ре□ шения практических задач; использовать язык математической логики для пред□ ставления знаний о предметных обла□ стях; Владеть: навыками использования логи□ ческих законов; способностью и готовно□ стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□ тиями теории вычислимых функций
			ОПК-3.19. Знает основные способы задания булевых функций и функций многозначной логики формулами и их свойства.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□ мов: вычислимость, разрешимость; важ□ нейшие понятия классической логики: ло□ гические исчисления, истинность и дока□ зуемость (выводимость) формул; альтер□ нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ ской логики и теории алгоритмов для ре□ шения практических задач; использовать язык математической логики для пред□ ставления знаний о предметных обла□ стях; Владеть: навыками использования логи□ ческих законов; способностью и готовно□ стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□ тиями теории вычислимых функций
			ОПК-3.20. Знает различные подходы к определению понятия алгоритма, методы доказательства алгоритмической неразрешимости и методы построения эффективных алгоритмов.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□ мов: вычислимость, разрешимость; важ□ нейшие понятия классической логики: ло□ гические исчисления, истинность и дока□ зуемость (выводимость) формул; альтер□ нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ ской логики и теории алгоритмов для ре□ шения практических задач; использовать язык математической логики для пред□ ставления знаний о предметных обла□ стях; Владеть: навыками использования логи□ ческих законов; способностью и готовно□ стью к изучению дальнейших понятий и теорий,

					разработанных в современной математической логике; основными поня тиями теории вычислимых функций
				Б1.О.27 Методы вычислений	
				Б1.О.31 Информатика	Знает: • различные подходы к определению понятия алгоритма; • понятия алгоритмической сходимости и алгоритмической
			ОПК-3.21. Умеет производить основные логические операции в исчислении высказываний и исчислении предикатов.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит мов: вычислимость, разрешимость; важ нейшие понятия классической логики: ло гические исчисления, истинность и дока зуемость (выводимость) формул; альтер нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче ской логики и теории алгоритмов для ре шения практических задач; использовать язык математической логики для пред ставления знаний о предметных обла стях; Владеть: навыками использования логи ческих законов; способностью и готовно стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня тиями теории вычислимых функций
			ОПК-3.22. Умеет находить и исследовать свойства представлений булевых и многозначных функций формулами в различных базисах.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит мов: вычислимость, разрешимость; важ нейшие понятия классической логики: ло гические исчисления, истинность и дока зуемость (выводимость) формул; альтер нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче ской логики и теории алгоритмов для ре шения практических задач; использовать язык математической логики для пред ставления знаний о предметных обла стях; Владеть: навыками использования логи ческих законов; способностью и готовно стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня тиями теории вычислимых функций

			ОПК-3.23. Умеет оценивать сложность алгоритмов и вычислений	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□мов: вычислимость, разрешимость; важ□нейшие понятия классической логики: ло□гические исчисления, истинность и дока□зуемость (выводимость) формул; альтер□нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ской логики и теории алгоритмов для ре□шения практических задач; использовать язык математической логики для пред□ставления знаний о предметных обла□стях; Владеть: навыками использования логи□ческих законов; спœособностью и готовно□стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□тиями теории вычислимых функций
			ОПК-3.24. Умеет применять методы математической логики и теории алгоритмов к решению задач математической кибернетики.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□мов: вычислимость, разрешимость; важ□нейшие понятия классической логики: ло□гические исчисления, истинность и дока□зуемость (выводимость) формул; альтер□нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ской логики и теории алгоритмов для ре□шения практических задач; использовать язык математической логики для пред□ставления знаний о предметных обла□стях; Владеть: навыками использования логи□ческих законов; способностью и готовно□стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□тиями теории вычислимых функций

			ОПК-3.25. Владеет навыками использования языка современной символической логики.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□мов: вычислимость, разрешимость; важ□нейшие понятия классической логики: ло□гические исчисления, истинность и дока□зуемость (выводимость) формул; альтер□нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ской логики и теории алгоритмов для ре□шения практических задач; использовать язык математической логики для пред□ставления знаний о предметных обла□стях; Владеть: навыками использования логи□ческих законов; способностью и готовно□стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□тиями теории вычислимых функций
			ОПК-3.26. Владеет навыками упрощения формул алгебры высказываний и алгебры предикатов.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□мов: вычислимость, разрешимость; важ□нейшие понятия классической логики: ло□гические исчисления, истинность и дока□зуемость (выводимость) формул; альтер□нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ской логики и теории алгоритмов для ре□шения практических задач; использовать язык математической логики для пред□ставления знаний о предметных обла□стях; Владеть: навыками использования логи□ческих законов; способностью и готовно□стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□тиями теории вычислимых функций

			ОПК-3.27. Владеет навыками применения методов и фактов теории алгоритмов, относящимися к решению переборных задач.	Б1.О.24 Математическая логика и теория алгоритмов	Знать: важные понятия теории алгорит□мов: вычислимость, разрешимость; важ□нейшие понятия классической логики: ло□гические исчисления, истинность и дока□зуемость (выводимость) формул; альтер□нативные понятия алгоритма; важные теоремы теории алгоритмов. Уметь: применять методы математиче□ской логики и теории алгоритмов для ре□шения практических задач; использовать язык математической логики для пред□ставления знаний о предметных обла□стях; Владеть: навыками использования логи□ческих законов; способностью и готовно□стью к изучению дальнейших понятий и теорий, разработанных в современной математической логике; основными поня□тиями теории вычислимых функций
			ОПК-3.28. Знает свойства основных дискретных структур: линейных рекуррентных последовательностей, графов, конечных автоматов, комбинаторных структур.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики
			ОПК-3.29. Знает основные понятия и методы теории графов.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики

			ОПК-3.30. Знает основные понятия и методы теории конечных автоматов.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики
			ОПК-3.31. Знает основные понятия и методы комбинаторного анализа.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики
			ОПК-3.32. Умеет решать задачи периодичности и эквивалентности для линейных рекуррентных последовательностей и конечных автоматов.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики

			ОПК-3.33. Умеет применять аппарат производящих функций и рекуррентных соотношений для решения перечислительных задач.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики
			ОПК-3.34. Умеет решать оптимизационные задачи на графах.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики
			ОПК-3.35. Умеет применять стандартные методы дискретной математики для решения профессиональных задач.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики

			ОПК-3.36. Владеет навыками решения типовых комбинаторных и теоретико-графовых задач.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики
			ОПК-3.37. Владеет навыками применения языка и средств дискретной математики при решении профессиональных задач.	Б1.О.25 Дискретная математика	Знать: - методы теории множеств, - методы математической логики, - методы алгебры высказываний, - методы теории графов, - методы теории автоматов, - методы теории производящих функций - методы теории алгоритмов. Уметь: -разрабатывать эффективные алгоритмы, базирующиеся на методах дискретной математики, и отлаживать программы с использованием современных компьютерных технологий; Владеть: - навыками моделирования прикладных задач методами дискретной математики
			ОПК-3.38. Знает основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных.	Б1.О.18 Математический анализ	
			ОПК-3.39. Знает основные методы дифференциального исчисления функций одной и нескольких действительных переменных.	Б1.О.18 Математический анализ	
			ОПК-3.40. Знает основные методы	Б1.О.18 Математический анализ	

			интегрального исчисления функций одной и нескольких действительных переменных.		
			ОПК-3.41. Знает основные методы исследования числовых и функциональных рядов.	Б1.О.18 Математический анализ	
			ОПК-3.42. Знает основные задачи теории функций комплексного переменного.	Б1.О.18 Математический анализ	
				Б1.О.54 Комплексный анализ	
			ОПК-3.43. Знает основные типы обыкновенных дифференциальных уравнений и методы их решения.	Б1.О.26 Дифференциальные уравнения	Знать: задачи профессиональной деятельно сти Уметь: разрабатывать, обосновывать и реа лизовывать процедуры решения задач про фессиональной деятельности Владеть: математическими методами разра ботки, обоснования и реализации задач про фессиональной деятельности
				Б1.О.53 Уравнения математической физики	
			ОПК-3.44. Умеет обосновывать основные положения теории пределов и непрерывности функций одной и нескольких действительных переменных.	Б1.О.18 Математический анализ	
			ОПК-3.45. Умеет обосновывать основные методы дифференциального исчисления функций одной и нескольких действительных	Б1.О.18 Математический анализ	

			переменных.		
			ОПК-3.46. Умеет обосновывать основные методы интегрального исчисления функций одной и нескольких действительных переменных.	Б1.О.18 Математический анализ	
			ОПК-3.47. Умеет обосновывать основные методы исследования числовых и функциональных рядов.	Б1.О.18 Математический анализ	
			ОПК-3.48. Владеет навыками использования справочных материалов по математическому анализу.	Б1.О.18 Математический анализ	
			ОПК-3.49. Знает основные понятия теории вероятностей, числовые и функциональные характеристики распределений случайных величин и их основные свойства.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.50. Знает классические предельные теоремы теории вероятностей.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение

					математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.51. Знает основные понятия теории случайных процессов.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.52. Знает постановку задач и основные понятия математической статистики.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.53. Знает стандартные методы получения точечных и интервальных оценок параметров вероятностных распределений.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.54. Знает стандартные методы проверки статистических гипотез.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических

					гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.55. Умеет обосновывать классические положения и стандартные методы теории вероятностей и случайных процессов.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.56. Умеет обосновывать классические положения и стандартные методы математической статистики.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.57. Умеет разрабатывать и использовать вероятностные и статистические модели при решении типовых прикладных задач.	Б1.О.20 Теория вероятностей и математическая статистика	Знание аппарата теории вероятностей, математической статистики, теории принятия статистических решений; Умение применять первичную статистическую обработки выборки, находить точечные и интервальные оценки параметров распределений, использовать критерии проверки статистических гипотез, определять наличие корреляционных связей между случайными величинами и строить функции регрессии. Владение математическим аппаратом, используемым для описания массовых случайных явлений.
			ОПК-3.58. Владеет навыками решения основных типов	Б1.О.26 Дифференциальные уравнения	Знать: задачи профессиональной деятельно□сти Уметь: разрабатывать, обосновывать и реа□лизовывать процедуры решения задач про□фессиональной деятельности Владеть:

			обыкновенных дифференциальных уравнений.		математическими методами разра□ ботки, обоснования и реализации задач про□ фессиональной деятельности
				Б1.О.53 Уравнения математической физики	
	ОПК-4	Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности;	ОПК-4.1. Знает основные законы механики и оптики.	Б1.О.13 Механика и оптика	Знать: формализм и основные законы классической механики, основные уравнения гидродинамики, основные методы и достижения оптики, а также границы их применимости.
			ОПК-4.2. Знает основные законы термодинамики и молекулярной физики.	Б1.О.15 Термодинамика	основные законы и положения термодинамики и статистической физики; классические и квантовые распределения
			ОПК-4.3. Знает основные законы электричества и магнетизма.	Б1.О.14 Электричество и магнетизм	знает базовые понятия и законы теории электричества и магнетизма
			ОПК-4.4. Знает основы теории колебаний и волн, оптики.	Б1.О.13 Механика и оптика	Знать: основные законы колебательного и волнового движения.
				Б1.О.14 Электричество и магнетизм	
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.5. Знает основы квантовой физики.	Б1.О.16 Квантовая теория	знает теоретические основы нерелятивистской квантовой теории; способы применения уравнений квантовой теории. принципы применения квантовой идеологии в информационных системах;
			ОПК-4.6. Умеет	Б1.О.13 Механика и	Уметь: построить конкретную физическую модель и реализовать

			использовать математические модели физических явлений и процессов.	оптика	ее содержание в прикладных задачах; проводить анализ полученных теоретических результатов. Владеть: приемами и методами решения типовых задач, представлениями о перспективных направлениях научных исследований в теоретической механике и их потенциальных возможностях при практической реализации в специальных областях
				Б1.О.14 Электричество и магнетизм	умеет использовать математические модели электромагнитных явлений и процессов
				Б1.О.15 Термодинамика	умеет использовать математические модели термодинамических явлений
				Б1.О.16 Квантовая теория	умеет использовать математические модели явлений для описания процессов в микромире
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
				Б1.О.53 Уравнения математической физики	
			ОПК-4.7. Умеет решать типовые прикладные физические задачи.	Б1.О.13 Механика и оптика	Уметь: построить конкретную физическую модель и реализовать ее содержание в прикладных задачах; проводить анализ полученных теоретических результатов. Владеть: приемами и методами решения типовых задач
				Б1.О.14 Электричество и магнетизм	умеет решать базовые практические задачи с использованием методов векторного анализа, принципа супрпозиции, основных законов электричества и магнетизма

				Б1.О.15 Термодинамика	умеет решать типовые прикладные физические задачи методами статистической физики
				Б1.О.16 Квантовая теория	решать основные задачи квантовой теории, эффективно применять квантовую теорию при описании модельных элементарных квантовых систем
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
			ОПК-4.8. Владеет методами исследования физических явлений и процессов.	Б1.О.13 Механика и оптика	Владеть: методами исследования, применяемыми в классической механике, гидродинамике и оптике.
				Б1.О.14 Электричество и магнетизм	владеет методами исследования процессов электромагнитной природы
				Б1.О.15 Термодинамика	владеет основными методами статистической физики и термодинамики для исследования термодинамических процессов
				Б1.О.16 Квантовая теория	владеет математическим аппаратом квантовой теории
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации

					уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.9. Знает принципы работы элементов и функциональных узлов электронной аппаратуры.	Б1.О.17 Электроника и схемотехника	Знать: дифференциальные уравнения простых электрических цепей Уметь: применять необходимые физические законы и модели для решения задач профессиональной деятельности Владеть: знаниями дифференциальных уравнений простых электрических цепей, умением применять необходимые физические законы и модели для решения задач профессиональной деятельности
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.10. Знает методы анализа и синтеза электронных схем.	Б1.О.17 Электроника и схемотехника	Знать: методы анализа электрических цепей в переходных и установившихся режимах в частотной и временной областях Уметь: применять необходимые физические законы и модели для решения задач профессиональной деятельности Владеть: методами анализа электрических цепей в переходных и установившихся режимах в частотной и временной областях, умением применять необходимые физические законы и модели для решения задач профессиональной деятельности
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи,

					обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.11. Знает типовые схемотехнические решения основных узлов и блоков электронной аппаратуры.	Б1.О.17 Электроника и схемотехника	Знать: методы анализа электрических цепей в переходных и установившихся режимах в частотной и временной областях Уметь: измерять параметры электрической цепи Владеть: методами измерения параметров электрической цепи, умением применять необходимые физические законы и модели для решения задач профессиональной деятельности
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.12. Умеет работать с современной элементной базой электронной аппаратуры.	Б1.О.17 Электроника и схемотехника	Знать: методы анализа электрических цепей в переходных и установившихся режимах в частотной и временной областях Уметь: анализировать процессы, протекающие в линейных и нелинейных электрических цепях Владеть: методами анализа

					процессов, протекающих в линейных и нелинейных электрических цепях, умением применять необходимые физические законы и модели для решения задач профессиональной деятельности
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
			ОПК-4.13. Умеет использовать стандартные методы и средства проектирования цифровых узлов и устройств.	Б1.О.17 Электроника и схемотехника	Знать: методы анализа электрических цепей в переходных и установившихся режимах в частотной и временной областях Уметь: расчитывать простых линейных и нелинейных электрических цепей Владеть: методами расчета простых линейных и нелинейных электрических цепей, умением применять необходимые физические законы и модели для решения задач профессиональной деятельности
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности

					средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.14. Владеет навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры.	Б1.О.17 Электроника и схемотехника	Знать: методы анализа физической сущности явлений и процессов, лежащих в основе функционирования микроэлектронной техники; Уметь: анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности; Владеть: навыками использования современной измерительной аппаратуры при экспериментальном исследовании электронной аппаратуры
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.15. Владеет навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации.	Б1.О.17 Электроника и схемотехника	Знать: методы анализа физической сущности явлений и процессов, лежащих в основе функционирования микроэлектронной техники; Уметь: анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности; Владеть: навыками чтения принципиальных схем, построения временных диаграмм работы узла, устройства по комплекту документации
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи,

					обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-4.16. Знает структуру и принципы работы современных и перспективных микропроцессоров.	Б1.О.22 Аппаратные средства вычислительной техники	Знает назначение и виды процессоров. Знает рабочий цикл процессора. Имеет представления о средствах организации многопрограммной работы процессора. Знает особенности архитектур и принципы работы современных МП.
			ОПК-4.17. Умеет анализировать и синтезировать электронные схемы.	Б1.О.17 Электроника и схемотехника	Знать: методы анализа физической сущности явлений и процессов, лежащих в основе функционирования микроэлектронной техники; Уметь: анализировать и синтезировать электронные схемы Владеть: навыками анализа и синтеза электронных схем
				Б1.О.22 Аппаратные средства вычислительной техники	Умеет выполнить сбор и анализ данных о различных типах шифраторов и дешифраторов. Умеет выполнить построение RAID массива заданного уровня
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима

					работы технических средств защиты ин□ формации
			ОПК-4.18. Умеет определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств.	Б1.О.22 Аппаратные средства вычислительной техники	Умеет получать данные о технических характеристиках персонального компьютера, об установленных программных и аппаратных средствах защиты данных
				Б2.О.01(У) Учебная практика (экспериментальн о-исследовательска я)	Знать: - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем. Уметь: - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных; - практическими навыками при□ менения технических и про□ граммных средств диагностики для оценки исправности и произ□ водительности оборудования.
			ОПК-4.19. Владеет навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.	Б1.О.22 Аппаратные средства вычислительной техники	Владеет методам защиты компьютера от НСД из внешней сети и поиска уязвимостей в системе защиты. Владеет навыками применения средств устранения неисправностей в TCP/IP
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения

					специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Знать: - стандарты описания архитек□ туры программного обеспечения; - основные платформы, техноло□ гии и инструментальные про□ граммно-аппаратные средства для реализации информацион□ ных систем. Уметь: - использовать средства защиты, представляемые систем управ□ ления базами данных; - использовать основные плат□ формы, технологии и инструмен□ тальные программно-аппарат□ ные средства для реализации информационных систем; - применять защищенные прото□ колы, межсетевые экраны и средства обнаружения вторже□ ний для защиты информации в сетях. Владеть: - практическими навыками при□ менения специализированных программных средств, предна□ значенных для обеспечения без□ опасности и целостности дан□ ных; - практическими навыками при□ менения технических и про□ граммных средств диагностики для оценки исправности и произ□ водительности оборудования.

			ОПК-4.20. Знает фундаментальные закономерности, связанные с получением сигналов и их передачей по каналам связи.	Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
			ОПК-4.21. Знает фундаментальные закономерности, связанные с обработкой и преобразованием сигналов в информационных системах.	Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
			ОПК-4.22. Знает функциональное назначение и принципы работы основных блоков современных средств защиты информации.	Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы

					основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
	ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;	ОПК-5.1. Знает источники и классификацию угроз информационной безопасности.	Б1.О.39 Основы информационной безопасности	
			ОПК-5.2. Знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России.	Б1.О.11 Введение в специальность	Знает и понимает содержание Конституции РФ, Законов РФ «Об образовании», «О высшем и послевузовском образовании». Знает содержание федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 10.05.01 «Компьютерная безопасность» Знает и понимает национальные интересы Российской Федерации в информационной сфере и их обеспечение. Знает организационную структуру и основные функции системы обеспечения информационной безопасности Российской Федерации. Знает и понимает задачи обеспечения безопасности России в информационной сфере
				Б1.О.39 Основы информационной безопасности	
			ОПК-5.3. Умеет классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности.	Б1.О.39 Основы информационной безопасности	
				Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: применять нормативные правовые акты, нормативные и методические документы, регламентирующие защиту сведений, составляющих государственную тайну и иных сведений ограниченного доступа Владеть: навыками работы с нормативными правовыми актами; навыками анализа нормативных правовых документов в области обеспечения информационной безопасности; навыками отнесения информации к различным видам и степеням конфиденциальности
				Б2.О.06(П) Производственная	Знать: - основы правовых знаний в различных сферах

				практика по получению профессиональных умений и навыков в области профессиональной деятельности	деятельно□ сти;- нормативные правовые акты для профессиональной дея□ тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо□ ваний к защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия (орга□ низации);- способы обеспечения за□ щиты и безопасности ИС; - сущность и понятия лицензи□ рования в области обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; Уметь:- использовать правовые зна□ ния в различных сферах дея□ тельности;- использовать нормативные правовые акты в профессио□ нальной деятельности;- классифицировать защищае□ мую информацию по видам тайны и степеням конфиден□ циальности;- определять классы защи□ щенности автоматизирован□ ных систем и средств вычис□ лительной техники, применять методы и средства проектиро□ вания программного обеспе□ чения, используемые при со□ здании защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть:- навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности;- навыками определения ос□ новных характеристик прили□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации;- навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в

					области инфор мационной безопасности;- международно-правовой тер минологией;- навыками работы с междуна родно-правовыми актами, нормативными правовыми ак тами России;- навыками сравнительного анализа российской модели регулирования информацион ных отношений с междуна родно-правовыми стандар тами и аналогичными институ тами зарубежных стран; - практическими навыками ис пользования инструменталь ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.4. Умеет классифицировать и оценивать угрозы информационной безопасности для объекта информатизации.	Б1.О.39 Основы информационной безопасности	
				Б1.О.48иУправление ресурсами в системах информационной безопасности	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно сти;- нормативные правовые акты для профессиональной дея тельности; - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо ваний к защите информации; - принципы формирования комплекса мер по обеспече нию информационной без опасности предприятия (орга низации);- способы обеспечения за щиты и безопасности ИС; - сущность и понятия лицензи рования в области обеспече ния защиты государственной тайны, технической защиты конфиденциальной информа ции, по аттестации объектов информатизации и сертифи кациисредств защиты инфор мации, характеристики их со ставляющих; Уметь:- использовать правовые зна ния в различных сферах дея тельности;- использовать нормативные правовые акты в профессио нальной деятельности;- классифицировать защищае мую информацию по видам тайны и степеням конфиден циальности;- определять классы защи щенности автоматизирован ных систем и средств вычис лительной техники, применять методы и средства проектиро вания

					программного обеспе□ чения, используемые при со□ здании защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть:- навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности;- навыками определения ос□ новных характеристик при ли□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации;- навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности; - международно-правовой тер□ минологией;- навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России;- навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми стандар□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.5. Знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Знать: основы правового обеспечения информационной безопасности; основные положения законодательства РФ в области информационной безопасности права, свободы и обязанности личности в области информационной безопасности; организационную структуру государственной системы обеспечения информационной безопасности РФ Уметь: применять действующую законодательную базу в области обеспечения безопасности информации; осуществлять поиск необходимых нормативных правовых актов и отдельных информационно-правовых норм в системе действующего законодательства, в том

					числе с помощью справочно-поисковых систем правовой информации.
			ОПК-5.6. Знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	положения отраслевого законодательства, регулирующего сферу информационной безопасности Уметь: оперировать основными категориями, понятиями, положениями отраслевого законодательства, регулирующего сферу информационной безопасности; применять положения отраслевого законодательства в области обеспечения безопасности информации; осуществлять поиск необходимых норм отраслевого законодательства
			ОПК-5.7. Знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Знать: понятие и виды защищаемой информации; основные положения законодательства Российской Федерации, нормативных правовых актов, нормативных и методических документов в области обеспечения безопасности государственной тайны и иных видов информации ограниченного доступа; организационные основы обеспечения безопасности государственной тайны и иных видов информации ограниченного доступа; характеристику преступлений и иных видов правонарушений в сфере информационной безопасности; меры юридической ответственности за правонарушения в области информационной безопасности. Уметь: осуществлять поиск необходимых положений законодательства Российской Федерации, нормативных правовых актов, нормативных и методических документов в области обеспечения безопасности государственной тайны и иных видов информации ограниченного доступа.

			ОПК-5.8. Знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Знать: место персональных данных в системе информации ограниченного доступа, категории и понятия в области безопасности персональных данных, основные положения нормативных правовых актом и методических документов, регламентирующих защиту персональных данных; основы правового регулирования охраны результатов интеллектуальной деятельности. Уметь: осуществлять поиск необходимых положений нормативных правовых актов и методических документов в области обеспечения безопасности персональных данных и охраны результатов интеллектуальной деятельности.
			ОПК-5.9. Умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: осуществлять поиск необходимых положений нормативных правовых актов и методических документов в области обеспечения безопасности информации и их анализ; обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, положениями действующего законодательства, нормативных правовых и методических документов; предпринимать необходимые меры по восстановлению нарушенных прав. Владеть: системным подходом к организации безопасности информации; навыками работы с нормативными правовыми актами; навыками анализа нормативных правовых документов в области обеспечения информационной безопасности; навыками обоснования решений, связанных с реализацией правовых норм по защите информации в пределах должностных обязанностей, положениями действующего законодательства, нормативных правовых и методических документов; навыками реализации необходимых мер по восстановлению нарушенных прав
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно□ сти;- нормативные правовые акты для профессиональной дея□ тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо□ ванийк защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия

					(орга□ низации);- способы обеспечения за□ щиты и безопасности ИС; - сущность и понятия лицензи□ рования в области обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; Уметь:- использовать правовые зна□ ния в различных сферах дея□ тельности;- использовать нормативные правовые акты в профессио□ нальной деятельности;- классифицировать защищае□ мую информацию по видам тайны и степеням конфиден□ циальности;- определять классы защи□ щенности автоматизирован□ ных систем и средств вычис□ лительной техники, применять методы и средства проектиро□ вания программного обеспе□ чения, используемые при со□ здании защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть:- навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности;- навыками определения ос□ новных характеристик при ли□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации;- навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности;- международно-правовой тер□ минологией;- навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России; - навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми стандар□ тами и аналогичными институ□ тами

					зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.10. Умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций, а также проводить анализ разработанных проектов; Владеть: навыками разработки проектов локальных правовых актов, инструкций, регламентов и организационно□ распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций, а также их анализа;
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно□ сти;- нормативные правовые акты для профессиональной дея□ тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо□ ваний к защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия (орга□ низации);- способы обеспечения за□ щиты и безопасности ИС; - сущность и понятия лицензи□ рования в области обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; Уметь:- использовать правовые зна□ ния в различных сферах дея□ тельности;- использовать нормативные правовые акты в профессио□ нальной деятельности; - классифицировать защищае□ мую информацию по видам тайны и степеням конфиден□ циальности;- определять классы защи□ щенности

					автоматизирован□ ных систем и средств вычис□ лительной техники, применять методы и средства проектиро□ вания программного обеспе□ чения, используемые при со□ здании защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть:- навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности;- навыками определения ос□ новных характеристик при ли□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации;- навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности;- международно-правовой тер□ минологией;- навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России;- навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми станда□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.11. Умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций Владеть: навыками определения требований при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации.

			безопасности информации.	Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно сти;- нормативные правовые акты для профессиональной дея тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо ваний к защите информации; - принципы формирования комплекса мер по обеспече нию информационной без опасности предприятия (орга низации);- способы обеспечения за щиты и безопасности ИС; - сущность и понятия лицензи рования в области обеспече ния защиты государственной тайны, технической защиты конфиденциальной информа ции, по аттестации объектов информатизации и сертифи кации средств защиты инфор мации, характеристики их со ставляющих; Уметь: - использовать правовые зна ния в различных сферах дея тельности;- использовать нормативные правовые акты в профессио нальной деятельности;- классифицировать защищае мую информацию по видам тайны и степеням конфиден циальности;- определять классы защи щенности автоматизирован ных систем и средств вычис лительной техники, применять методы и средства проектиро вания программного обеспе чения, используемые при со здании защищенных компью терных систем, методы опре деления требований к защите информации; - проводить анализ информа ционной безопасности объек тов и систем на соответствие требованиям стандартов в об ласти информационной без опасности. Владеть:- навыками применения пра вовых знаний в различных сферах деятельности; - навыками применения нор мативных правовых актов в профессиональной деятель ности;- навыками определения ос новных характеристик при ли цензировании в области обес печения защиты государ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за щиты информации;- навыками проведения ана лиза информационной без опасности

					объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности;- международно-правовой тер□ минолгией; - навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России;- навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми стандар□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.12. Умеет формулировать основные требования информационной безопасности при эксплуатации компьютерной системы.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; Владеть: навыками определения требований информационной безопасности при эксплуатации компьютерной системы
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно□ сти;- нормативные правовые акты для профессиональной дея□ тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо□ ваний к защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия (орга□ низации);- способы обеспечения за□ щиты и безопасности ИС; - сущность и понятия лицензи□ рования в области обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; Уметь:- использовать правовые зна□ ния в различных сферах дея□ тельности;- использовать нормативные правовые акты в профессио□ нальной деятельности;- классифицировать защищае□ мую информацию по видам тайны и степеням конфиден□ циальности;- определять классы защи□ щенности автоматизирован□ ных систем и средств вычис□ лительной техники, применять методы и средства проектиро□ вания

					программного обеспе□ чения,используемые при со□ здании защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть: - навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности;- навыками определения ос□ новных характеристик при ли□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации;- навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности;- международно-правовой тер□ минологией;- навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России;- навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми стандар□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.13. Умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций Владеть: навыками определения требований по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации
				Б2.О.06(П) Производственная практика по получению	Знать: - основы правовых знаний в различных сферах деятельно□ сти;- нормативные правовые акты для

				профессиональных умений и навыков в области профессиональной деятельности	профессиональной дея□ тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо□ ваний к защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия (орга□ низации);- способы обеспечения за□ щиты и безопасности ИС; - сущность и понятия лицензи□ рования в области обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; Уметь:- использовать правовые зна□ ния в различных сферах дея□ тельности;- использовать нормативные правовые акты в профессио□ нальной деятельности;- классифицировать защищае□ мую информацию по видам тайны и степеням конфиден□ циальности;- определять классы защи□ щенности автоматизирован□ ных систем и средств вычис□ лительной техники, применять методы и средства проектиро□ вания программного обеспе□ чения, используемые при со□ здании защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть:- навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности;- навыками определения ос□ новных характеристик при ли□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации;- навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности;- международно-

					правовой тер□ минологией;- навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России;- навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми стандар□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.14. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

				Б1.О.51 Защита информации от утечки по техническим каналам	знать: способы и средства защиты информации от утечки по техниче□ ским каналам и контроля эффектив□ ности защиты информации; уметь: определять необходимые способы и средства защиты инфор□ мации от утечки по техническим ка□ налам и контроля эффективности защиты информации; владеть: навыками применения спо□ собов и средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации
			ОПК-5.15. Знает организацию защиты информации от утечки по техническим каналам на объектах информатизации.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

				Б1.О.51 Защита информации от утечки по техническим каналам	знать: основы принципов организаци защиты информации от утечки по техническим каналам на объектах информатизации; уметь: определять необходимые принципы организации защиты ин□ формации от утечки по техническим каналам на объектах информатиза□ ции; владеть: практическими навыками организации защиты информации от утечки по техническим каналам на объектах информатизации
			ОПК-5.16. Знает возможности технических средств перехвата информации.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации

				Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные принципы примене□ ния технических средств перехвата информации; уметь: анализировать возможные условия применения технических средств перехвата информации; владеть: практическими навыками определения характеристик техниче□ ских средств перехвата информации
			ОПК-5.17. Умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: особенности формирования угроз информационной безопасности объекта по техническим каналам; уметь: анализировать и оценивать угрозы информационной безопасно□ сти объекта по техническим каналам; владеть: практическими навыками по оценке характеристик угрозы ин□ формационной безопасности объек□ та по техническим каналам
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно□ сти;- нормативные правовые акты для профессиональной дея□ тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо□ ваний к защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия (орга□ низации);- способы обеспечения за□ щиты и безопасности ИС; - сущность и понятия лицензи□ рования вобласти обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; Уметь:- использовать правовые зна□ ния вразличных сферах дея□ тельности;- использовать нормативные правовые акты в профессио□ нальной деятельности;- классифицировать защищае□ мую информацию по видам тайны и степеням конфиден□ циальности;- определять классы защи□ щенности автоматизирован□ ных системи средств вычис□ лительной техники, применять методы и средства проектиро□ вания программного обеспе□ чения, используемые при со□ здании

					защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть:- навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности;- навыками определения ос□ новных характеристик при ли□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации; - навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности;- международно-правовой тер□ минологией;- навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России;- навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми стандар□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-5.18. Знает нормативные документами в области технической защиты информации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: положения нормативных до□ кументов в области технической за□ щиты информации; уметь: определить необходимые к использованию нормативные доку□ менты в области технической защи□ ты информации; владеть: практическими навыками по использованию нормативных до□ кументов в области технической за□ щиты информации
			ОПК-5.19. Владеет методами и средствами технической защиты информации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные методы и средства технической защиты информации; уметь: определять актуальные ме□ тоды и средства технической защиты информации; владеть: практическими навыками применения методов и средств тех□ нической защиты информации

				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно сти;- нормативные правовые акты для профессиональной дея тельности;- стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы определения требо ваний к защите информации; - принципы формирования комплекса мер по обеспече нию информационной без опасности предприятия (орга низации);- способы обеспечения за щиты и безопасности ИС; - сущность и понятия лицензи рования в области обеспече ния защиты государственной тайны, технической защиты конфиденциальной информа ции, по аттестации объектов информатизации и сертифи кации средств защиты инфор мации, характеристики их со ставляющих; Уметь:- использовать правовые зна ния в различных сферах дея тельности;- использовать нормативные правовые акты в профессио нальной деятельности;- классифицировать защищае мую информацию по видам тайны и степеням конфиден циальности;- определять классы защи щенности автоматизирован ных систем исредств вычис лительной техники, применять методы и средства проектиро вания программного обеспе чения, используемые при со здании защищенных компью терных систем, методы опре деления требований к защите информации; - проводить анализ информа ционной безопасности объек тов и систем на соответствие требованиям стандартов в об ласти информационной без опасности. Владеть:- навыками применения пра вовых знаний в различных сферах деятельности; - навыками применения нор мативных правовых актов в профессиональной деятель ности;- навыками определения ос новных характеристик при ли цензировании в области обес печения защиты государ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за щитыинформации; - навыками проведения ана лиза информационной без опасности

					объектов и систем на соответствие требованиям стандартов в области инфор мационной безопасности;- международно-правовой тер минологией;- навыками работы с междуна родно-правовыми актами, нормативными правовыми ак тами России;- навыками сравнительного анализа российской модели регулирования информацион ных отношений с междуна родно-правовыми стандар тами и аналогичными институ тами зарубежных стран; - практическими навыками ис пользования инструменталь ных интеллектуальных систем для обоснования требований к защите информации.
	ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ОПК-6.1. Знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Знать: положения нормативных правовых актов, регламентирующих деятельность по лицензированию в области обеспечения защиты государственной тайны, технической защите конфиденциальной информации, по аттестации объектов информатизации и сертификации Уметь: применять положения нормативных правовых актов, регламентирующих деятельность по лицензированию в области обеспечения защиты государственной тайны, технической защите конфиденциальной информации, по аттестации объектов информатизации и сертификации
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: сущность и понятия лицензи рования в области обеспечения за щиты государственной тайны, техни ческой защиты конфиденциальной информации, по аттестации объек тов информатизации и сертификации средств защиты информации, харак теристики их составляющих; уметь: классифицировать защища емую информацию по видам тайны и степеням конфиденциальности; владеть: навыками определения основных характеристик при лицен зировании в области обеспечения защиты государственной тайны, тех нической защиты конфиденциальной информации, при аттестации объек тов информатизации и сертификации средств защиты информации
			ОПК-6.2. Знает задачи	Б1.О.49 Организационное и правовое обеспечение	Знать: положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России, задачи и

			органов защиты государственной тайны и служб защиты информации на предприятиях.	информационной безопасности	их полномочия в области обеспечения безопасности информации; задачи и полномочия служб защиты информации на предприятия Уметь: применять положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России при реализации задач и полномочий служб защиты информации на предприятия
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: задачи органов защиты госу□ дарственной тайны и служб защиты информации на предприятиях; уметь: определять основные пути решения задач органов защиты госу□ дарственной тайны и служб защиты информации на предприятиях; владеть: основами решения задач органов защиты государственной тайны и служб защиты информации на предприятиях
			ОПК-6.3. Знает систему организационных мер, направленных на защиту информации ограниченного доступа.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Знать: основы организационного обеспечения информационной безопасности; организационные меры защиты информации ограниченного доступа; Уметь: применять организационные меры защиты информации ограниченного доступа;
				Б1.О.48 Управление ресурсами в системах информационной безопасности	
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные принципы органи- зационных мер, направленных на защиту информации ограниченного доступа; уметь: анализировать возможные организационные меры, направлен□ ные на защиту информации ограни□ ченного доступа; владеть: практическими навыками определения организационных мер, направленных на защиту информа□ ции ограниченного доступа
			ОПК-6.4. Знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	Б1.О.40 Модели безопасности компьютерных систем	Знать: нормативные, руководящие и методические документы уполномочен□ ных федеральных органов исполни□ тельной власти по защите информации ограниченного доступа Уметь: применять нормативные, руко□ водящие и методические документы уполномоченных федеральных органов исполнительной власти по защите ин□ формации ограниченного доступа при оценке защищенности компьютерных систем

			ограниченного доступа.		Владеть: практическими навыками применения нормативных, руководящих и методических документов уполномо□ ченных федеральных органов исполни□ тельной власти по защите информации ограниченного доступа для проектиро□ вания, разработки и оценивания защи□ щенности компьютерной системы.
				Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Знать: положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России по защите информации ограниченного доступа Уметь: применять положения нормативных правовых актов, нормативных и методических документов ФСБ России, ФСТЭК России при реализации задач и полномочий по защите информации ограниченного доступа
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные нормативные, руко□ водящие и методические документы уполномоченных федеральных орга□ нов исполнительной власти по защи□ те информации ограниченного до□ ступа; уметь: определить необходимые и пользоваться нормативными, руко□ водящими и методическими доку□ менты уполномоченных федераль□ ных органов исполнительной власти по защите информации ограниченно□ го доступа; владеть: практическими навыками применения нормативных, руково□ дящих и методических документов уполномоченных федеральных орга□ нов исполнительной власти по защи□ те информации ограниченного до□ ступа
			ОПК-6.5. Знает основные угрозы безопасности информации и модели нарушителя компьютерных систем.	Б1.О.40 Модели безопасности компьютерных систем	Знать: источники угроз информацион□ ной безопасности в компьютерных си□ стемах и сетях и меры по их предот□ вращению, стандарты по классифика□ ции и описанию уязвимостей информа□ ционных систем, формальные модели безопасности компьютерных систем Уметь; проводить классификацию угроз и уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению Владеть: практическими навыками ис□ пользования инструментальных средств для моделирование угроз без□ опасности в компьютерных системах с учетом мер по их предотвращению

				Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Знать: понятие, классификации угроз безопасности информации и модели нарушителя компьютерных систем Уметь: определять основные угрозы безопасности информации и модели нарушителя компьютерных систем.
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные угрозы безопасно сти информации и модели наруши теля компьютерных систем; уметь: определить опасные угрозы и нарушителя информационной без опасности компьютерных систем; владеть: практическими навыками анализа и оценки угроз и нарушителя информационной безопасности ком пьютерных систем
			ОПК-6.6. Умеет разрабатывать модели угроз и модели нарушителя компьютерных систем.	Б1.О.40 Модели безопасности компьютерных систем	Знать: руководящие документы ФСТЭК России (Гостехкомиссии России). Уметь; разрабатывать модели угроз и модели нарушителя компьютерных си стем; Владеть: практическими навыками разработки модели угроз и модели нарушителя компьютерных систем
				Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: определять основные угрозы безопасности информации и разрабатывать модели угроз и модели нарушителя компьютерных систем; Владеть: навыками определения основных угроз безопасности информации и разработки модели угроз и модели нарушителя компьютерных систем
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: порядок разработки модели угроз и модели нарушителя компью терных систем; уметь: определить необходимые компоненты модели угроз и модели нарушителя компьютерных систем; владеть: практическими навыками разработки модели угроз и модели нарушителя компьютерных систем
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно сти; - нормативные правовые акты для профессиональной дея тельности; - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - сущность и понятия лицензи рования в области обеспече ния защиты государственной тайны, технической защиты конфиденциальной информа ции, по аттестации объектов информатизации и сертифи кации средств защиты инфор мации, характеристики их со ставляющих; -

					методы определения требо□ваний к защите информации; - принципы формирования комплекса мер по обеспече□нию информационной без□опасности предприятия (орга□низации);- способы обеспечения за□щиты и безопасности ИС. Уметь: - использовать правовые зна□ния в различных сферах дея□тельности; - использовать нормативные правовые акты в профессио□нальной деятельности; - классифицировать защищае□мую информацию по видам тайны и степеням конфиден□циальности; - определять классы защи□щенности автоматизирован□ных систем и средств вычис□лительной техники, применять методы и средства проектиро□вания программного обеспе□чения, используемые при со□здании защищенных компью□терных систем, методы опре□деления требований к защите информации; - проводить анализ информа□ционной безопасности объек□тов и систем на соответствие требованиям стандартов в об□ласти информационной без□опасности. Владеть: - навыками определения ос□новных характеристик при ли□цензировании в области обес□печения защиты государ□ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□щиты информации; - навыками применения пра□вовых знаний в различных сферах деятельности; - навыками применения нор□мативных правовых актов в профессиональной деятель□ности; - навыками проведения ана□лиза информационной без□опасности объектов и систем на соответствие требованиям стандартов в области инфор□мационной безопасности; - международно-правовой тер□минологией; - навыками работы с междуна□родно-правовыми актами, нормативными правовыми ак□тами России; - навыками сравнительного анализа российской модели регулирования информацион□ных отношений с междуна□родно-правовыми стандар□тами и аналогичными институ□тами зарубежных стран; - практическими навыками ис□пользования

					инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-6.7. Умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Владеть: навыками разработки проектов инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: особенности формирования документов по защите информации ограниченного доступа в организа□ ции; уметь: применять знания об объекте при разработке документов по защи□ те информации ограниченного до□ ступа в организации; владеть: практическими навыками по разработке документов по защите информации ограниченного доступа в организации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно□сти; - нормативные правовые акты для профессиональной дея□ тельности; - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - сущность и понятия лицензи□ рования в области обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; - методы определения требо□ ваний к защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия (орга□ низации);- способы обеспечения за□ щиты и безопасности ИС. Уметь: - использовать правовые зна□ ния в различных сферах дея□ тельности; - использовать нормативные правовые акты в профессио□ нальной деятельности; - классифицировать

					защищае мую информацию по видам тайны и степеням конфиден циальности; - определять классы защи щенности автоматизирован ных систем и средств вычис лительной техники, применять методы и средства проектиро вания программного обеспе чения, используемые при со здании защищенных компью терных систем, методы опре деления требований к защите информации; - проводить анализ информа ционной безопасности объек тов и систем на соответствие требованиям стандартов в об ласти информационной без опасности. Владеть: - навыками определения ос новных характеристик при ли цензировании в области обес печения защиты государ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за щиты информации; - навыками применения пра вовых знаний в различных сферах деятельности; - навыками применения нор мативных правовых актов в профессиональной деятель ности; - навыками проведения ана лиза информационной без опасности объектов и систем на соответствие требованиям стандартов в области инфор мационной безопасности; - международно-правовой тер минологией; - навыками работы с междуна родно-правовыми актами, нормативными правовыми ак тами России; - навыками сравнительного анализа российской модели регулирования информацион ных отношений с междуна родно-правовыми стандар тами и аналогичными институ тами зарубежных стран; - практическими навыками ис пользования инструменталь ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-6.8. Умеет определить политику контроля доступа работников к информации ограниченного доступа.	Б1.О.40 Модели безопасности компьютерных систем	Знать: руководящие документы ФСТЭК России (Гостехкомиссии России). Уметь; определить политику контроля доступа работников к информации ограниченного доступа. Владеть: практическими навыками определения политики контроля досту па работников к информации ограни ченного доступа.

				Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: определить политику контроля доступа работников к информации ограниченного доступа на основе анализа действующих положений законодательства, нормативных правовых актов и методических рекомендаций Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Владеть: определения политики контроля доступа работников к информации ограниченного доступа
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: особенности формирования документов по защите информации ограниченного доступа в организа ции; уметь: применять знания об объекте при разработке документов по защи□ те информации ограниченного до□ ступа в организации; владеть: практическими навыками по разработке документов по защите информации ограниченного доступа в организации
			ОПК-6.9. Умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации.	Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю Владеть: навыками определения основных требований, предъявляемых к физической защите объекта и пропускному режиму в организации
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные требования, предъ□ являемые к физической защите объ□ екта и пропускному режиму в органи□ зации; уметь: предъявлять требования к физической защите объекта и про□ пускному режиму в организации; владеть: практическими навыками по разработке требований, предъяв□ ляемых к физической защите объек□ та и пропускному режиму в органи□ зации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и	Знать: - основы правовых знаний в различных сферах деятельно□ сти; - нормативные правовые акты для профессиональной дея□ тельности; - стандарты информационной безопасности и руководящие документы ФСТЭК России

				навыков в области профессиональной деятельности	(Гостехкомиссии России); - сущность и понятия лицензи□ рования в области обеспече□ ния защиты государственной тайны, технической защиты конфиденциальной информа□ ции, по аттестации объектов информатизации и сертифи□ кации средств защиты инфор□ мации, характеристики их со□ ставляющих; - методы определения требо□ ваний к защите информации; - принципы формирования комплекса мер по обеспече□ нию информационной без□ опасности предприятия (орга□ низации);- способы обеспечения за□ щиты и безопасности ИС. Уметь: - использовать правовые зна□ ния в различных сферах дея□ тельности; - использовать нормативные правовые акты в профессио□ нальной деятельности; - классифицировать защищае□ мую информацию по видам тайны и степеням конфиден□ циальности; - определять классы защи□ щенности автоматизирован□ ных систем и средств вычис□ лительной техники, применять методы и средства проектиро□ вания программного обеспе□ чения, используемые при со□ здании защищенных компью□ терных систем, методы опре□ деления требований к защите информации; - проводить анализ информа□ ционной безопасности объек□ тов и систем на соответствие требованиям стандартов в об□ ласти информационной без□ опасности. Владеть: - навыками определения ос□ новных характеристик при ли□ цензировании в области обес□ печения защиты государ□ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за□ щиты информации; - навыками применения пра□ вовых знаний в различных сферах деятельности; - навыками применения нор□ мативных правовых актов в профессиональной деятель□ ности; - навыками проведения ана□ лиза информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности; - международно-правовой тер□ минологией; - навыками работы с междуна□ родно-

					правовыми актами, нормативными правовыми ак□ тами России; - навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно правовыми стандар□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
			ОПК-6.10. Умеет применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.	Б1.О.40 Модели безопасности компьютерных систем	Знать: стандарты информационной безопасности и руководящие докумен□ ты ФСТЭК России (Гостехкомиссии России). Уметь; применять отечественные и за□ рубежные стандарты в области компь□ ютерной безопасности для проектиро□ вания, разработки и оценивания защи□ щенности компьютерной системы Владеть: практическими навыками применения отечественных и зарубеж□ ных стандартов в области компьютер□ ной безопасности для проектирования, разработки и оценивания защищенно□ сти компьютерной системы
				Б1.О.49 Организационное и правовое обеспечение информационной безопасности	Уметь: применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы; Владеть: навыками применения отечественных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы
				Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные положения отече□ ственных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компью□ терной системы; уметь: анализировать положения отечественных и зарубежных стан□ дартов в области компьютерной без□ опасности для проектирования, раз□ работки и оценивания защищенности компьютерной системы; владеть: практическими навыками по применению отечественных и за□ рубежных стандартов в области ком□ пьютерной безопасности для проек□ тирования, разработки и оценивания защищенности компьютерной систе□ мы

				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основы правовых знаний в различных сферах деятельно сти; - нормативные правовые акты для профессиональной дея тельности; - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - сущность и понятия лицензи рования в области обеспече ния защиты государственной тайны, технической защиты конфиденциальной информа ции, по аттестации объектов информатизации и сертифи кации средств защиты инфор мации, характеристики их со ставляющих; - методы определения требо ваний к защите информации; - принципы формирования комплекса мер по обеспече нию информационной без опасности предприятия (орга низации); - способы обеспечения за щиты и безопасности ИС. Уметь: - использовать правовые зна ния в различных сферах дея тельности; - использовать нормативные правовые акты в профессио нальной деятельности; - классифицировать защищае мую информацию по видам тайны и степеням конфиден циальности; - определять классы защи щенности автоматизирован ных систем и средств вычис лительной техники, применять методы и средства проектиро вания программного обеспе чения, используемые при со здании защищенных компью терных систем, методы опре деления требований к защите информации; - проводить анализ информа ционной безопасности объек тов и систем на соответствие требованиям стандартов в об ласти информационной без опасности. Владеть: - навыками определения ос новных характеристик при ли цензировании в области обес печения защиты государ ственной тайны, технической защиты конфиденциальной информации, при аттестации объектов информатизации и сертификации средств за щиты информации; - навыками применения пра вовых знаний в различных сферах деятельности; - навыками применения нор мативных правовых актов в профессиональной деятель ности; - навыками проведения ана лиза

					информационной без□ опасности объектов и систем на соответствие требованиям стандартов в области инфор□ мационной безопасности; - международно-правовой тер□ минологией; - навыками работы с междуна□ родно-правовыми актами, нормативными правовыми ак□ тами России; - навыками сравнительного анализа российской модели регулирования информацион□ ных отношений с междуна□ родно-правовыми стандар□ тами и аналогичными институ□ тами зарубежных стран; - практическими навыками ис□ пользования инструменталь□ ных интеллектуальных систем для обоснования требований к защите информации.
	ОПК-7	Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ;	ОПК-7.1. Знает общие принципы построения, области и особенности применения языков программирования высокого уровня.	Б1.О.35 Объектно-ориентированное программирование	Знать: общие принципы объектно□ ориентированного программирования.
				Б1.О.36 Введение в программирование	Знать: общие принципы построения, области и особенности применения языков программирования высокого уровня
				Б1.О.37 Методы программирования	Знать: общие принципы построения, области и особенности применения языков программирования высокого уровня.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния

					логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ; - принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками

					разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ.
			ОПК-7.2. Знает язык программирования высокого уровня (объектно-ориентированное программирование).	Б1.О.35 Объектно-ориентированное программирование	Знать: объектно-ориентированный язык программирования C#.
				Б1.О.36 Введение в программирование	Знать: объектно-ориентированный язык программирования
				Б1.О.55 Дисциплины специализации	
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ления памятью ЭВМ; - фундаментальные принципы по□вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□туру их основных типов; - определения и понимать суть та□ких понятий как алгоритм, типы и структуры данных, управление па□мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки

					данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в сре-дах разра□ботки программ; - принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для ре-шения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ.
			ОПК-7.3. Знает язык ассемблера	Б1.О.35 Объектно-ориентированное программировани	Знать: принципы представления данных в объектно□ ориентированном языке программирования

			персонального компьютера.	е	
				Б1.О.36 Введение в программировани е	Знать: язык ассемблера персонального компьютера
				Б1.О.37 Методы программировани я	Знать: язык ассемблера персонального компьютера
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы оформления и структу□ рирования программного кода; - правила

					математической логики, для составления логических выра жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни ческих компьютерных средств, тре бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож ность алгоритмов. Владеть: - навыками самостоятельной ра боты с компьютером, программи рования на машинно-ориентиро ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин формационных систем и техноло гий; - навыками разработки программ; - навыками разработки, документи рования, тестирования и отладки программ; - навыками документирования про граммного кода в виде коммента риев; - навыками тестирование и от ладки программ.
			ОПК-7.4. Умеет работать с интегрированной средой разработки программного обеспечения.	Б1.О.35 Объектно-ориентированное программирование	Уметь: работать со средой программирования языка программирования C#
				Б1.О.36 Введение в программирование	Уметь: работать с интегрированной средой разработки программного обеспечения
				Б1.О.37 Методы программирования	Уметь: работать с интегрированной средой разработки программного обеспечения
				Б1.О.55.04 Интеллектуальны	знать: • современные средства разработки программного

				е системы обработки информации	обеспечения на языках высокого уровня для задач интеллектуальных систем обработки информации; уметь: • выбирать необходимые инструментальные средства для разработки программ в различных ОС и средах; • формализовать поставленную задачу; • разрабатывать прикладные интеллектуальные системы для обработки различных видов информации. владеть; • навыками использования библиотек прикладных программ, программных сред разработки интеллектуальных программных систем
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием

					коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач;- принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ.
			ОПК-7.5. Умеет разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых	Б1.О.35 Объектно-ориентированное программирование	Уметь: разрабатывать и реализовывать решения задач на объектно-ориентированном языке
				Б1.О.36 Введение в программирование	Уметь: разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач

			профессиональных задач.	Б1.О.37 Методы программировани я	Уметь: разрабатывать и реализовывать на языке высокого уровня алгоритмы решения типовых профессиональных задач.
				Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б1.О.55 Дисципл лины специализации	
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена

					информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки

					программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ.
			ОПК-7.6. Владеет навыками разработки, документирования, тестирования и отладки программ.	Б1.О.35 Объектно-ориентированное программирование	Владеть: навыками разработки, документирования, тестирования и отладки программ
				Б1.О.36 Введение в программирование	Владеть: навыками разработки, документирования, тестирования и отладки программ.
				Б1.О.37 Методы программирования	Владеть: навыками разработки, документирования, тестирования и отладки программ.
				Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных

					программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б1.О.55.04 Интеллектуальные системы обработки информации	владеет: • навыками формализации знаний, разработки баз знаний, онтологий; • навыками разработки, тестирования, отлаживания и оформления программ на языках высокого уровня, включая языки логического программирования; • навыками организации процесса разработки программного обеспечения интеллектуальных систем обработки информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в

					программах; - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов. Владеть: - навыками самостоятельной ра□боты с компьютером,

					программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ.
			ОПК-7.7. Знает базовые структуры данных.	Б1.О.35 Объектно-ориентированное программирование	Знать: базовые структуры данных объектно-ориентированного языка
				Б1.О.36 Введение в программирование	Знать: базовые структуры данных
				Б1.О.37 Методы программирования	Знать: базовые структуры данных
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: базовые классы, реализующие структуры в языке C#, динамические структуры данных (стеки, очереди), деревья, графы. Уметь: применять базовые классы, реализующие структуры на языке C#, динамические структуры данных (стеки, очереди), деревья графы. Владеть (иметь навык(и)): Базовыми классами, реализующими структуры на языке C#, динамические структуры данных (стеки, очереди), деревья графы.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ления памятью ЭВМ; - фундаментальные принципы по□вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□туру их основных типов; - определения и понимать суть та□ких понятий как алгоритм, типы и структуры данных, управление па□мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в

					массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов.

					Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ.
			ОПК-7.8. Знает основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико-графовые алгоритмы.	Б1.О.35 Объектно-ориентированное программировани е	Знать: основныем алгоритмы сортировки и поиска данных, комбинаторные и теретико□ графовые алгоритмы.
				Б1.О.36 Введение в программировани е	Знать: основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико□ графовые алгфитмы.
				Б1.О.37 Методы программировани я	Знать основные алгоритмы сортировки и поиска данных, комбинаторные и теоретико□ графовые алгоритмы.
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: основные алгоритмы сортировки и поиска данных, рекурсивные алгоритмы, алгоритмы с возвратом, применяемые в комбинаторных алгоритмах и алгоритмах на графах. Уметь: реализовать алгоритмы сортировки и поиска данных, рекурсивные алгоритмы, алгоритмы с возвратом, применяемые в комбинаторных алгоритмах и алгоритмах на графах. Владеть (иметь навык(и)): алгоритмами сортировки и поиска данных, рекурсивные алгоритмы и алгоритмы с возвратом, применяемые в комбинаторных алгоритмах и алгоритмах на графах.
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы

					и структуры данных, управление па□мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками

					и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ.
			ОПК-7.9. Знает общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения.	Б1.О.35 Объектно-ориентированное программирование	Знать: общие сведения о методах проектирования объектно□ ориентированных программ, документирования с использованием комментариев и мета-данных, разработки, тестирования и отладки программ.
				Б1.О.36 Введение в программирование	Знать: общие сведения о методах проектирования, документирования, тестирования и отладки программного обеспечения
				Б1.О.37 Методы программирования	Знать: общие сведения о методах проектирования, документирования, разработки, тестирования и отладки программного обеспечения.
				Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности

					компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков,

					деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ.
				Б1.О.55Дисциплины специализа	

				ции	
			ОПК-7.10. Умеет применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.	Б1.О.35 Объектно-ориентированное программирование	Уметь: применять современные методы объектно-ориентированного программирования и возможности языка программирования для решения задач.
				Б1.О.36 Введение в программирование	Уметь: применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач
				Б1.О.37 Методы программирования	Уметь: применять известные методы программирования и возможности базового языка программирования для решения типовых профессиональных задач.
				Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами

					данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б1.О.55.04 Интеллектуальные системы обработки информации	знать: • методы программирования и методы разработки эффективных алгоритмов решения прикладных задач в области интеллектуальных технологий; • базовые структуры данных. уметь: проводить разработку программ с использованием библиотек прикладных программ, программных сред разработки интеллектуальных программных систем. владеть: владеет приемами программирования, отладки и тестирования на языках декларативного программирования.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; -

					способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ.
			ОПК-7.11. Владеет навыками разработки алгоритмов решения типовых профессиональных задач.	Б1.О.35 Объектно-ориентированное программировани е	Владеть: навыками разработки объектно-ориентированных алгоритмов для разработки и реализации программ.
				Б1.О.36 Введение в программировани	Владеть: навыками разработки алгоритмов решения типовых

				е	профессиональных задач
				Б1.О.37 Методы программировани я	Владеть: навыками разработки алгоритмов решения типовых профессиональных задач.
				Б1.О.55.04 Интеллектуальны е системы обработки информации	знать: • принципы проектирования и реализации систем вывода на знаниях; • основные модели представления, хранении и обработки знаний в ИС, стандарты, спецификации; • методы обработки экспертных данных; уметь: использовать методы математического моделирования, расчетные формулы, таблицы, графики, компьютерные программы при разработке прикладных интеллектуальных систем обработки различных видов информации. владеть: • навыками применения методов обработки экспертных данных; • разработки систем нечеткого вывода на знаниях; • проведения логического и семантического анализа на данных.
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур

					объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ.

			ОПК-7.12. Знает необходимые и достаточные условия оптимальности задачи математического программирования.	Б1.О.28 Методы оптимизации	Знать: методы и инструментальные средства программирования Уметь:осуществлять обоснованный выбор инструментария программирования и спосо□ бов организации программ Владеть: языками высокого и низкого уровня создания программ
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ. Уметь: - объяснять основополагающие

					принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ.
			ОПК-7.13. Умеет применять методы одномерной оптимизации при решении прикладных задач.	Б1.О.28 Методы оптимизации	Знать: методы и инструментальные средства программирования Уметь:осуществлять обоснованный выбор инструментария программирования и спосо□бов организации программ Владеть: языками высокого и низкого уровня создания программ
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ления памятью ЭВМ; - фундаментальные принципы по□вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□туру их основных типов; -

					определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать

					алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ.
			ОПК-7.14. Умеет использовать методы многомерной безусловной оптимизации при решении профессиональных задач.	Б1.О.28 Методы оптимизации	Знать: методы и инструментальные средства программирования Уметь:осуществлять обоснованный выбор инструментария программирования и спосо□ бов организации программ Владеть: языками высокого и низкого уровня создания программ
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения

					задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки

					программ.
			ОПК-7.15. Знает методы условной оптимизации при решении прикладных задач.	Б1.О.28 Методы оптимизации	Знать: методы и инструментальные средства программирования Уметь:осуществлять обоснованный выбор инструментария программирования и спосо□ бов организации программ Владеть: языками высокого и низкого уровня создания программ
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы оформления и структу□ рирования программного кода; - правила

					математической логики, для составления логических выра жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни ческих компьютерных средств, тре бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож ность алгоритмов. Владеть: - навыками самостоятельной ра боты с компьютером, программи рования на машинно-ориентиро ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин формационных систем и техноло гий; - навыками разработки программ; - навыками разработки, документи рования, тестирования и отладки программ; - навыками документирования про граммного кода в виде коммента риев; - навыками тестирование и от ладки программ.
			ОПК-7.16. Знает задачи вариационного исчисления, оптимального управления и линейного программирования.	Б1.О.28 Методы оптимизации	Знать: методы и инструментальные средства программирования Уметь:осуществлять обоснованный выбор инструментария программирования и спосо бов организации программ Владеть: языками высокого и низкого уровня создания программ
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ ления памятью ЭВМ; - фундаментальные принципы по вышения

					производительности ЭВМ; - классификацию современных компьютерных систем и архитек□туру их основных типов; - определения и понимать суть та□ких понятий как алгоритм, типы и структуры данных, управление па□мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах; - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно- ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого

					уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ.
	ОПК-8	Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей;	ОПК-8.1. Знает строение мультипликативной группы колец вычетов.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.2. Знает способы представления действительных чисел цепными дробями.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.3. Знает основные свойства символов Лежандра и Якоби.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.4. Знает критерии простоты и их использование для факторизации натуральных чисел.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов

			ОПК-8.5. Знает алгоритмы проверки чисел на простоту; построения больших простых чисел.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.6. Умеет строить большие простые числа.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.7. Умеет применять алгоритмы проверки чисел на простоту; построения больших простых чисел.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.8. Умеет применять алгоритмы разложения чисел на множители.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.9. Владеет навыками применения теории чисел в криптографии и других дисциплинах.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-8.10. Умеет разрабатывать модели безопасности компьютерных систем с использованием необходимого математического аппарата и средств компьютерного	Б1.О.40 Модели безопасности компьютерных систем	знать: стандарты информационной безопасности и руководящие докумен□ ты ФСТЭК России (Гостехкомиссии России), формальные модели безопас□ ности. уметь:. разрабатывать модели без□ опасности компьютерных систем с ис□ пользованием необходимого математи□ ческого аппарата и средств компьютер□ ного моделирования владеть:. Владеть практическими навыками разработки моделей без□ опасности компьютерных систем в сре□ де инструментальных средств

			моделирования.	Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа дан□ ных и машинного обучения в рам□ ках статистического и детерми□ нистского подходов; - технологии организации и прове□ дения статистического компьютер□ ного моделирования алгоритмов обработки информации, возможно□ сти современных программных сред для реализации исследова□ ний и разработок в области алго□ ритмов анализа данных и машин□ ного обучения;- роль и место средств математи□ ческого и имитационного модели□ рования при проектировании слож□ ных систем, применяемые при этом технологии структурно - функ□ ционального и объектного визуаль□ ного моделирования. Уметь: - использовать стандартное и ори□ гинальное программное обеспече□ ние для проведения исследований и разработок в области алгорит□ мов анализа данных и машинного обучения, формировать рекомен□ дации по принципам построения и параметрам алгоритмов в области профессиональной деятельности; - проводить синтез и анализ алго□ ритмов обработки информации для решения конкретных практиче□ ских задач, использовать матема□ тические методы в интересах ана□ литической и численной оценки ос□ новных показателей эффективно□ сти алгоритмов анализа данных и машинного обучения; - проводить разработку простей□ ших компьютерных моделей. Владеть: - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки информации в части анализа данных и машин□ ного обучения; - навыками разработки и модели□ рования алгоритмов обработки ин□ формации в современных инстру□ ментальных средах, навыками про□ ведения компьютерного экспери□ мента по оценке эффективности алгоритмов анализа данных и ма□ шинного обучения, навыками те□ стирования компьютерных моде□ лей алгоритмов обработки инфор□ мации.
			ОПК-8.11. Владеет	Б1.О.40 Модели	знать: этапы создания защищенных компьютерных систем и сетей;

			способами моделирования безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах.	безопасности компьютерных систем	фор□мальные модели безопасности компью□терных систем; методы и средства про□ектирования технологически безопасно□го программного обеспечения; методы обоснования требований и оценки за□щищенности систем обработки инфор□мации. уметь: проводить анализ формальных моделей безопасности; оценку требо□ваний к защищенным компьютерным системам и оценку эффективности их функционирования. владеть: практическими навыками ис□пользования инструментальных интел□лектуальных систем для оценки требо□ваний к защищенности компьютерных систем и эффективности их функцио□нирования; практическими навыками использования CASE-средств при ана□лизе проектных решений по обеспече□нию защищенности компьютерных си□стем.
				Б1.О.42 Основы построения защищенных компьютерных сетей	владеть: методом отладки групповых политик в режимах "результата" и "моделирования"
				Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие

					требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа дан□ ных и машинного обучения в рам□ ках статистического и детерми□ нистского подходов; - технологии организации и прове□ дения статистического компьютер□ ного моделирования алгоритмов обработки информации, возможно□ сти современных программных сред для реализации исследова□ ний и разработок в области алго□ ритмов анализа данных и машин□ ного обучения;- роль и место средств математи□ ческого и имитационного модели□ рования при проектировании слож□ ных систем, применяемые при этом технологии структурно - функ□ ционального и объектного визуаль□ ного моделирования. Уметь: - использовать стандартное и ори□ гинальное программное обеспече□ ние для проведения исследований и разработок в области алгорит□ мов анализа данных и машинного обучения, формировать рекомен□ дации по принципам построения и параметрам алгоритмов в области профессиональной деятельности; - проводить синтез и анализ алго□ ритмов обработки информации для решения конкретных практиче□ ских задач, использовать матема□ тические методы в интересах ана□ литической и численной оценки ос□ новных показателей эффективно□ сти алгоритмов анализа данных и машинного

					обучения; - проводить разработку простей□ших компьютерных моделей. Владеть: - практическими навыками разра□ботки и применения алгоритмов и технологий обработки информации в части анализа данных и машин□ного обучения; - навыками разработки и модели□рования алгоритмов обработки ин□формации в современных инстру□ментальных средах, навыками про□ведения компьютерного экспери□мента по оценке эффективности алгоритмов анализа данных и ма□шинного обучения, навыками те□стирования компьютерных моде□лей алгоритмов обработки инфор□мации.
			ОПК-8.12. Знает современные методы обработки информации и машинного обучения.	Б1.О.30 Технологии обработки информации	Знать: базовые понятия методов и технологий обра□ботки информации; современные методы и алгоритмы анализа данных и машинного обу□чения в рамках статистического и детерми□нистского подходов. Уметь: проводить синтез и анализ алгоритмов обра□ботки информации для решения конкретных практических задач, использовать математи□ческие методы в интересах аналитической и численной оценки основных показателей эф□фективности алгоритмов анализа данных и машинного обучения. Владеть: практическими навыками разработки и при□менения алгоритмов и технологий обработки информации в части анализа данных и ма□шинного обучения; навыками разработки и моделирования алгоритмов обработки ин□формации в современных инструментальных средах.
			ОПК-8.13. Умеет применять методы машинного обучения при проведении разработок в области обеспечения безопасности компьютерных систем.	Б1.О.30 Технологии обработки информации	Знать: технологии организации и проведения стати□стического компьютерного моделирования алгоритмов обработки информации, возмож□ности современных программных сред для реализации исследований и разработок в об□ласти алгоритмов анализа данных и машин ного обучения. Уметь: использовать стандартное и оригинальное программное обеспечение для проведения исследований и разработок в области алго□ритмов анализа данных и машинного обуче□ния, формировать рекомендации по принци□пам построения и параметрам алгоритмов в области профессиональной деятельности. Владеть:

					навыками проведения компьютерного экспе□ римента по оценке эффективности алгорит□ мов анализа данных и машинного обучения, навыками тестирования компьютерных моде□ лей алгоритмов обработки информации в среде Matlab.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа дан□ ных и машинного обучения в рам□ ках статистического и детерми□ нистского подходов; - технологии организации и прове□ дения статистического компьютер□ ного моделирования алгоритмов обработки информации, возможно□ сти современных программных сред для реализации исследова□ ний и разработок в области алго□ ритмов анализа данных и машин□ ного обучения;- роль и место средств математи□ ческого и имитационного модели□ рования при проектировании слож□ ных систем, применяемые при этом технологии структурно - функ□ ционального и объектного визуаль□ ного моделирования. Уметь: - использовать стандартное и ори□ гинальное программное обеспече□ ние для проведения исследований и разработок в области алгорит□ мов анализа данных и машинного обучения, формировать рекомен□ дации по принципам построения и параметрам алгоритмов в области профессиональной деятельности; - проводить синтез и анализ алго□ ритмов обработки информации для решения конкретных практиче□ ских задач, использовать матема□ тические методы в интересах ана□ литической и численной оценки ос□ новных показателей эффективно□ сти алгоритмов анализа данных и машинного обучения; - проводить разработку простей□ ших компьютерных моделей. Владеть: - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки информации в части анализа данных и машин□ ного обучения; - навыками разработки и модели□ рования алгоритмов обработки ин□ формации в современных инстру□ ментальных средах, навыками про□ ведения компьютерного экспери□ мента по оценке эффективности

					алгоритмов анализа данных и ма□ шинного обучения, навыками те□ стирования компьютерных моде□ лей алгоритмов обработки инфор□ мации.
			ОПК-8.14. Знает методологию экспериментальных исследований и испытаний.		
			ОПК-8.15. Умеет применять методы экспериментального исследования при решении профессиональных задач.	Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - базовые понятия методов обра□ ботки информации, современные методы и алгоритмы анализа дан□ ных и машинного обучения в рам□ ках статистического и детерми□ нистского подходов; - технологии организации и прове□ дения статистического компьютер□ ного моделирования алгоритмов обработки информации, возможно□ сти современных программных сред для реализации исследова□ ний и разработок в области алго□ ритмов анализа данных и машин□ ного обучения;- роль и место средств математи□ ческого и имитационного модели□ рования при проектировании слож□ ных систем, применяемые при этом технологии структурно - функ□ ционального и объектного визуаль□ ного моделирования. Уметь: - использовать стандартное и ори□ гинальное программное обеспече□ ние для проведения исследований и разработок в области алгорит□ мов анализа данных и машинного обучения, формировать рекомен□ дации по принципам построения и параметрам алгоритмов в области профессиональной деятельности; - проводить синтез и анализ алго□ ритмов обработки информации для решения конкретных практиче□ ских задач, использовать матема□ тические методы в интересах ана□ литическй и численной оценки ос□ новных показателей эффективно□ сти алгоритмов анализа данных и машинного обучения; - проводить разработку простей□ ших компьютерных моделей. Владеть: - практическими навыками разра□ ботки и применения алгоритмов и технологий обработки информации в части анализа данных и машин□ ного обучения; - навыками разработки и

					модели□рования алгоритмов обработки ин□формации в современных инстру□ментальных средах, навыками про□ведения компьютерного экспери□мента по оценке эффективности алгоритмов анализа данных и ма□шинного обучения, навыками те□стирования компьютерных моде□лей алгоритмов обработки инфор□мации.
	ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации;	ОПК-9.1. Знает технические каналы утечки информации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные принципы класси□фикации и количественных характе□ристик технических каналов утечки информации; уметь: определять основные харак□теристики технических каналов утеч□ки информации; владеть: практическими навыками классификации и определения коли□чественных характеристик техниче□ских каналов утечки информации
			ОПК-9.2. Знает возможности технических средств перехвата информации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные принципы примене□ния технических средств перехвата информации; уметь: анализировать возможные условия применения технических средств перехвата информации; владеть: практическими навыками определения характеристик техниче□ских средств перехвата информации
			ОПК-9.3. Умеет организовать защиту информации от утечки по техническим каналам на объектах информатизации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: принципы формирования по□литик безопасности для компьютер□ной инфраструктуры организации; принципы формирования процедур безопасности для заданных политик; уметь: проектировать систему защи□ты с использование программно□аппаратных средств защиты инфор□мации; формировать и анализиро□вать показатели защищенности; владеть: методами моделирования телекоммуникационных сетей; настраивать основные типы теле□коммуникационного оборудования IP сетей; основными пакетами, приме□няемыми для расчётов и моделиро□вания в телекоммуникациях
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы формирования по□литик безопасности для ком□пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации ин□формационных систем в соот□ветствии с требованиями по защите информации; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симмет□ричных и

					асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи;- основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - проектировать систему за□ щиты с использование про□ граммно аппаратных средств защиты информации; - формировать и анализиро□ вать показатели защищенно□ сти; - определять информацион□ ную инфраструктуру и инфор□ мационные ресурсы организа□ ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ ции; - составлять план управления рисками; - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы

					организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые методы и средства техниче□ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□боты с известными криптогра□фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□рации в области криптографи□ческой защиты информации при разработке ПО в области информационной безопасно□сти; - практическими навыками те□стирования и оценки стойко□сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ния количественных характе□ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□налам и контроля эффектив□ности защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации.
			ОПК-9.4. Умеет пользоваться нормативными документами в области	Б1.О.51 Защита информации от утечки по техническим каналам	знать: принципы организации ин□формационных систем в соответ□ствии с требованиями по защите ин□формации; математические основы симметричных и асимметричных

			технической защиты информации.		криптографических систем; уметь: определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; анализировать показатели качества и критерии оценки систем и отдельных методов и средств защи□ ты информации; владеть: практическими навыками применения национальных стандар□ тов Российской Федерации в области криптографической защиты инфор□ мации при разработке ПО в области информационной безопасности; практическими навыками тестирова□ния и оценки стойкости программ, использующих СКЗИ
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы формирования по□ литик безопасности для ком□ пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации ин□ формационных систем в соот□ ветствии с требованиями по защите информации; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи;- основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - проектировать систему за□ щиты с использование про□ граммно

					аппаратных средств защиты информации; - формировать и анализиро□вать показатели защищенно□сти; - определять информацион□ную инфраструктуру и инфор□мационные ресурсы организа□ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ции; - составлять план управления рисками; - классифицировать функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□стем; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - определять необходимые принципы организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые методы и средства техниче□ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□боты с известными криптогра□фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□рации в области криптографи□ческой защиты информации при разработке

					ПО в области информационной безопасно сти; - практическими навыками те стирования и оценки стойко сти программ, использующих СКЗИ; - практическими навыками классификации и определе ния количественных характе ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка налам и контроля эффектив ности защиты информации; - практическими навыками ор ганизации защиты информа ции от утечки по техническим каналам на объектах инфор матизации; - практическими навыками применения нормативных до кументов в области техниче ской защиты информации; - практическими навыками анализа и оценки угроз ин формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации.
			ОПК-9.5. Знает основные характеристики сигналов электросвязи, спектры и виды модуляции.	Б1.О.33 Сети и системы передачи информации	Знает основные характеристики каналов физического уровня. Умеет рассчитывать бюджет канала связи по его параметрам. Владеет методами моделирования каналов физического уровня
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
			ОПК-9.6. Знает принципы построения и функционирования систем и сетей передачи	Б1.О.33 Сети и системы передачи информации	Знает принципы построения сетей связи.и передачи информации Умеет классифицировать фукциональность элементов сетей связи.и передачи информации по семиуровневой модели

			информации. способы передачи и распределения информации в телекоммуникационных системах и сетях.		взаимодействия открытых систем. Владеет методами моделирования телекоммуникационных сетей.
			ОПК-9.7. Знает основные телекоммуникационные протоколы.	Б1.О.33 Сети и системы передачи информации	Знает наиболее распространённые стеки протоколов сетей связи и передаччи информации. Умеет ориентироваться в основных стандартах отрасли. Владеет методами моделирования элементов современных телекоммуникационных протоколов.
			ОПК-9.8. Умеет анализировать тенденции развития систем и сетей электросвязи, внедрения новых служб и услуг связи.	Б1.О.33 Сети и системы передачи информации	Знает осовные тренды развития телекоммуникаций. Умеет оценивать потребности пользовантеля в видах услуги и их качестве. Владеет основными пакетами, применяемыми для рассчётов и моделирования в телекоммуникациях.
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□номерности, связанные с получе□нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□онных системах при обеспечении защиты информации. уметь: производить оценку тех□нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□стики состояния устройств защи□ты информации знать: функциональное назначе□ние и принципы работы основных блоков современных средств за□щиты информации уметь: выполнять работы по вос□становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ций владеть: навыками восстановле□ния штатного режима работы технических средств защиты ин□формации
			ОПК-9.9. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем.	Б1.О.42 Основы построения защищенных компьютерных сетей	уметь: разрабатывать политики и процедуры безопасности в области компьютерных сетей
				Б2.О.06(П) Производственная практика по получению профессиональных умений и	Знать: - принципы формирования по□литик безопасности для ком□пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации ин□формационных систем в

				навыков в области профессиональной деятельности	соот□ ветствии с требованиями по защите информации; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи;- основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - проектировать систему за□ щиты с использование про□ граммно аппаратных средств защиты информации; - формировать и анализиро□ вать показатели защищенно□ сти; - определять информацион□ ную инфраструктуру и инфор□ мационные ресурсы организа□ ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ ции; - составлять план управления рисками; - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; -

					определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - определять необходимые принципы организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые методы и средства техниче□ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□боты с известными криптогра□фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□рации в области криптографи□ческой защиты информации при разработке ПО в области информационной безопасно□сти; - практическими навыками те□стирования и оценки стойко□сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ния количественных характе□ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□налам и контроля эффектив□ности защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации.

			ОПК-9.10. Знает общие и специфические угрозы безопасности баз данных.	Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
			ОПК-9.11. Знает основные тенденции развития методов защиты информации в операционных системах и	Б1.О.41 Защита в операционных системах	Знает основные тенденции развития методов защиты информации в операционных системах и системах управления базами данных
				Б1.О.42 Основы построения	знать: методологию проектирования СЗИ на основе анализа рисков

			системах управления базами данных.	защищенных компьютерных сетей	
				Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
			ОПК-9.12. Знает общие и специфические угрозы	Б1.О.41 Защита в операционных системах	Знает общие и специфические угрозы безопасности операционных систем и систем управления баз данных

			безопасности операционных систем и систем управления баз данных.	Б1.О.42 Основы построения защищенных компьютерных сетей	знать: классификацию угроз в контексте проектирования СЗИ
				Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.

			ОПК-9.13. Знает способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: принципы построения сетей связи и передачи информации; принципы взаимодействия телеком□ муникационных систем согласно принципам взаимодействия откры□ тых систем; основные тренды разви□ тия телекоммуникаций; владеть: методами и средствами технической защиты информации
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых систем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симметрич□ ных и асимметричных крипто□ графических систем, принципы генерации, хранения и исполь□ зования криптографических ключей, принципы создания электронных подписей при ре□ шении задач аутентификации, механизм работы хеш-функ□ ций, современные стандарты шифрования, хеширования, электронной подписи; - основные принципы класси□ фикации и количественных ха□ рактеристик технических кана□ лов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной без□ опасности объекта информа□ тизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели вза□ имодействия открытых систем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности поль□ зователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства

					(криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации защиты информации от утечки по тех□ ническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые ме□ тоды и средства технической защиты информации. Владеть: - методами моделирования те□ лекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз инфор□ мационной безопасности объ□ екта информатизации; -

					практическими навыками применения методов и средств технической защиты информации
			ОПК-9.14. Знает основы физической защиты объектов информатизации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: принципы работы симметрич□ ных и асимметричных криптографи□ ческих систем, принципы генерации, хранения и использования крипто□ графических ключей, принципы со□ здания электронных подписей при решении задач аутентификации, ме□ ханизм работы хеш-функций, совре□ менные стандарты шифрования, хе□ ширования, электронной подписи; владеть: методами расчета и ин□ струментального контроля показате□ лей эффективности технической за□ щиты информации
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых систем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симметрич□ ных и асимметричных крипто□ графических систем, принципы генерации, хранения и исполь□ зования криптографических ключей, принципы создания электронных подписей при ре□ шении задач аутентификации, механизм работы хеш-функ□ ций, современные стандарты шифрования, хеширования, электронной подписи; - основные принципы класси□ фикации и количественных ха□ рактеристик технических кана□ лов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной без□ опасности объекта информа□ тизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели вза□ имодействия

					открытых систем; - настраивать основные типы телекоммуникационного обо рудования IP сетей; - оценивать потребности поль зователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех ническим каналам и контроля эффективности защиты ин формации; - определять необходимые принципы организации защиты информации от утечки по тех ническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни ческой защиты информации; - определить опасные угрозы информационной безопасно сти объекта информатизации; - определить необходимые ме тоды и средства технической защиты информации. Владеть: - методами моделирования те лекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо рудования IP сетей; - основными пакетами, приме няемыми для расчётов и мо делирования в телекоммуни кациях; - практическими навыками применения современных криптографических алгорит мов и протоколов; - практическими навыками ра боты с известными криптогра фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде рации в области криптографи ческой защиты информации при разработке ПО в области информационной безопасно сти; - практическими навыками те стирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим кана лам и контроля эффективно сти защиты информации; - практическими навыками ор ганизации защиты

					информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз инфор□ мационной безопасности объ□ екта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-9.15. Умеет анализировать и оценивать угрозы информационной безопасности объекта.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: - принципы формирования политик безопасности для компью□ терной инфраструктуры организации; принципы формирования процедур безопасности для заданных политик; уметь: проектировать систему защи□ ты с использование программно□ аппаратных средств защиты инф мации; формировать и анализиро□ вать показатели защищенности; владеть: методами моделирования телекоммуникационных сетей; - настраивать основные типы теле□ коммуникационного оборудования IP сетей
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - принципы формирования политик безопасности для компьютерной инфраструктуры организации; - принципы формирования проце□ дур безопасности для заданных политик; - принципы организации информа□ ционных систем в соответствии с требованиями по защите инфор□ мации; - математические основы симмет□ ричных и асимметричных крипто□ графических систем; - принципы работы симметричных и асимметричных криптографиче□ ских систем, принципы генерации, хранения и использования крипто□ графических ключей, принципы со□ здания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, современные стандарты шифрова□ ния, хеширования, электронной подписи; - основные принципы классифика□ ции и количественных характери□ стик технических каналов утечки информации; - основные способы и средства за□ щиты информации от утечки по техническим каналам и контроля эффективности защиты информа□ ции; - основы принципов организации защиты информации от утечки по техническим каналам на объектах

					информатизации; - основные нормативные докумен□тами в области технической за□щиты информации; - угрозы информационной безопас□ности объекта информатизации; - методы и средства технической защиты информации. Уметь: - проектировать систему защиты с использование программно-аппа□ратных средств защиты информа□ции; - формировать и анализировать показатели защищенности; - определять информационную ин□фраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели каче□ства и критерии оценки систем и отдельных методов и средств за□щиты информации; - составлять план управления рис□ками; - классифицировать функциональ□ность элементов сетей связи и пе□редачи информации по семиуров□невой модели взаимодействия от□крытых систем; - настраивать основные типы теле□коммуникационного оборудования IP сетей; - оценивать потребности пользова□теля в видах услуги и их качестве; - устанавливать, настраивать и ис□пользовать на практике специали□зированные криптографические программные средства (криптогра□фические библиотеки OpenSSL, cryptopp и пр.); - применять математические мо□дели для оценки стойкости СКЗИ; - определять необходимые спо□собы и средства защиты информа□ции от утечки по техническим кана□лам и контроля эффективности за□щиты информации; - определять необходимые прин□ципы организации защиты инфор□мации от утечки по техническим каналам на объектах информати□зации; - определить необходимые и поль□зоваться нормативными докумен□тами в области технической за□щиты информации; - определить опасные угрозы ин□формационной безопасности объ□екта информатизации; - определить необходимые методы и средства технической защиты информации. Владеть: - методами моделирования теле□коммуникационных сетей; - настраивать основные типы теле□коммуникационного оборудования IP сетей; - основными пакетами, применяе□мыми для расчётов и моделирова□ния в телекоммуникациях; - практическими

					навыками приме□нения современных криптографи□ческих алгоритмов и протоколов; - практическими навыками работы с известными криптографическими библиотеками; - практическими навыками приме□нения национальных стандартов Российской Федерации в области криптографической защиты инфор□мации при разработке ПО в обла□сти информационной безопасно□сти; - практическими навыками тести□рования и оценки стойкости про□грамм, использующих СКЗИ; - практическими навыками класси□фикации и определения количе□ственных характеристик техниче□ских каналов утечки информации; - практическими навыками приме□нения способов и средств защиты информации от утечки по техниче□ским каналам и контроля эффек□тивности защиты информации; - практическими навыками органи□зации защиты информации от утечки по техническим каналам на объектах информатизации; - практическими навыками приме□нения нормативных документов в области технической защиты ин□формации; - практическими навыками анализа и оценки угроз информационной безопасности объекта информати□зации; - практическими навыками приме□нения методов и средств техниче□ской защиты информации.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си□стем согласно принципам вза□имодействия открытых систем; - основные тренды развития телекоммуникаций; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симметрич□ных и асимметричных крипто□графических систем, принципы генерации, хранения и исполь□зования криптографических ключей, принципы создания электронных подписей при ре□шении задач аутентификации, механизм работы хеш-функ□ций, современные стандарты шифрования, хеширования, электронной подписи; - основные принципы класси□фикации и количественных ха□рактеристик технических кана□лов утечки информации; - основные способы и сред□ства

					защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской защиты информации; - угрозы информационной без□опасности объекта информа□тизации; - методы и средства техниче□ской защиты информации. Уметь: - классифицировать функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели вза□имодействия открытых систем; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - оценивать потребности поль□зователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - определять необходимые принципы организации защиты информации от утечки по тех□ническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые ме□тоды и средства технической защиты информации. Владеть: - методами моделирования те□лекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□боты с известными криптогра□фическими библиотеками; - практическими навыками

					применения национальных стандартов Российской Федерации в области криптографической защиты информации при разработке ПО в области информационной безопасности; - практическими навыками тестирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; - практическими навыками организации защиты информации от утечки по техническим каналам на объектах информатизации; - практическими навыками применения нормативных документов в области технической защиты информации; - практическими навыками анализа и оценки угроз информационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-9.16. Владеет методами и средствами технической защиты информации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: основные принципы классификации и количественных характеристик технических каналов утечки информации; основные способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; уметь: оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные криптографические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); владеть: практическими навыками тестирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических каналов утечки информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - принципы формирования политик безопасности для компьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации информационных систем в соответствии

					с требованиями по защите инфор□мации; - математические основы симмет□ричных и асимметричных крипто□графических систем; - принципы работы симметричных и асимметричных криптографиче□ских систем, принципы генерации, хранения и использования крипто□графических ключей, принципы со□здания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, современные стандарты шифрова□ния, хеширования, электронной подписи; - основные принципы классифика□ции и количественных характери□стик технических каналов утечки информации; - основные способы и средства за□щиты информации от утечки по техническим каналам и контроля эффективности защиты информа□ции; - основы принципов организации защиты информации от утечки по техническим каналам на объектах информатизации; - основные нормативные докумен□тами в области технической за□щиты информации; - угрозы информационной безопас□ности объекта информатизации; - методы и средства технической защиты информации. Уметь: - проектировать систему защиты с использование программно-аппа□ратных средств защиты информа□ции; - формировать и анализировать показатели защищенности; - определять информационную ин□фраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели каче□ства и критерии оценки систем и отдельных методов и средств за□щиты информации; - составлять план управления рис□ками; - классифицировать функциональ□ность элементов сетей связи и пе□редачи информации по семиуров□невой модели взаимодействия от□крытых систем; - настраивать основные типы теле□коммуникационного оборудования IP сетей; - оценивать потребности пользова□теля в видах услуги и их качестве; - устанавливать, настраивать и ис□пользовать на практике специали□зированные криптографические программные средства (криптогра□фические библиотеки OpenSSL, cryptopp и пр.); - применять математические мо□дели для оценки стойкости СКЗИ;

					- определять необходимые спо□ собы и средства защиты информа□ ции от утечки по техническим кана□ лам и контроля эффективности за□ щиты информации; - определять необходимые прин□ ципы организации защиты инфор□ мации от утечки по техническим каналам на объектах информати□ зации; - определить необходимые и поль□ зоваться нормативными докумен□ тами в области технической за□ щиты информации; - определить опасные угрозы ин□ формационной безопасности объ□ екта информатизации; - определить необходимые методы и средства технической защиты информации. Владеть: - методами моделирования теле□ коммуникационных сетей; - настраивать основные типы теле□ коммуникационного оборудования IP сетей; - основными пакетами, применяе□ мыми для расчётов и моделирова□ ния в телекоммуникациях; - практическими навыками приме□ нения современных криптографи□ ческих алгоритмов и протоколов; - практическими навыками работы с известными криптографическими библиотеками; - практическими навыками приме□ нения национальных стандартов Российской Федерации в области криптографической защиты инфор□ мации при разработке ПО в обла□ сти информационной безопасно□ сти; - практическими навыками тести□ рования и оценки стойкости про□ грамм, использующих СКЗИ; - практическими навыками класси□ фикации и определения количе□ ственных характеристик техниче□ ских каналов утечки информации; - практическими навыками приме□ нения способов и средств защиты информации от утечки по техниче□ ским каналам и контроля эффек□ тивности защиты информации; - практическими навыками органи□ зации защиты информации от утечки по техническим каналам на объектах информатизации; - практическими навыками приме□ нения нормативных документов в области технической защиты ин□ формации; - практическими навыками анализа и оценки угроз информационной безопасности объекта информати□ зации; - практическими навыками приме□ нения методов и средств техниче□ ской защитыинформации.

				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых систем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симметрич□ ных и асимметричных крипто□ графических систем, принципы генерации, хранения и исполь□ зования криптографических ключей, принципы создания электронных подписей при ре□ шении задач аутентификации, механизм работы хеш-функ□ ций, современные стандарты шифрования, хеширования, электронной подписи; - основные принципы класси□ фикации и количественных ха□ рактеристик технических кана□ лов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной без□ опасности объекта информа□ тизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели вза□ имодействия открытых систем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности поль□ зователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы

					организации защиты информации от утечки по тех□ническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые ме□ тоды и средства технической защиты информации. Владеть: - методами моделирования те□ лекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз инфор□ мационной безопасности объ□ екта информатизации; - практическими навыками применения методов и средств технической защиты информации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и	Знать: - принципы формирования по□ литик безопасности для ком□ пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; -

				навыков в области профессиональной деятельности	принципы организации ин□ формационных систем в соот□ ветствии с требованиями по защите информации; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - проектировать систему за□ щиты с использование про□ граммно аппаратных средств защиты информации; - формировать и анализиро□ вать показатели защищенно□ сти; - определять информацион□ ную инфраструктуру и инфор□ мационные ресурсы организа□ ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ ции; - составлять план управления рисками; - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); -

					применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - определять необходимые принципы организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые методы и средства техниче□ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□боты с известными криптогра□фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□рации в области криптографи□ческой защиты информации при разработке ПО в области информационной безопасно□сти; - практическими навыками те□стирования и оценки стойко□сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ния количественных характе□ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□налам и контроля эффектив□ности защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств

					технической защиты информации.
			ОПК-9.17. Владеет методами расчета и инструментального контроля показателей эффективности технической защиты информации.	Б1.О.51 Защита информации от утечки по техническим каналам	знать: угрозы информационной без□ опасности объекта информатизации; методы и средства технической за□ щиты информации. уметь: определить опасные угрозы информационной безопасности объ□ екта информатизации; определить необходимые методы и средства технической защиты информации. владеть: практическими навыками анализа и оценки угроз информаци□ онной безопасности объекта инфор□ матизации; - практическими навыками примене□ ния методов и средств технической защиты информации.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - принципы формирования политик безопасности для компьютерной инфраструктуры организации; - принципы формирования проце□ дур безопасности для заданных политик; - принципы организации информа□ ционных систем в соответствии с требованиями по защите инфор□ мации; - математические основы симмет□ ричных и асимметричных крипто□ графических систем; - принципы работы симметричных и асимметричных криптографиче□ ских систем, принципы генерации, хранения и использования крипто□ графических ключей, принципы со□ здания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, современные стандарты шифрова□ ния, хеширования, электронной подписи; - основные принципы классифика□ ции и количественных характери□ стик технических каналов утечки информации; - основные способы и средства за□ щиты информации от утечки по техническим каналам и контроля эффективности защиты информа□ ции; - основы принципов организации защиты информации от утечки по техническим каналам на объектах информатизации; - основные нормативные докумен□ тами в области технической за□ щиты информации; - угрозы информационной безопас□ ности объекта информатизации; - методы и средства технической защиты информации. Уметь: - проектировать систему защиты с использование программно-аппа□ ратных средств защиты информа□ ции; - формировать и

					анализировать показатели защищенности; - определять информационную ин□ фраструктуру и информационные ресурсы организации, подлежащие защите; - анализировать показатели каче□ ства и критерии оценки систем и отдельных методов и средств за□ щиты информации; - составлять план управления рис□ ками; - классифицировать функциональ□ ность элементов сетей связи и пе□ редачи информации по семиуров□ невой модели взаимодействия от□ крытых систем; - настраивать основные типы теле□ коммуникационного оборудования IP сетей; - оценивать потребности пользова□ теля в видах услуги и их качестве; - устанавливать, настраивать и ис□ пользовать на практике специали□ зированные криптографические программные средства (криптогра□ фические библиотеки OpenSSL, cryptopp и пр.); - применять математические мо□ дели для оценки стойкости СКЗИ; - определять необходимые спо□ собы и средства защиты информа□ ции от утечки по техническим кана□ лам и контроля эффективности за□ щиты информации;- определять необходимые прин□ ципы организации защиты инфор□ мации от утечки по техническим каналам на объектах информати□ зации; - определить необходимые и поль□ зоваться нормативными докумен□ тами в области технической за□ щиты информации;- определить опасные угрозы ин□ формационной безопасности объ□ екта информатизации;- определить необходимые методы и средства технической защиты информации. Владеть: - методами моделирования теле□ коммуникационных сетей; - настраивать основные типы теле□ коммуникационного оборудования IP сетей; - основными пакетами, применяе□ мыми для расчётов и моделирова□ ния в телекоммуникациях; - практическими навыками приме□ нения современных криптографи□ ческих алгоритмов и протоколов; - практическими навыками работы с известными криптографическими библиотеками; - практическими навыками приме□ нения национальных стандартов Российской Федерации в области криптографической защиты инфор□ мации при разработке ПО в обла□ сти информационной безопасно□ сти;-

					практическими навыками тести□рования и оценки стойкости про□граммы, использующих СКЗИ; - практическими навыками класси□фикации и определения количе□ственных характеристик техниче□ских каналов утечки информации; - практическими навыками приме□нения способов и средств защиты информации от утечки по техниче□ским каналам и контроля эффек□тивности защиты информации; - практическими навыками органи□зации защиты информации от утечки по техническим каналам на объектах информатизации; - практическими навыками приме□нения нормативных документов в области технической защиты ин□формации; - практическими навыками анализа и оценки угроз информационной безопасности объекта информати□зации; - практическими навыками приме□нения методов и средств техниче□ской защиты информации.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си□стем согласно принципам вза□имодействия открытых систем; - основные тренды развития телекоммуникаций; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симметрич□ных и асимметричных крипто□графических систем, принципы генерации, хранения и исполь□зования криптографических ключей, принципы создания электронных подписей при ре□шении задач аутентификации, механизм работы хеш-функ□ций, современные стандарты шифрования, хеширования, электронной подписи; - основные принципы класси□фикации и количественных ха□рактеристик технических кана□лов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской защиты информации; - угрозы информационной без□опасности

					объекта информа□ тизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели вза□ имодействия открытых систем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности поль□ зователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации защиты информации от утечки по тех□ ническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые ме□ тоды и средства технической защиты информации. Владеть: - методами моделирования те□ лекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойкости программ, использующих СКЗИ; - практическими навыками классификации и определения количественных характеристик технических

					каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз инфор□мационной безопасности объ□екта информатизации; - практическими навыками применения методов и средств технической защиты информации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы формирования по□литик безопасности для ком□пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации ин□формационных систем в соот□ветствии с требованиями по защите информации; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симмет□ричных и асимметричных криптографических систем, принципы генерации, хране□ния и использования крипто□графических ключей, прин□ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□менные стандарты шифрова□ния, хеширования, электрон□ной подписи; - основные принципы класси□фикации и количественных характеристик технических ка□налов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской защиты информации; - угрозы информационной безопасности объекта инфор□матизации; - методы и средства техниче□ской защиты информации. Уметь: - проектировать систему за□щиты с использование про□граммно

					аппаратных средств защиты информации; - формировать и анализиро вать показатели защищенно сти; - определять информацион ную инфраструктуру и инфор мационные ресурсы организа ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа ции; - составлять план управления рисками; - классифицировать функцио нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си стем; - настраивать основные типы телекоммуникационного обо рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех ническим каналам и контроля эффективности защиты ин формации; - определять необходимые принципы организации за щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни ческой защиты информации; - определить опасные угрозы информационной безопасно сти объекта информатизации; - определить необходимые методы и средства техниче ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо рудования IP сетей; - основными пакетами, приме няемыми для расчётов и мо делирования в телекоммуни кациях; - практическими навыками применения современных криптографических алгорит мов и протоколов; - практическими навыками ра боты с известными криптогра фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде рации в области криптографи ческой защиты информации приразработке

					ПО в области информационной безопасно сти; - практическими навыками те стирования и оценки стойко сти программ, использующих СКЗИ; - практическими навыками классификации и определе ния количественных характе ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка налам и контроля эффектив ности защиты информации; - практическими навыками ор ганизации защиты информа ции от утечки по техническим каналам на объектах инфор матизации; - практическими навыками применения нормативных до кументов в области техниче ской защиты информации; - практическими навыками анализа и оценки угроз ин формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации.
	ОПК-10	Способен анализировать тенденции развития методов и средств криптографиче ской защиты информации, использовать средства криптографиче ской защиты информации при решении задач профессиональ ной деятельности;	ОПК-10.1. Знает основные задачи, решаемые криптографическими методами.	Б1.О.45 Методы и средства криптографическо й защиты информации	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных

					систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах.
			ОПК-10.2. Знает математические модели шифров, подходы к оценке их стойкости.	Б1.О.45 Методы и средства криптографической защиты информации	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах.
			ОПК-10.3. Знает зарубежные и российские криптографические стандарты.	Б1.О.45 Методы и средства криптографической защиты информации	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности

					компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах.
			ОПК-10.4. Умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами.	Б1.О.45 Методы и средства криптографической защиты информации	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических

					алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические

					библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□ формации;- определять необходимые принципы организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации;- определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками;- практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти;- практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; -

					практическими навыками применения методов и средств технической защиты информации
			ОПК-10.5. Умеет применять математические методы при исследовании криптографических алгоритмов.	Б1.О.45 Методы и средства криптографической защиты информации	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных

					подписей при решении задач аутентификации, механизм работы хеш-функций, совре□менные стандарты шифрова□ния, хеширования, электрон□ной подписи; - основные принципы класси□фикации и количественных характеристик технических ка□налов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской защиты информации; - угрозы информационной безопасности объекта инфор□матизации; - методы и средства техниче□ской защиты информации. Уметь: - классифицировать функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□стем; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - определять необходимые принципы организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые методы и средства техниче□ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными

					пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.6. Владеет навыками использования типовых криптографических алгоритмов.	Б1.О.45 Методы и средства криптографической защиты информации	Знание: основных задач, решаемых криптографическими методами; математических моделей шифров, подходов к оценке их стойкости; зарубежных и российских криптографических стандартов; принципов оценки защищённости информации в компьютерных системах. Знание методов реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Знание методов анализа безопасности компьютерных систем. Умение корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; анализировать защиту компьютерных систем на соответствие

					отечественным и зарубежным стандартам в области компьютерной безопасности; составлять научные отчёты и обзоры по результатам выполнения исследований; оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах. Владение: навыками использования типовых криптографических алгоритмов; методами анализа безопасности компьютерных систем; методиками оценки эффективности реализации систем защиты информации навыками работы с программными средствами общего и специального назначения; методами оценки защищённости информации в компьютерных системах.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи

					информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты

					информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ фрмационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.7. Знает типовые криптопротоколы, используемые в сетях связи.	Б1.О.46 Криптографические протоколы	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.
			ОПК-10.8. Знает основные типы криптопротоколов и принципов их построения с использованием шифрсистем.	Б1.О.46 Криптографические протоколы	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение

					подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.
			ОПК-10.9. Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.	Б1.О.46 Криптографические протоколы	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем;- основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы

					класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; -

					практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.10. Умеет проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств.	Б1.О.46 Криптографические протоколы	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических

					протоколов.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем;- основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по

					тех□ническим каналам и контроля эффективности защиты ин□ формации;- определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации;- определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками;- практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти;- практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации

			ОПК-10.11. Владеет подходами к разработке и анализу безопасности криптографических протоколов.	Б1.О.46 Криптографические протоколы	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.
			ОПК-10.12. Знает основные методы проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-10.13. Знает базовые понятия теории эллиптических кривых.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
			ОПК-10.14. Умеет эффективно производить операции с большими	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения

			числами, а также в кольцах вычетов, кольцах многочленов и конечных полях.		математических моделей элементов безопасности и разработки криптографических алгоритмов
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по

					тех□ ническим каналам и контроля эффективности защиты ин□ формации;- определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации;- определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками;- практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти;- практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.15. Умеет	Б1.О.47 Теоретико-	Знание теоретико-числовых методов защиты информации. Умение

			исследовать и решать сравнения в кольцах вычетов.	числовые методы в криптографии	реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические

					модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации;- определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками;- практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти;- практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; - практическими навыками применения методов и средств

					технической защиты информации
			ОПК-10.16. Умеет использовать достаточные условия простоты для построения больших простых чисел.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные

					крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз

					ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.17. Умеет оценивать теоретическую сложность применяемых алгоритмов.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си□стем согласно принципам вза□имодействия открытых си□стем; - основные тренды развития телекоммуникаций; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симмет□ричных и асимметричных криптографических систем, принципы генерации, хране□ния и использования крипто□графических ключей, прин□ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□менные стандарты шифрова□ния, хеширования, электрон□ной подписи; - основные принципы класси□фикации и количественных характеристик технических ка□налов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской защиты информации; - угрозы информационной безопасности объекта инфор□матизации; - методы и средства техниче□ской защиты информации. Уметь: - классифицировать функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□стем; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - оценивать потребности пользователя в

					видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения

					нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.18. Владеет навыками эффективного вычисления в кольцах вычетов и в кольцах многочленов.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си□стем согласно принципам вза□имодействия открытых си□стем;- основные тренды развития телекоммуникаций; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симмет□ричных и асимметричных криптографических систем, принципы генерации, хране□ния и использования крипто□графических ключей, прин□ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□менные стандарты шифрова□ния, хеширования, электрон□ной подписи; - основные принципы класси□фикации и количественных характеристик технических ка□налов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской защиты информации; - угрозы информационной безопасности объекта инфор□матизации; - методы и средства техниче□ской защиты информации. Уметь: - классифицировать функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых

					си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты

					информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.19. Владеет методами построения быстрых вычислительных алгоритмов алгебры и теории чисел.	Б1.О.47 Теоретико-числовые методы в криптографии	Знание теоретико-числовых методов защиты информации. Умение реализовывать алгоритмы защиты данных на основе теоретико-числовых методов. Владение навыками построения математических моделей элементов безопасности и разработки криптографических алгоритмов
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си□ стем согласно принципам вза□ имодействия открытых си□ стем; - основные тренды развития телекоммуникаций; - математические основы сим□ метричных и асимметричных криптографических систем; - принципы работы симмет□ ричных и асимметричных криптографических систем, принципы генерации, хране□ ния и использования крипто□ графических ключей, прин□ ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать

					функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□стем; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - определять необходимые принципы организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые методы и средства техниче□ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□боты с известными криптогра□фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□рации в области криптографи□ческой защиты информации при разработке ПО в области информационной безопасно□сти; - практическими навыками те□стирования и оценки стойко□сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ния количественных характе□ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по

					техническим ка□налам и контроля эффектив□ности защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.20. Умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач.	Б1.О.46 Криптографические протоколы	Знание: типовых криптопротоколов, используемых в сетях связи; принципов их построения с использованием шифрсистем; протоколов: распределения ключей, идентификации, разделения секрета, методов разработки криптографических протоколов. Умение: разворачивать инфраструктуру открытых ключей для решения криптографических задач; проводить анализ криптографических протоколов, в том числе с использованием автоматизированных средств; разрабатывать математические модели безопасности криптографических протоколов, проводить анализ безопасности криптографических протоколов. Владение подходами к разработке и анализу безопасности криптографических протоколов; навыками программной реализации криптографических протоколов, моделирования с помощью современных языков программирования и математических пакетов перспективных криптографических протоколов.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си□стем согласно принципам вза□имодействия открытых си□стем; - основные тренды развития телекоммуникаций; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симмет□ричных и асимметричных криптографических систем, принципы генерации, хране□ния и использования крипто□графических ключей, прин□ципы создания электронных

					подписей при решении задач аутентификации, механизм работы хеш-функций, совре□ менные стандарты шифрова□ ния, хеширования, электрон□ ной подписи; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными

					пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ ния количественных характе□ ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□ налам и контроля эффектив□ ности защиты информации; - практическими навыками ор□ ганизации защиты информа□ ции от утечки по техническим каналам на объектах инфор□ матизации; - практическими навыками применения нормативных до□ кументов в области техниче□ ской защиты информации; - практическими навыками анализа и оценки угроз ин□ формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.21. Знает фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации.	Б1.О.29 Теория информации	знать: фундаментальные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды), свойства энтропии и взаимной информации
				Б1.О.31 Информатика	Знает понятия: энтропии, источника сообщений, канала связи, кодов и кодирования.
			ОПК-10.22. Знает основные результаты о кодировании дискретных источников сообщений	Б1.О.29 Теория информации	знать: основные результаты о кодировании дискретных источников сообщений при наличии и отсутствии шума
				Б1.О.31 Информатика	Знает: • понятие пропускной способности канала связи • теорему Шеннона о кодировании каналов связи с шумом

			при наличии и отсутствии шума.	Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
			ОПК-10.23. Знает основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга).	Б1.О.29 Теория информации	знать: основные методы оптимального кодирования источников информации и помехоустойчивого кодирования каналов связи (коды - линейные, циклические, Хемминга)
				Б1.О.31 Информатика	Знает: • основы оптимального кодирования источников информации (префиксные коды Шеннона-Фано и Хаффмана) информации; • основы помехоустойчивого кодирования каналов связи (код Хэмминга, расстояние Хэмминга)
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации

			ОПК-10.24. Знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования.	Б1.О.29 Теория информации	знать: понятие пропускной способности канала связи, прямую и обратную теоремы кодирования
				Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако номерности, связанные с получе нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци онных системах при обеспечении защиты информации. уметь: производить оценку тех нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно стики состояния устройств защи ты информации знать: функциональное назначе ние и принципы работы основных блоков современных средств за щиты информации уметь: выполнять работы по вос становлению работоспособности средств защиты информации при возникновении нештатных ситуа ций владеть: навыками восстановле ния штатного режима работы технических средств защиты ин формации
			ОПК-10.25. Умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность).	Б1.О.29 Теория информации	уметь: вычислять теоретико информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа ции; - принципы взаимодействия телекоммуникационных си стем согласно принципам вза имодействия открытых си стем;- основные тренды развития телекоммуникаций; - математические основы сим метричных и асимметричных криптографических систем; - принципы работы симмет ричных и асимметричных криптографических систем, принципы генерации, хране ния и использования крипто графических ключей, прин ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре менные стандарты шифрова ния, хеширования, электрон ной подписи; - основные принципы класси фикации и количественных характеристик технических ка налов утечки информации; - основные способы и сред ства защиты информации от утечки по техническим кана лам и контроля эффективно сти защиты информации; - основы

					принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - основные нормативные доку□ ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке

					ПО в области информационной безопасно сти; - практическими навыками те стирования и оценки стойко сти программ, использующих СКЗИ; - практическими навыками классификации и определе ния количественных характе ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка налам и контроля эффектив ности защиты информации; - практическими навыками ор ганизации защиты информа ции от утечки по техническим каналам на объектах инфор матизации; - практическими навыками применения нормативных до кументов в области техниче ской защиты информации; - практическими навыками анализа и оценки угроз ин формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.26. Умеет решать типовые задачи кодирования и декодирования.	Б1.О.29 Теория информации	уметь: решать типовые задачи кодирования и декодирования
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа ции; - принципы взаимодействия телекоммуникационных си стем согласно принципам вза имодействия открытых си стем; - основные тренды развития телекоммуникаций; - математические основы сим метричных и асимметричных криптографических систем; - принципы работы симмет ричных и асимметричных криптографических систем, принципы генерации, хране ния и использования крипто графических ключей, прин ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре менные стандарты шифрова ния, хеширования, электрон ной подписи; - основные принципы класси фикации и количественных характеристик технических ка налов утечки информации; - основные способы и сред ства защиты информации от утечки по техническим кана лам и контроля эффективно сти защиты информации; - основы принципов организа ции защиты информации от утечки по

					техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской защиты информации; - угрозы информационной безопасности объекта инфор□матизации; - методы и средства техниче□ской защиты информации. Уметь: - классифицировать функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□стем; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - определять необходимые принципы организации за□щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ческой защиты информации; - определить опасные угрозы информационной безопасно□сти объекта информатизации; - определить необходимые методы и средства техниче□ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов; - практическими навыками ра□боты с известными криптогра□фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□рации в области криптографи□ческой защиты информации при разработке ПО в области информационной безопасно□сти; - практическими

					навыками те□стирования и оценки стойко□сти программ, использующих СКЗИ; - практическими навыками классификации и определе□ния количественных характе□ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□налам и контроля эффектив□ности защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.27. Владеет основами построения математических моделей текстовой информации и моделей систем передачи информации.	Б1.О.29 Теория информации	владеть: основами построения математических моделей текстовой информации и моделей систем передачи информации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си□стем согласно принципам вза□имодействия открытых си□стем; - основные тренды развития телекоммуникаций; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симмет□ричных и асимметричных криптографических систем, принципы генерации, хране□ния и использования крипто□графических ключей, прин□ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□менные стандарты шифрова□ния, хеширования, электрон□ной подписи; - основные принципы класси□фикации и количественных характеристик технических ка□налов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; -

					основные нормативные доку□ментами в области техниче□ ской защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□ сти программ,

					использующих СКЗИ; - практическими навыками классификации и определе□ния количественных характе□ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□налам и контроля эффектив□ности защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
			ОПК-10.28. Владеет навыками применения математического аппарата для решения прикладных теоретико-информационных задач.	Б1.О.29 Теория информации	владеть: навыками применения математического аппарата для решения при□кладных теоретико□информационных задач
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си□стем согласно принципам вза□имодействия открытых си□стем; - основные тренды развития телекоммуникаций; - математические основы сим□метричных и асимметричных криптографических систем; - принципы работы симмет□ричных и асимметричных криптографических систем, принципы генерации, хране□ния и использования крипто□графических ключей, прин□ципы создания электронных подписей при решении задач аутентификации, механизм работы хеш-функций, совре□менные стандарты шифрова□ния, хеширования, электрон□ной подписи; - основные принципы класси□фикации и количественных характеристик технических ка□налов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - основные нормативные доку□ментами в области техниче□ской

					защиты информации; - угрозы информационной безопасности объекта инфор□ матизации; - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - оценивать потребности пользователя в видах услуги и их качестве; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - определять необходимые принципы организации за□ щиты информации от утечки по техническим каналам на объектах информатизации; - определить необходимые и пользоваться нормативными документами в области техни□ ческой защиты информации; - определить опасные угрозы информационной безопасно□ сти объекта информатизации; - определить необходимые методы и средства техниче□ ской защиты информации. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - практическими навыками применения национальных стандартов Российской Феде□ рации в области криптографи□ ческой защиты информации при разработке ПО в области информационной безопасно□ сти; - практическими навыками те□ стирования и оценки стойко□ сти программ, использующих СКЗИ; - практическими навыками классификации

					и определе□ния количественных характе□ристик технических каналов утечки информации; - практическими навыками применения способов и средств защиты информации от утечки по техническим ка□налам и контроля эффектив□ности защиты информации; - практическими навыками ор□ганизации защиты информа□ции от утечки по техническим каналам на объектах инфор□матизации; - практическими навыками применения нормативных до□кументов в области техниче□ской защиты информации; - практическими навыками анализа и оценки угроз ин□формационной безопасности объекта информатизации; - практическими навыками применения методов и средств технической защиты информации
	ОПК-11	Способен разрабатывать политики безопасности, политики управления доступом и информационн ыми потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации;	ОПК-11.1. Знает основные понятия и определения, используемые при описании моделей безопасности компьютерных систем.	Б1.О.40 Модели безопасности компьютерных систем	знать: основные понятия и определе□ния, используемые при описании моде□лей безопасности компьютерных си□стем уметь: правильно применять основные понятия и определения при разработке формальных моделей безопасности компьютерных систем владеть:. практическими навыками разработки формальных моделей без□опасности компьютерных систем
			ОПК-11.2. Знает основные виды политик управления доступом и информационными потоками в компьютерных системах.	Б1.О.40 Модели безопасности компьютерных систем	знать: формальные модели политик безопасности, политик управления до□ступом и информационными потоками в компьютерных системах уметь: разрабатывать формальные модели политик безопасности, политик управления доступом и информацион□ными потоками в компьютерных систе□мах владеть:. практическими навыками разработки формальных моделей по□литик безопасности, политик управле□ния доступом и информационными по□токами в компьютерных системах
			ОПК-11.3. Знает основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности	Б1.О.40 Модели безопасности компьютерных систем	знать: основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолиро□ванной программной среды и безопас□ности информационных потоков уметь: разрабатывать формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков владеть: практическими

			информационных потоков.		навыками раз□работки формальных модели дискре□ционного, мандатного, ролевого управ□ления доступом, модели изолирован□ной программной среды и безопасности информационных потоков
			ОПК-11.4. Умеет разрабатывать модели угроз и модели нарушителя безопасности компьютерных систем.	Б1.О.40 Модели безопасности компьютерных систем	знать: руководящие документы ФСТЭК (Гостехкомиссии) России, определяю□щие модель угроз и модель нарушите□ля безопасности компьютерных систем уметь; разрабатывать модели угроз и модели нарушителя безопасности ком□пьютерных систем владеть:. практическими навыками разработки модели угроз и модели нарушителя безопасности компьютер□ных систем
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы формирования по□литик безопасности для ком□пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации ин□формационных систем в соот□ветствии с требованиями по защите информации. Уметь: - проектировать систему за□щиты с использование про□граммно-аппаратных средств защиты информации; - формировать и анализиро□вать показатели защищенно□сти; - определять информацион□ную инфраструктуру и инфор□мационные ресурсы организа□ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ции; - составлять план управления рисками. Владеть: - навыками контроля ком□плекса мер безопасности ин□формации на защищаемом объекте с учетом требований руководящих и нормативных документов
			ОПК-11.5. Умеет разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;	Б1.О.40 Модели безопасности компьютерных систем	знать: формальные модели политик безопасности, политик управления до□ступом и информационными потоками в компьютерных системах уметь: разрабатывать формальные модели политик безопасности, политик управления доступом и информацион□ными потоками в компьютерных систе□мах владеть:. практическими навыками разработки формальных моделей по□литик безопасности, политик управле□ниядоступом

					и информационными по□ токами в компьютерных системах.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы формирования по□ литик безопасности для ком□ пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации ин□ формационных систем в соот□ ветствии с требованиями по защите информации. Уметь: - проектировать систему за□ щиты с использование про□ граммно-аппаратных средств защиты информации; - формировать и анализиро□ вать показатели защищенно□ сти; - определять информацион□ ную инфраструктуру и инфор□ мационные ресурсы организа□ ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ ции; - составлять план управления рисками. Владеть: - навыками контроля ком□ плекса мер безопасности ин□ формации на защищаемом объекте с учетом требований руководящих и нормативных документов
			ОПК-11.6. Знает средства и методы хранения и передачи аутентификационной информации.	Б1.О.41 Защита в операционных системах	Знает средства и методы хранения и передачи аутентификационной информации
			ОПК-11.7. Знает основные требования к подсистеме аудита и политике аудита.	Б1.О.41 Защита в операционных системах	Знает основные требования к подсистеме аудита и политике аудита
			ОПК-11.8. Знает защитные механизмы и средства обеспечения безопасности операционных систем.	Б1.О.41 Защита в операционных системах	Знает защитные механизмы и средства обеспечения безопасности операционных систем
			ОПК-11.9. Умеет формулировать и настраивать политику безопасности основных операционных систем.	Б1.О.41 Защита в операционных системах	Умеет формулировать и настраивать политику безопасности основных операционных систем
				Б2.О.06(П) Производственная практика по получению профессиональны	Знать: - принципы формирования по□ литик безопасности для ком□ пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; -

				х умений и навыков в области профессиональной деятельности	принципы организации ин□ формационных систем в соот□ ветствии с требованиями по защите информации. Уметь: - проектировать систему за□ щиты с использование про□ граммно-аппаратных средств защиты информации; - формировать и анализиро□ вать показатели защищенно□ сти; - определять информацион□ ную инфраструктуру и инфор□ мационные ресурсы организа□ ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ ции; - составлять план управления рисками. Владеть: - навыками контроля ком□ плекса мер безопасности ин□ формации на защищаемом объекте с учетом требований руководящих и нормативных документов
			ОПК-11.10. Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.	Б1.О.41 Защита в операционных системах	Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем
				Б1.О.42 Основы построения защищенных компьютерных сетей	уметь: разрабатывать политики и процедуры безопасности в области компьютерных сетей
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы формирования по□ литик безопасности для ком□ пьютерной инфраструктуры организации; - принципы формирования процедур безопасности для заданных политик; - принципы организации ин□ формационных систем в соот□ ветствии с требованиями по защите информации. Уметь: - проектировать систему за□ щиты с использование про□ граммно-аппаратных средств защиты информации; - формировать и анализиро□ вать показатели защищенно□ сти; - определять информацион□ ную инфраструктуру и инфор□ мационные ресурсы организа□ ции, подлежащие защите; - анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информа□ ции; - составлять план управления рисками. Владеть: - навыками контроля ком□ плекса мер безопасности ин□ формации на защищаемом объекте с учетом требований руководящих и нормативных документов

	ОПК-12	Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения;	ОПК-12.1. Знает принципы построения современных операционных систем и особенности их применения.	Б1.О.32 Операционные системы	Знает принципы построения современных операционных систем и особенности их применения
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
			ОПК-12.2. Знает принципы разработки специального программного	Б1.О.32 Операционные системы	Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей

			обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей.	Б1.О.41 Защита в операционных системах	Знает принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных возможностей
			ОПК-12.3. Знает основные принципы конфигурирования и администрирования операционных систем.	Б1.О.32 Операционные системы	Знает основные принципы конфигурирования и администрирования операционных систем
			ОПК-12.4. Владеет навыками системного программирования.	Б1.О.32 Операционные системы	Владеет навыками системного программирования
				Б1.О.41 Защита в операционных системах	Владеет навыками системного программирования
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - архитектуру и принципы по□ строения и защиты операци□ онных систем; - программные интерфейсы настроек политик управления доступом в операционных си□ стемах UNIX, FreeBSD, GNU/Linux и MS Windows - стандартные средства и ме□ тоды восстановления состоя□ ний операционных и файло□ вых систем. Уметь: - использовать встроенные средства защиты информации операционных систем GNU/Linux и MS Windows для противодействия угрозам без□ опасности информации; - использовать встроенные и сторонние средства восста□ новления информации. Владеть: - навыками настройки антиви□ русной защиты и сетевого экрана операционных систем GNU/Linux и MS Windows; - создания точек восстановле□ ния операционных систем; - навыками работы с про□ граммным обеспечением для восстановления файловой си□ стемы.
			ОПК-12.5. Умеет осуществлять администрирование программного обеспечения специального назначения,	Б1.О.32 Операционные системы	Умеет осуществлять администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отечественного производства
				Б1.О.50 Инсталляция и настройка программного	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления

			включая операционные системы, в том числе отечественного производства.	обеспечения	базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - архитектуру и принципы по□ строения и защиты операци□ онных систем; - программные интерфейсы настроек политик управления доступом в операционных си□ стемах UNIX, FreeBSD, GNU/Linux и MS Windows - стандартные средства и ме□ тоды восстановления состоя□ ний операционных и файло□ вых систем. Уметь: - использовать встроенные средства защиты информации операционных систем GNU/Linux и MS Windows для противодействия угрозам без□ опасности информации; - использовать встроенные и сторонние средства

					восста□новления информации. Владеть: - навыками настройки антиви□русной защиты и сетевого экрана операционных систем GNU/Linux и MS Windows; - создания точек восстановле□ния операционных систем; - навыками работы с про□граммным обеспечением для восстановления файловой си□стемы.
			ОПК-12.6. Знает методы восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций.	Б1.О.32 Операционные системы	Знает методы восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции

					администратора системы.
			ОПК-12.7. Умеет восстанавливать работоспособность программ специального назначения при возникновении нештатных ситуаций.	Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессионально	Знать: - архитектуру и принципы по□ строения и защиты операци□ онных систем; - программные интерфейсы настроек политик управления доступом в операционных си□ стемах UNIX, FreeBSD, GNU/Linux и MS Windows - стандартные средства и ме□ тоды восстановления состоя□ ний операционных и

				й деятельности	файло□ вых систем. Уметь: - использовать встроенные средства защиты информации операционных систем GNU/Linux и MS Windows для противодействия угрозам без□ опасности информации; - использовать встроенные и сторонние средства восста□ новления информации. Владеть: - навыками настройки антиви□ русной защиты и сетевого экрана операционных систем GNU/Linux и MS Windows; - создания точек восстановле□ ния операционных систем; - навыками работы с про□ граммным обеспечением для восстановления файловой си□ стемы.
	ОПК-13	Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности;	ОПК-13.1. Умеет формулировать и настраивать политику безопасности основных операционных систем.	Б1.О.41 Защита в операционных системах	Умеет формулировать и настраивать политику безопасности основных операционных систем
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; -

					алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ; - состав и принципы функциониро□ вания программно-аппаратных средств защиты информации; - принципы формирования поли□ тики информационной безопасно□ сти организации; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□ мостей информационных систем, методы оценки рисков информаци□ онных систем, методы и средства проектирования технологически безопасного программного обеспе□ чения; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ ского анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□ тического и динамического ана□ лиза программ, методы проведе□ ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□ фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать

					алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и проводить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных систем и моделирование угроз безопасно□сти в компьютерных системах с учетом мер по их предотвраще□нию; - применять на практике получен□ные знания и навыки для проверки работоспособности ПО и его ана□лиза на наличие уязвимостей (экс□пертиза исходного кода, статиче□ский и динамический анализ, фай□зингтестирование); - применять на практике получен□ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики без□опасности объекта защиты для ти□повых решений и требований; - практическими навыками

					приме□нения стандартов информацион□ной безопасности при создании за□щищенных систем обработки ин□формации; - навыками использования инстру□ментальных интеллектуальных си□стем для обоснования требований и оценки защищенности систем об□работки информации; - практическими навыками исполь□зования инструментальных средств для моделирования угроз безопасности в компьютерных си□стемах с учетом мер по их предот□вращению и проектирования тех□нологически безопасного про□граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□чия уязвимостей, навыками ис□пользования специализированных утилит статического и динамиче□ского анализа кода; - специализированными инстру□ментами и практическими навы□ками анализа ПО на наличие уяз□вимостей; - практическими навыками разра□ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня;- язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□нения логических выражений в реализации условных операто□ров и

					циклов; - технологии построения алго□ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических

					компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для

					ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□граммы; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев;- навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний;- практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы

					и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□ менения логических выраже□ ний в реализации условных операторов и циклов- технологии построения алго□ ритмов для решения практи□ ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□ наторных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы

					устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных систем и средств вычисли□тельной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на

					практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих

					криптографические методы и алгоритмы.
			ОПК-13.2. Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.	Б1.О.41 Защита в операционных системах	Владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ; - состав и принципы функциониро□ вания

					программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков информаци□онных систем, методы и средства проектирования технологически безопасного программного обеспе□чения; - источники угроз информационной безопасности в компьютерных си□стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ского анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□тического и динамического ана□лиза программ, методы проведе□ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов постро□ения защищенных информационных систем; определять

					классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи щенным системам обработки ин формации и проводить оценку эф фективности их функционирова ния; - составлять задание по безопас ности и профиль защиты при со здании защищенных систем обра ботки информации; обосновывать требования к защищенным систе мам обработки информации и про водить оценку эффективности их функционирования; - проводить классификацию уязви мостей информационных систем и моделирование угроз безопасно сти в компьютерных системах с учетом мер по их предотвраще нию; - применять на практике получен ные знания и навыки для проверки работоспособности ПО и его ана лиза на наличие уязвимостей (экс пертиза исходного кода, статиче ский и динамический анализ, фай ззингтестирование); - применять на практике получен ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра боты с компьютером, программи рования на машинно-ориентиро ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин формационных систем и техноло гий; - навыками разработки программ; - навыками разработки, документи рования, тестирования и отладки программ; - навыками документирования про граммного кода в виде коммента риев; - навыками тестирование и от ладки программ; - навыками формирования и настройки локальной политики без опасности объекта защиты для ти повых решений и требований; - практическими навыками приме нения стандартов информацион ной безопасности при создании за щищенных систем обработки ин формации; - навыками использования инстру ментальных интеллектуальных си стем для обоснования требований и оценки защищенности систем об работки информации; - практическими навыками исполь зования инструментальных средств для моделирования угроз безопасности в компьютерных си стемах с учетом мер по

					их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы

					построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач

					в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и

					требо□ ваний; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ; - структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современ□ ных компьютерных систем и архитектуру их основных ти□ пов; - определения и понимать суть таких понятий как алго□ ритм, типы и структуры дан□ ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□ менения

					логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по

					уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных систем и средств вычисли□тельной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на

					машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструментальных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.3. Знает общие принципы построения и использования современных языков программирования высокого уровня.	Б1.О.36 Введение в программировани е	Знать: общие принципы построения и использования современных языков программирования высокого уровня.
				Б1.О.37 Методы программировани я	Знать: общие принципы построения и использования современных языков программирования высокого уровня
				Б2.О.04(Пд) Производственная практика	Знать: - фундаментальные принципы фоннеймановской

				(преддипломная)	архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по

					классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных си- стем и средств вычислитель□ной техники; обосновывать требования к защищенным си□стемам обработки информа□ции и проводить оценку эф□фективности их функциониро□вания; - составлять

					задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования

					спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
			ОПК-13.4. Знает язык программирования высокого уровня (объектно-ориентированное программирование).	Б1.О.35 Объектно-ориентированное программирование	Знать: объектно-ориентированный язык программирования.
				Б1.О.37 Методы программирования	Знать: язык программирования высокого уровня (объектно□ ориентированное программирование).
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□нения логических выражений в реализации условных операто□ров и циклов; - технологии построения алго□ритмов для решения практиче□ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; -

					алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого

					уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной

					политики безопасности объекта защиты для типовых решений и требо□ ваний; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
			ОПК-13.5. Умеет работать с интегрированными средами разработки программного обеспечения.	Б1.О.36 Введение в программировани е	Уметь: Работать с интегрированными средами разработки программного обеспечения.
				Б1.О.37 Методы программировани я	Уметь: работать с интегрированными средами разработки программного обеспечения.
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа,

					компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ; - состав и принципы функциониро□ вания программно-аппаратных средств защиты информации; - принципы формирования поли□ тики информационной безопасно□ сти организации; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□ мостей информационных систем, методы оценки рисков информаци□ онных систем, методы и средства проектирования технологически безопасного программного обеспе□ чения; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ ского анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□ тического и

					динамического ана□ лиза программ, методы проведе□ ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□ фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов; - конфигурировать программно-ап□ паратные средства защиты инфор□ мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□ щенным системам обработки ин□ формации и проводить оценку эф□ фективности их функционирова□ ния; - составлять задание по безопас□ ности и профиль защиты при со□ здании защищенных систем обра□ ботки информации; обосновывать требования к защищенным систе□ мам обработки информации и про□ водить оценку эффективности их функционирования; - проводить классификацию уязви□ мостей информационных систем и моделирование угроз безопасно□ сти в компьютерных системах с учетом мер по их предотвраще□ нию; - применять на практике получен□ ные знания и навыки для проверки работоспособности ПО и его ана□ лиза на наличие уязвимостей

					(экс□ пертиза исходного кода, статиче□ ский и динамический анализ, фай□ ззингтестирование); - применять на практике получен□ ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики без□ опасности объекта защиты для ти□ повых решений и требований; - практическими навыками приме□ нения стандартов информацион□ ной безопасности при создании за□ щищенных систем обработки ин□ формации; - навыками использования инстру□ ментальных интеллектуальных си□ стем для обоснования требований и оценки защищенности систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования угроз безопасности в компьютерных си□ стемах с учетом мер по их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ; - структуру фоннеймановского процессора и

					организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□нения логических выражений в реализации условных операто□ров и циклов; - технологии построения алго□ритмов для решения практиче□ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных

					систем, методы оценки рисков информацион□ ных систем,методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□ мации. Уметь: - объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании

					защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев;- навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического

					анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□менения логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила

					математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации

					инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для

					обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.6. Владеет навыками разработки, отладки, документирования и тестирования программ.	Б1.О.37 Методы программировани я	Владеть: навыками разработки, отладки, документирования и тестирования программ.
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения

					практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ; - состав и принципы функциониро□ вания программно-аппаратных средств защиты информации; - принципы формирования поли□ тики информационной безопасно□ сти организации; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□ мостей информационных систем, методы оценки рисков информаци□ онных систем, методы и средства проектирования технологически безопасного программного обеспе□ чения; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ ского анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□ тического и динамического ана□ лиза программ, методы проведе□ ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□ фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических

					задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и провдить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных систем и моделирование угроз безопасно□сти в компьютерных системах с учетом мер по их предотвраще□нию; - применять на практике получен□ные знания и навыки для проверки работоспособности ПО и его ана□лиза на наличие уязвимостей (экс□пертиза исходного кода, статиче□ский и динамический анализ, фай□ззингтестирование); - применять на практике получен□ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки

					программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики без□опасности объекта защиты для ти□повых решений и требований; - практическими навыками приме□нения стандартов информацион□ной безопасности при создании за□щищенных систем обработки ин□формации; - навыками использования инстру□ментальных интеллектуальных си□стем для обоснования требований и оценки защищенности систем об□работки информации; - практическими навыками исполь□зования инструментальных средств для моделирования угроз безопасности в компьютерных си□стемах с учетом мер по их предот□вращению и проектирования тех□нологически безопасного про□граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□чия уязвимостей, навыками ис□пользования специализированных утилит статического и динамиче□ского анализа кода; - специализированными инстру□ментами и практическими навы□ками анализа ПО на наличие уяз□вимостей; - практическими навыками разра□ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ; - структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в

					массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического

					анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных си-стем и средств вычислитель□ной техники; обосновывать требования к защищенным си□стемам обработки информа□ции и проводить оценку эф□фективности их функциониро□вания; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного

					кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев;- навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний;- практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
				Б2.О.06(П) Производственная практика по получению	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и

				профессиональных умений и навыков в области профессиональной деятельности	организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□менения логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных

					систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных систем и средств вычисли□тельной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании

					защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практическихзадач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной поли□тики безопасности объекта за□щиты для типовых решений и требований; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния

					специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.7. Владеет навыками использования инструментальных средств отладки и дизассемблирования программного кода.	Б1.О.35 Объектно-ориентированное программировани е	Владеть: навыками использования инструментальных средств отладки и дизассемблирования программного кода.
				Б1.О.36 Введение в программировани е	Владеть: навыками использования инструментальных средств отладки и дизассемблирования программного кода.
				Б1.О.37 Методы программировани я	Владеть: навыками использования инструментальных средств отладки и дизассемблирования программного кода.
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры

					данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ; - состав и принципы функциониро□ вания программно-аппаратных средств защиты информации; - принципы формирования поли□ тики информационной безопасно□ сти организации; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□ мостей информационных систем, методы оценки рисков информаци□ онных систем, методы и средства проектирования технологически безопасного программного обеспе□ чения; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ ского анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□ тического и динамического ана□ лиза программ, методы проведе□ ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□ фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде

					разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и проводить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных систем и моделирование угроз безопасно□сти в компьютерных системах с учетом мер по их предотвраще□нию; - применять на практике получен□ные знания и навыки для проверки работоспособности ПО и его ана□лиза на наличие уязвимостей (экс□пертиза исходного кода, статиче□ский и динамический анализ, фай□ззингтестирование); - применять на практике получен□ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования

					про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики без□опасности объекта защиты для ти□повых решений и требований; - практическими навыками приме□нения стандартов информацион□ной безопасности при создании за□щищенных систем обработки ин□формации; - навыками использования инстру□ментальных интеллектуальных си□стем для обоснования требований и оценки защищенности систем об□работки информации; - практическими навыками исполь□зования инструментальных средств для моделирования угроз безопасности в компьютерных си□стемах с учетом мер по их предот□вращению и проектирования тех□нологически безопасного про□граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□чия уязвимостей, навыками ис□пользования специализированных утилит статического и динамиче□ского анализа кода; - специализированными инстру□ментами и практическими навы□ками анализа ПО на наличие уяз□вимостей; - практическими навыками разра□ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ; - структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков

					программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств

					крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные

					знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев;- навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний;- практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы иалго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления

				области профессиональной деятельности	памятью ЭВМ; - фундаментальные принципы повышения производительно сти ЭВМ; - классификацию современ ных компьютерных систем и архитектуру их основных ти пов; - определения и понимать суть таких понятий как алго ритм, типы и структуры дан ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра ботки данных в массивах и файлах; - формы и способы представ ления данных в программах; - области и особенности при менения языков программиро вания высокого уровня; - язык программирования вы сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при менения логических выраже ний в реализации условных операторов и циклов- технологии построения алго ритмов для решения практи ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби наторных задач; - алгоритмы построения и по иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ ного кода; - правила математической ло гики, для составления логиче ских выражений в алгоритмах программ; - состав и принципы функцио нирования программно-аппа ратных средств защиты ин формации; - принципы формирования по литики информационной без опасности организации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин формационных систем, ме тоды оценки рисков информа ционных систем, методы и средства проектирования тех нологически безопасного

					про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компью□терных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и

					прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной поли□тики безопасности объекта за□щиты для типовых решений и требований; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и

					практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.8. Знает современные технологии программирования.	Б1.О.36 Введение в программировани е	Знать: Современные технологии программирования.
				Б1.О.37 Методы программировани я	Знать: знает современные технологии программирования
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы

					документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ ного кода; - правила математической ло гики, для составления логиче ских выражений в алгоритмах программ; - состав и принципы функцио нирования программно-аппа ратных средств защиты ин формации; - принципы формирования по литики информационной без опасности организации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор мационных систем, методы оценки рисков информацион ных систем, методы и сред-ства проектирования техноло гически безопасного про граммного обеспечения; - источники угроз информаци онной безопасности в компью терных системах и сетях, ос новные виды уязвимостей ПО, принципы работы средств ста тического и динамического анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина мического анализа программ, методы проведения экспер тизы исходного кода; - принципы функционирования программных средств крипто графической защиты инфор мации. Уметь:- объяснять основополагаю щие принципы создания и раз вития архитектуры компьютер ных систем; - выполнять работы по уста новке, настройке и обслужива нию технических компьютер ных средств, требующие зна ния их архитектуры и системы команд; - составлять алгоритмы реше ния практических задач, гра мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы вать алгоритмы решения за дач на языке высокого уровня; - строить математические мо дели для алгоритмов задач в области программирования; - разрабатывать и реализовы вать

					алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных си- стем и средств вычислитель□ной техники; обосновывать требования к защищенным си□стемам обработки информа□ции и проводить оценку эф□фективности их функциониро□вания; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний; - практическими навыками применения стандартов

					ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
			ОПК-13.9. Знает показатели качества программного обеспечения.	Б1.О.37 Методы программировани я	Знать: показатели качества программного обеспечения
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ; - структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное

					программирование. - способы построения и приме□нения логических выражений в реализации условных операто□ров и циклов; - технологии построения алго□ритмов для решения практиче□ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития

					архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером,

					про□граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев;- навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний;- практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
			ОПК-13.10. Знает базовые структуры данных.	Б1.О.37 Методы программирования	Знать: базовые структуры данных
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: базовые классы, реализующие структуры в языке C#, динамические структуры данных (стеки, очереди), деревья, графы. Уметь: разрабатывать компоненты для программ, с использованием базовых классов, реализующие динамические

					структуры данных (стеки, очереди), деревья графы. Владеть (иметь навык(и)): навыками разработки компонент для программ, реализующие динамические структуры данных (стеки, очереди), деревья графы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек туры ЭВМ;- структуру фоннеймановского процессора и организацию си стемы команд ЭВМ; - принципы обмена информа цией с внешними устрой ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно сти ЭВМ; - классификацию современных компьютерных систем и архи тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про грамма, компилятор и т.п. - алгоритмы поиска и обра ботки данных в массивах и файлах; - формы и способы представ ления данных в программах; - области и особенности при менения языков программиро вания высокого уровня;- язык программирования вы сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме нения логических выражений в реализации условных операто ров и циклов; - технологии построения алго ритмов для решения практиче ских задач;- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина торных задач; - алгоритмы построения и по иска данных на деревьях и графах;- способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ ного кода; - правила математической ло гики, для составления логиче ских выражений в алгоритмах программ; - состав и принципы

					функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных

					ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для

					моделирова ния угроз безопасности в ком пьютерных система с учетом мер по их предотвращению и проектирования технологиче ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе циализированных утилит ста тического и динамического анализа кода; - специализированными ин струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз работки, использования (из вестных криптографических библиотек) и тестирования специализированных алгорит мов и ПО, реализующих крип тографические методы и алго ритмы.
			ОПК-13.11. Знает основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности.	Б1.О.37 Методы программирования	Знать основные комбинаторные и теоретико-графовые алгоритмы, а также способы их эффективной реализации и оценки вычислительной сложности.
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: основные алгоритмы сортировки и поиска данных, рекурсивные алгоритмы, алгоритмы с возвратом, применяемые в комбинаторных алгоритмах и алгоритмах на графах. Уметь: реализовать компоненты для программ с использованием алгоритмов сортировки и поиска данных, рекурсивных алгоритмов, алгоритмов с возвратом, применяемых в комбинаторных алгоритмах и алгоритмах на графах. Владеть (иметь навык(и)): навыками разработки компонент для программ с использованием алгоритмов сортировки и поиска данных, рекурсивных алгоритмов и алгоритмов с возвратом, применяемых в комбинаторных алгоритмах и алгоритмах на графах
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек туры ЭВМ;- структуру фоннеймановского процессора и организацию си стемы команд ЭВМ; - принципы обмена информа цией с внешними устрой ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно сти ЭВМ; - классификацию современных компьютерных систем и архи тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и

					структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы

					устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике

					полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев;- навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний;- практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.

			ОПК-13.12. Умеет формализовать поставленную задачу.	Б1.О.37 Методы программирования	Уметь: формализовать поставленную задачу
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: основы современной технологии разработки программ. Уметь: формализовать поставленную задачу для реализации алгоритмов и программ. Владеть (иметь навык(и): формализации поставленной задачи для разработки алгоритмов и программ.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы

					оформления и структу рирования программного кода; - правила математической логики, для составления логических выра жений в алгоритмах программ; - состав и принципы функциониро вания программно-аппаратных средств защиты информации; - принципы формирования поли тики информационной безопасно сти организации; - источники угроз информационной безопасности в компьютерных си стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви мостей информационных систем, методы оценки рисков информаци онных систем, методы и средства проектирования технологически безопасного программного обеспе чения; - источники угроз информационной безопасности в компьютерных си стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче ского анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста тического и динамического ана лиза программ, методы проведе ния экспертизы исходного кода; - принципы функционирования программных средств криптогра фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни ческих компьютерных средств, тре бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож ность алгоритмов; - конфигурировать программно-ап паратные средства защиты инфор мации инфраструктуры и

					конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и проводить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных систем и моделирование угроз безопасно□сти в компьютерных системах с учетом мер по их предотвраще□нию; - применять на практике получен□ные знания и навыки для проверки работоспособности ПО и его ана□лиза на наличие уязвимостей (экс□пертиза исходного кода, статиче□ский и динамический анализ, фай□ззингтестирование); - применять на практике получен□ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики без□опасности объекта защиты для ти□повых решений и требований; - практическими навыками приме□нения стандартов информацион□ной безопасности при создании за□щищенных систем обработки ин□формации; - навыками использования инстру□ментальных интеллектуальных си□стем для обоснования требований и оценки защищенности

					систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования угроз безопасности в компьютерных си□ стемах с учетом мер по их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и

					интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде

					разработки программ на языке высокого уровня; - разрабатывать и реализовы вать алгоритмы решения за дач на языке высокого уровня; - строить математические мо дели для алгоритмов задач в области программирования; - разрабатывать и реализовы вать алгоритмы решения за дач поиска, сортировки, ра боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм мно-аппаратные средства за щиты информации инфра структуры и конечных систем; - проводить разработку поли тики информационной без опасности для различных ва риантов построения защищен ных информационных систем; определять классы защищен ности автоматизированных си стем и средств вычислитель ной техники; обосновывать требования к защищенным си стемам обработки информа ции и проводить оценку эф фективности их функциониро вания; - составлять задание по без опасности и профиль защиты при создании защищенных си стем обработки информации; обосновывать требования к защищенным системам обра ботки информации и прово дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис ходного кода, статический и динамический анализ, фай ззингтестирование); - применять на практике полу ченные знания и навыки для анализа ПО на наличие уязви мостей. Владеть: - навыками самостоятельной работы с компьютером, про граммирования на машинно ориентированном языке; - базовой подготовкой в обла сти программирования для ре шения практических задач в области информационных си стем и технологий; - навыками разработки про грамм; - навыками разработки, доку ментирования, тестирования и отладки программ; - навыками документирования программного

					кода в виде ком□ ментариев;- навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний;- практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современ□ ных компьютерных систем и архитектуру их основных ти□ пов; - определения и понимать суть таких понятий как алго□ ритм, типы и структуры дан□ ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков

					программиро вания высокого уровня; - язык программирования вы сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при менения логических выраже ний в реализации условных операторов и циклов- технологии построения алго ритмов для решения практи ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби наторных задач; - алгоритмы построения и по иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ ного кода; - правила математической ло гики, для составления логиче ских выражений в алгоритмах программ; - состав и принципы функцио нирования программно-аппа ратных средств защиты ин формации; - принципы формирования по литики информационной без опасности организации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин формационных систем, ме тоды оценки рисков информа ционных систем, методы и средства проектирования тех нологически безопасного про граммного обеспечения; - источники угроз информаци онной безопасности в компью терных системах и сетях, ос новные виды уязвимостей ПО, принципы работы средств ста тического и динамического анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина мического анализа программ, методы проведения экспер тизы исходного кода; - принципы функционирова ния программных средств

					криптографической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития архитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию технических компьютерных средств, требующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать программно-аппаратные средства защиты информации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построения защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования; - составлять задание по безопасности и профиль защиты при создании защищенных систем обработки информации; обосновывать требования к защищенным системам обработки информации и проводить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полученные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файзингтестирование); - применять на практике

					полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.13. Умеет разрабатывать	Б1.О.37 Методы программировани я	У меть: разрабатывать эффективные алгоритмы и программы.

			эффективные алгоритмы и программы.	Б1.О.55.05 Алгоритмы и структуры данных	Знать: основы современной технологии разработки программ. Уметь: разрабатывать алгоритмы для поставленной задачи. Владеть (иметь навык(и): разработки алгоритмов для поставленной задачи
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ; - состав и принципы функциониро□ вания

					программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков информаци□онных систем, методы и средства проектирования технологически безопасного программного обеспе□чения; - источники угроз информационной безопасности в компьютерных си□стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ского анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□тического и динамического ана□лиза программ, методы проведе□ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять

					классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи щенным системам обработки ин формации и проводить оценку эф фективности их функционирова ния; - составлять задание по безопас ности и профиль защиты при со здании защищенных систем обра ботки информации; обосновывать требования к защищенным систе мам обработки информации и про водить оценку эффективности их функционирования; - проводить классификацию уязви мостей информационных систем и моделирование угроз безопасно сти в компьютерных системах с учетом мер по их предотвраще нию; - применять на практике получен ные знания и навыки для проверки работоспособности ПО и его ана лиза на наличие уязвимостей (экс пертиза исходного кода, статиче ский и динамический анализ, фай ззингтестирование); - применять на практике получен ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра боты с компьютером, программи рования на машинно-ориентиро ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин формационных систем и техноло гий; - навыками разработки программ; - навыками разработки, документи рования, тестирования и отладки программ; - навыками документирования про граммного кода в виде коммента риев; - навыками тестирование и от ладки программ; - навыками формирования и настройки локальной политики без опасности объекта защиты для ти повых решений и требований; - практическими навыками приме нения стандартов информацион ной безопасности при создании за щищенных систем обработки ин формации; - навыками использования инстру ментальных интеллектуальных си стем для обоснования требований и оценки защищенности систем об работки информации; - практическими навыками исполь зования инструментальных средств для моделирования угроз безопасности в компьютерных си стемах с учетом мер по

					их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы

					построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь: - объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач

					в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и

					требо□ ваний; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ; - структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современ□ ных компьютерных систем и архитектуру их основных ти□ пов; - определения и понимать суть таких понятий как алго□ ритм, типы и структуры дан□ ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□ менения

					логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по

					уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных систем и средств вычисли□тельной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на

					машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.14. Умеет проводить оценку вычислительной сложности алгоритма.	Б1.О.37 Методы программирования	Уметь: проводить оценку вычислительной сложности алгоритма.
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: методику оценки вычислительной сложности алгоритма. Уметь: проводить оценку вычислительной сложности алгоритма. Владеть (иметь навык(и)): оценки вычислительной сложности

					алгоритма.
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений в алгоритмах программ; - состав и принципы функциониро□ вания программно-аппаратных средств защиты информации; - принципы формирования поли□ тики информационной безопасно□ сти организации; - источники угроз информационной безопасности в

					компьютерных си□ стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□ мостей информационных систем, методы оценки рисков информаци□ онных систем, методы и средства проектирования технологически безопасного программного обеспе□ чения; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ ского анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□ тического и динамического ана□ лиза программ, методы проведе□ ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□ фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов; - конфигурировать программно-ап□ паратные средства защиты инфор□ мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов постро□ ения защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□ щенным системам обработки ин□ формации и проводить

					оценку эф□ фективности их функционирова□ ния; - составлять задание по безопас□ ности и профиль защиты при со□ здании защищенных систем обра□ ботки информации; обосновывать требования к защищенным систе□ мам обработки информации и про□ водить оценку эффективности их функционирования; - проводить классификацию уязви□ мостей информационных систем и моделирование угроз безопасно□ сти в компьютерных системах с учетом мер по их предотвраще□ нию; - применять на практике получен□ ные знания и навыки для проверки работоспособности ПО и его ана□ лиза на наличие уязвимостей (экс□ пертиза исходного кода, статиче□ ский и динамический анализ, фай□ ззингтестирование); - применять на практике получен□ ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики без□ опасности объекта защиты для ти□ повых решений и требований; - практическими навыками приме□ нения стандартов информацион□ ной безопасности при создании за□ щищенных систем обработки ин□ формации; - навыками использования инстру□ ментальных интеллектуальных си□ стем для обоснования требований и оценки защищенности систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования угроз безопасности в компьютерных си□ стемах с учетом мер по их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия

					уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в

					средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь: - объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать

					вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования

					ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□менения логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения

					задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических

					задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных систем и средств вычисли□тельной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками

					разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.15. Умеет планировать разработку сложного программного обеспечения.	Б1.О.37 Методы программирования	Уметь: планировать разработку сложного программного обеспечения
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: основы современной технологии разработки программ. Уметь: планировать разработку сложного программного обеспечения. Владеть (иметь навык(и)): планирования разработки сложного программного обеспечения.
				Б2.О.03(Н) Производственная практика (научно-	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и

				исследовательская работа)	организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ления памятью ЭВМ; - фундаментальные принципы по□вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□туру их основных типов; - определения и понимать суть та□ких понятий как алгоритм, типы и структуры данных, управление па□мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно□ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ; - состав и принципы функциониро□вания программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков

					информаци□ онных систем, методы и средства проектирования технологически безопасного программного обеспе□ чения; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ ского анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□ тического и динамического ана□ лиза программ, методы проведе□ ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□ фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов; - конфигурировать программно-ап□ паратные средства защиты инфор□ мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□ щенным системам обработки ин□ формации и проводить оценку эф□ фективности их функционирова□ ния; - составлять задание по безопас□ ности и профиль защиты при со□ здании защищенных систем обра□ ботки информации; обосновывать

					требования к защищенным систе мам обработки информации и про водить оценку эффективности их функционирования; - проводить классификацию уязви мостей информационных систем и моделирование угроз безопасно сти в компьютерных системах с учетом мер по их предотвраще нию; - применять на практике получен ные знания и навыки для проверки работоспособности ПО и его ана лиза на наличие уязвимостей (экс пертиза исходного кода, статиче ский и динамический анализ, фай ззингтестирование); - применять на практике получен ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра боты с компьютером, программи рования на машинно-ориентиро ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин формационных систем и техноло гий; - навыками разработки программ; - навыками разработки, документи рования, тестирования и отладки программ; - навыками документирования про граммного кода в виде коммента риев; - навыками тестирование и от ладки программ; - навыками формирования и настройки локальной политики без опасности объекта защиты для ти повых решений и требований; - практическими навыками приме нения стандартов информацион ной безопасности при создании за щищенных систем обработки ин формации; - навыками использования инстру ментальных интеллектуальных си стем для обоснования требований и оценки защищенности систем об работки информации; - практическими навыками исполь зования инструментальных средств для моделирования угроз безопасности в компьютерных си стемах с учетом мер по их предот вращению и проектирования тех нологически безопасного про граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали чия уязвимостей, навыками ис пользования специализированных утилит статического и динамиче ского анализа кода; - специализированными инстру ментами и практическими

					навы□ками анализа ПО на наличие уяз□вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня;- язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач;- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах;- способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских

					выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку

					поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных си- стем и средств вычислитель□ной техники; обосновывать требования к защищенным си□стемам обработки информа□ции и проводить оценку эф□фективности их функциониро□вания; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками

					ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современ□ ных компьютерных систем и архитектуру их основных ти□ пов; - определения и понимать суть таких понятий как алго□ ритм, типы и структуры дан□ ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня;- язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□ менения логических выраже□ ний в реализации условных операторов и циклов- технологии построения алго□ ритмов для решения практи□ ческих задач;- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев,

					графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и

					реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде

					комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.16. Владеет методами оценки качества готового программного обеспечения.	Б1.О.37 Методы программировани я	Владеть: методами оценки качества готового программного обеспечения.
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: методы тестирования и отладки программного обеспечения. Уметь: проводить тестирование и отладку программного обеспечения. Владеть (иметь навык(и)): тестирования и отладки программного обеспечения.
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения

					производительности ЭВМ; - классификацию современных компьютерных систем и архитек□туру их основных типов; - определения и понимать суть та□ких понятий как алгоритм, типы и структуры данных, управление па□мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно□ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах раз-ра□ботки программ; - принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ; - состав и принципы функциониро□вания программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков информаци□онных систем, методы и средства проектирования технологически безопасного программного обеспе□чения; - источники угроз информационной безопасности в компьютерных

					си□стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ского анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□тического и динамического ана□лиза программ, методы проведе□ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и проводить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных

					систем и моделирование угроз безопасно сти в компьютерных системах с учетом мер по их предотвраще нию; - применять на практике получен ные знания и навыки для проверки работоспособности ПО и его ана лиза на наличие уязвимостей (экс пертиза исходного кода, статиче ский и динамический анализ, фай ззингтестирование); - применять на практике получен ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра боты с компьютером, программи рования на машинно-ориентиро ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин формационных систем и техноло гий;- навыками разработки программ; - навыками разработки, документи рования, тестирования и отладки программ; - навыками документирования про граммного кода в виде коммента риев; - навыками тестирование и от ладки программ; - навыками формирования и настройки локальной политики без опасности объекта защиты для ти повых решений и требований; - практическими навыками приме нения стандартов информацион ной безопасности при создании за щищенных систем обработки ин формации; - навыками использования инстру ментальных интеллектуальных си стем для обоснования требований и оценки защищенности систем об работки информации; - практическими навыками исполь зования инструментальных средств для моделирования угроз безопасности в компьютерных си стемах с учетом мер по их предот вращению и проектирования тех нологически безопасного про граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали чия уязвимостей, навыками ис пользования специализированных утилит статического и динамиче ского анализа кода; - специализированными инстру ментами и практическими навы ками анализа ПО на наличие уяз вимостей; - практическими навыками разра ботки, использования (известных криптографических библиотек) и тестирования

					специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня;- язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач;- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах;- способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики

					информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□ мационных систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем

					и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования

					технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□менения логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы

					документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ ного кода; - правила математической ло гики, для составления логиче ских выражений в алгоритмах программ; - состав и принципы функцио нирования программно-аппа ратных средств защиты ин формации; - принципы формирования по литики информационной без опасности организации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин формационных систем, ме тоды оценки рисков информа ционных систем, методы и средства проектирования тех нологически безопасного про граммного обеспечения; - источники угроз информаци онной безопасности в компью терных системах и сетях, ос новные виды уязвимостей ПО, принципы работы средств ста тического и динамического анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина мического анализа программ, методы проведения экспер тизы исходного кода; - принципы функционирова ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю щие принципы создания и раз вития архитектуры компью терных систем; - выполнять работы по уста новке, настройке и обслужива нию технических компьютер ных средств, требующие зна ния их архитектуры и системы команд; - составлять алгоритмы реше ния практических задач, гра мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы вать алгоритмы решения за дач на языке высокого уровня; - строить математические мо дели для алгоритмов задач в области программирования; - разрабатывать и реализовы вать

					алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных систем и средств вычисли□тельной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной поли□тики безопасности объекта за□щиты для типовых решений и

					требований; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.17. Владеет навыками разработки алгоритмов для решения типовых профессиональных задач.	Б1.О.37 Методы программировани я	Владеть: навыками разработки алгоритмов для решения типовых профессиональных задач.
				Б1.О.55.05 Алгоритмы и структуры данных	Знать: основы современной технологии разработки программ. Уметь: разрабатывать алгоритмы для решения сложных задач. Владеть (иметь навык(и)): разработки алгоритмов для решения сложных задач.
				Б2.О.03(Н) Производственная практика (научно-исследовательска я работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ления памятью ЭВМ; - фундаментальные принципы по□вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□туру их основных типов; - определения и понимать суть та□ких понятий как алгоритм, типы

					и структуры данных, управление па□мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно□ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ; - состав и принципы функциониро□вания программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков информаци□онных систем, методы и средства проектирования технологически безопасного программного обеспе□чения; - источники угроз информационной безопасности в компьютерных си□стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ского анализа кода, методы устра□нения уязвимостей; - известные методы анализа

					ПО на наличие уязвимостей, методы ста□тического и динамического ана□лиза программ, методы проведе□ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и проводить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных систем и моделирование угроз безопасно□сти в компьютерных системах с учетом мер по их предотвраще□нию; - применять на практике получен□ные знания и навыки для проверки

					работоспособности ПО и его ана□ лиза на наличие уязвимостей (экс□ пертиза исходного кода, статиче□ ский и динамический анализ, фай□ ззингтестирование); - применять на практике получен□ ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики без□ опасности объекта защиты для ти□ повых решений и требований; - практическими навыками приме□ нения стандартов информацион□ ной безопасности при создании за□ щищенных систем обработки ин□ формации; - навыками использования инстру□ ментальных интеллектуальных си□ стем для обоснования требований и оценки защищенности систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования угроз безопасности в компьютерных си□ стемах с учетом мер по их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная	Знать: - фундаментальные принципы фоннеймановской

				практика (преддипломная)	архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня;- язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач;- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах;- способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации;- источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по

					классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных си- стем и средств вычислитель□ной техники; обосновывать требования к защищенным си□стемам обработки информа□ции и проводить оценку эф□фективности их функциониро□вания; - составлять

					задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования

					спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□менения логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и

					структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компью□терных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать

					програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ зингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования

					ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.18. Умеет применять средства и методы анализа программного обеспечения для выявления закладок.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные

					сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием

					коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ; - состав и принципы функциониро□вания программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков информаци□онных систем, методы и средства проектирования технологически безопасного программного обеспе□чения; - источники угроз информационной безопасности в компьютерных си□стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ского анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□тического и динамического ана□лиза программ, методы проведе□ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную

					слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и проводить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных систем и моделирование угроз безопасно□сти в компьютерных системах с учетом мер по их предотвраще□нию; - применять на практике получен□ные знания и навыки для проверки работоспособности ПО и его ана□лиза на наличие уязвимостей (экс□пертиза исходного кода, статиче□ский и динамический анализ, фай□ззингтестирование); - применять на практике получен□ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий; - навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики без□опасности объекта защиты для ти□повых решений и требований; - практическими навыками приме□нения стандартов информацион□ной безопасности при создании за□щищенных систем обработки ин□формации; -

					навыками использования инстру□ ментальных интеллектуальных си□ стем для обоснования требований и оценки защищенности систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования угроз безопасности в компьютерных си□ стемах с учетом мер по их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения

					задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических

					задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных си- стем и средств вычислитель□ной техники; обосновывать требования к защищенным си□стемам обработки информа□ции и проводить оценку эф□фективности их функциониро□вания; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; -

					навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев;- навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний;- практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ботки данных в

					массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□ менения логических выраже□ ний в реализации условных операторов и циклов- технологии построения алго□ ритмов для решения практи□ ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□ наторных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического

					анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компью□ терных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей

					(экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.19. Умеет	Б1.О.44 Защита программ	Знание видов деструктивных действий программных продуктов,

			применять методы анализа проектных решений для обеспечения защищенности компьютерных систем.	и данных	современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа,

					компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно□ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ; - состав и принципы функциониро□вания программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков информаци□онных систем, методы и средства проектирования технологически безопасного программного обеспе□чения; - источники угроз информационной безопасности в компьютерных си□стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ского анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□тического и

					динамического ана□лиза программ, методы проведе□ния экспертизы исходного кода; - принципы функционирования программных средств криптогра□фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ческих компьютерных средств, тре□бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ность алгоритмов; - конфигурировать программно-ап□паратные средства защиты инфор□мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов постро□ения защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□щенным системам обработки ин□формации и проводить оценку эф□фективности их функционирова□ния; - составлять задание по безопас□ности и профиль защиты при со□здании защищенных систем обра□ботки информации; обосновывать требования к защищенным систе□мам обработки информации и про□водить оценку эффективности их функционирования; - проводить классификацию уязви□мостей информационных систем и моделирование угроз безопасно□сти в компьютерных системах с учетом мер по их предотвраще□нию; - применять на практике получен□ные знания и навыки для проверки работоспособности ПО и его ана□лиза на наличие уязвимостей

					(экс□ пертиза исходного кода, статиче□ ский и динамический анализ, фай□ ззингтестирование); - применять на практике получен□ ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий;- навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ;- навыками формирования и настройки локальной политики без□ опасности объекта защиты для ти□ повых решений и требований;- практическими навыками приме□ нения стандартов информацион□ ной безопасности при создании за□ щищенных систем обработки ин□ формации; - навыками использования инстру□ ментальных интеллектуальных си□ стем для обоснования требований и оценки защищенности систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования угроз безопасности в компьютерных си□ стемах с учетом мер по их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и

					организацию си□стемы юманд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□нения логических выражений в реализации условных операто□ров и циклов; - технологии построения алго□ритмов для решения практиче□ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных

					систем, методы оценки рисков информацион□ ных систем, методы и сред-ства проектирования техноло□ гически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании

					защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического

					анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□мов и ПО, реализующих крип□тографические методы и алго□ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современ□ных компьютерных систем и архитектуру их основных ти□пов; - определения и понимать суть таких понятий как алго□ритм, типы и структуры дан□ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня;- язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□менения логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач;- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила

					математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы функцио□ нирования программно-аппа□ ратных средств защиты ин□ формации; - принципы формирования по□ литики информационной без□ опасности организации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компью□ терных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации

					инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для

					обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.20. Знает программные методы предотвращения несанкционированного доступа к данным.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные

					программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□ торных задач; - алгоритмы построения и по□ иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и

					структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать

					програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для

					обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
			ОПК-13.21. Уметь применять современные средства обеспечения информационной безопасности программ и данных.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные

					программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ ладки программ в средах разра□ ботки программ;- принципы

					оформления и структу рирования программного кода; - правила математической логики, для составления логических выра жений в алгоритмах программ; - состав и принципы функциониро вания программно-аппаратных средств защиты информации; - принципы формирования поли тики информационной безопасно сти организации; - источники угроз информационной безопасности в компьютерных си стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви мостей информационных систем, методы оценки рисков информаци онных систем, методы и средства проектирования технологически безопасного программного обеспе чения; - источники угроз информационной безопасности в компьютерных си стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче ского анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста тического и динамического ана лиза программ, методы проведе ния экспертизы исходного кода; - принципы функционирования программных средств криптогра фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни ческих компьютерных средств, тре бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож ность алгоритмов; - конфигурировать программно-ап паратные средства защиты инфор мации инфраструктуры и

					конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□ щенным системам обработки ин□ формации и проводить оценку эф□ фективности их функционирова□ ния; - составлять задание по безопас□ ности и профиль защиты при со□ здании защищенных систем обра□ ботки информации; обосновывать требования к защищенным систе□ мам обработки информации и про□ водить оценку эффективности их функционирования; - проводить классификацию уязви□ мостей информационных систем и моделирование угроз безопасно□ сти в компьютерных системах с учетом мер по их предотвраще□ нию; - применять на практике получен□ ные знания и навыки для проверки работоспособности ПО и его ана□ лиза на наличие уязвимостей (экс□ пертиза исходного кода, статиче□ ский и динамический анализ, фай□ ззингтестирование); - применять на практике получен□ ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики без□ опасности объекта защиты для ти□ повых решений и требований; - практическими навыками приме□ нения стандартов информацион□ ной безопасности при создании за□ щищенных систем обработки ин□ формации; - навыками использования инстру□ ментальных интеллектуальных си□ стем для обоснования требований и оценки защищенности

					систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования угроз безопасности в компьютерных си□ стемах с учетом мер по их предот□ вращению и проектирования тех□ нологически безопасного про□ граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□ чия уязвимостей, навыками ис□ пользования специализированных утилит статического и динамиче□ ского анализа кода; - специализированными инстру□ ментами и практическими навы□ ками анализа ПО на наличие уяз□ вимостей; - практическими навыками разра□ ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня; - язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□ нения логических выражений в реализации условных операто□ ров и циклов; - технологии построения алго□ ритмов для решения практиче□ ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и

					интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде

					разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного

					кода в виде ком□ ментариев;- навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний;- практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современ□ ных компьютерных систем и архитектуру их основных ти□ пов; - определения и понимать суть таких понятий как алго□ ритм, типы и структуры дан□ ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков

					программиро вания высокого уровня; - язык программирования вы сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при менения логических выраже ний в реализации условных операторов и циклов- технологии построения алго ритмов для решения практи ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби наторных задач; - алгоритмы построения и по иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ ного кода; - правила математической ло гики, для составления логиче ских выражений в алгоритмах программ; - состав и принципы функцио нирования программно-аппа ратных средств защиты ин формации; - принципы формирования по литики информационной без опасности организации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин формационных систем, ме тоды оценки рисков информа ционных систем, методы и средства проектирования тех нологически безопасного про граммного обеспечения; - источники угроз информаци онной безопасности в компью терных системах и сетях, ос новные виды уязвимостей ПО, принципы работы средств ста тического и динамического анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина мического анализа программ, методы проведения экспер тизы исходного кода; - принципы функционирова ния программных средств

					криптографической защиты информации. Уметь: - объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компью□ терных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике

					полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.22. Знает основные программные методы защиты данных	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о

			от несанкционированного доступа.		наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современных компьютерных систем и архи□ тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□ грамма, компилятор и т.п. - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в

					программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□нения логических выражений в реализации условных операто□ров и циклов; - технологии построения алго□ритмов для решения практиче□ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного

					кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ,

					фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев;- навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ ваний;- практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обработки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□ циализированных утилит ста□ тического и динамического анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз□ работки, использования (из□ вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
			ОПК-13.23. Умеет проводить анализ программных средств,	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о

			применяемых для контроля и защиты информации.		наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в

					программах, - области и особенности примене□ния языков программирования вы□сокого уровня; - язык программирования высокого уровня, структурное и объектно□ориентированное программирова□ние. - способы построения и примене□ния логических выражений в реа□лизации условных операторов и циклов; - технологии построения алгорит□мов для решения практических за□дач; - комбинаторные алгоритмы для решения задач в области програм□мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□фейсов; - принципы представления спис□ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□грамм с использованием коммен□тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ботки программ;- принципы оформления и структу□рирования программного кода; - правила математической логики, для составления логических выра□жений в алгоритмах программ; - состав и принципы функциониро□вания программно-аппаратных средств защиты информации; - принципы формирования поли□тики информационной безопасно□сти организации; - источники угроз информационной безопасности в компьютерных си□стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви□мостей информационных систем, методы оценки рисков информаци□онных систем, методы и средства проектирования технологически безопасного программного обеспе□чения; - источники угроз информационной безопасности в компьютерных си□стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче□ского анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□тического и динамического ана□лиза программ, методы проведе□ния экспертизы исходного кода; - принципы функционирования

					программных средств криптогра□ фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар□ хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни□ ческих компьютерных средств, тре□ бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы□ бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож□ ность алгоритмов; - конфигурировать программно-ап□ паратные средства защиты инфор□ мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов построе□ ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□ щенным системам обработки ин□ формации и проводить оценку эф□ фективности их функционирова□ ния; - составлять задание по безопас□ ности и профиль защиты при со□ здании защищенных систем обра□ ботки информации; обосновывать требования к защищенным систе□ мам обработки информации и про□ водить оценку эффективности их функционирования; - проводить классификацию уязви□ мостей информационных систем и моделирование угроз безопасно□ сти в компьютерных системах с учетом мер по их предотвраще□ нию; - применять на практике получен□ ные знания и навыки для проверки работоспособности ПО и его ана□ лиза на наличие уязвимостей (экс□ пертиза исходного кода, статиче□ ский и динамический анализ, фай□ ззинтестирование); - применять на практике

					получен□ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□боты с компьютером, программи□рования на машинно-ориентиро□ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□формационных систем и техноло□гий;- навыками разработки программ; - навыками разработки, документи□рования, тестирования и отладки программ; - навыками документирования про□граммного кода в виде коммента□риев; - навыками тестирование и от□ладки программ;- навыками формирования и настройки локальной политики без□опасности объекта защиты для ти□повых решений и требований;- практическими навыками приме□нения стандартов информацион□ной безопасности при создании за□щищенных систем обработки ин□формации; - навыками использования инстру□ментальных интеллектуальных си□стем для обоснования требований и оценки защищенности систем об□работки информации; - практическими навыками исполь□зования инструментальных средств для моделирования угроз безопасности в компьютерных си□стемах с учетом мер по их предот□вращению и проектирования тех□нологически безопасного про□граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□чия уязвимостей, навыками ис□пользования специализированных утилит статического и динамиче□ского анализа кода; - специализированными инстру□ментами и практическими навы□ками анализа ПО на наличие уяз□вимостей; - практическими навыками разра□ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ; - структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления

					памятью ЭВМ; - фундаментальные принципы повышения производительно сти ЭВМ; - классификацию современных компьютерных систем и архи тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про грамма, компилятор и т.п. - алгоритмы поиска и обра ботки данных в массивах и файлах; - формы и способы представ ления данных в программах; - области и особенности при менения языков программиро вания высокого уровня; - язык программирования вы сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме нения логических выражений в реализации условных операто ров и циклов; - технологии построения алго ритмов для решения практиче ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбина торных задач; - алгоритмы построения и по иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ ного кода; - правила математической ло гики, для составления логиче ских выражений в алгоритмах программ; - состав и принципы функцио нирования программно-аппа ратных средств защиты ин формации; - принципы формирования по литики информационной без опасности организации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор мационных систем, методы оценки рисков информацион ных систем, методы и сред-ства проектирования техноло гически безопасного

					про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирования программных средств крипто□ графической защиты инфор□ мации. Уметь:- объяснять основополагаю□ щие принципы создания и раз□ вития архитектуры компьютер□ ных систем; - выполнять работы по уста□ новке, настройке и обслужива□ нию технических компьютер□ ных средств, требующие зна□ ния их архитектуры и системы команд; - составлять алгоритмы реше□ ния практических задач, гра□ мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач на языке высокого уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и

					прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной политики безопасности объекта защиты для типовых решений и требо□ваний; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обработки информации; - практическими навыками ис□пользования инструментальных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе□циализированных утилит ста□тического и динамического анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; -

					практическими навыками раз□ работки, использования (из□вестных криптографических библиотек) и тестирования специализированных алгорит□ мов и ПО, реализующих крип□ тографические методы и алго□ ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек□ туры ЭВМ;- структуру фоннеймановского процессора и организацию си□ стемы команд ЭВМ; - принципы обмена информа□ цией с внешними устрой□ ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□ сти ЭВМ; - классификацию современ□ ных компьютерных систем и архитектуру их основных ти□ пов; - определения и понимать суть таких понятий как алго□ ритм, типы и структуры дан□ ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра□ ботки данных в массивах и файлах; - формы и способы представ□ ления данных в программах; - области и особенности при□ менения языков программиро□ вания высокого уровня;- язык программирования вы□ сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и при□ менения логических выраже□ ний в реализации условных операторов и циклов- технологии построения алго□ ритмов для решения практи□ ческих задач;- комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□ наторных задач; - алгоритмы построения и по□ иска данных на деревьях и графах;- способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ ного кода; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ; - состав и принципы

					функцио нирования программно-аппа ратных средств защиты ин формации; - принципы формирования по литики информационной без опасности организации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин формационных систем, ме тоды оценки рисков информа ционных систем, методы и средства проектирования тех нологически безопасного про граммного обеспечения; - источники угроз информаци онной безопасности в компью терных системах и сетях, ос новные виды уязвимостей ПО, принципы работы средств ста тического и динамического анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина мического анализа программ, методы проведения экспер тизы исходного кода; - принципы функционирова ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю щие принципы создания и раз вития архитектуры компью терных систем; - выполнять работы по уста новке, настройке и обслужива нию технических компьютер ных средств, требующие зна ниях архитектуры и системы команд; - составлять алгоритмы реше ния практических задач, гра мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы вать алгоритмы решения за дач на языке высокого уровня; - строить математические мо дели для алгоритмов задач в области программирования; - разрабатывать и реализовы вать алгоритмы решения за дач поиска, сортировки, ра боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм мно-аппаратные средства за щиты информации инфра структуры и конечных систем; - проводить разработку поли тики информационной без опасности для различных

					ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных систем и средств вычисли□ тельной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной поли□ тики безопасности объекта за□ щиты для типовых решений и требований; - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками

					ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-13.24. Умеет проводить аттестацию программ и алгоритмов на предмет соответствия требованиям защиты информации.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными

					программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Знать: - фундаментальные принципы фоннеймановской архитектуры ЭВМ; - структуру фоннеймановского про□ цессора и организацию системы команд ЭВМ; - принципы обмена информацией с внешними устройствами и управ□ ления памятью ЭВМ; - фундаментальные принципы по□ вышения производительности ЭВМ; - классификацию современных компьютерных систем и архитек□ туру их основных типов; - определения и понимать суть та□ ких понятий как алгоритм, типы и структуры данных, управление па□ мятью, программа, компилятор и т.п.; - алгоритмы поиска и обработки данных в массивах и файлах; - формы и способы представления данных в программах, - области и особенности примене□ ния языков программирования вы□ сокого уровня; - язык программирования высокого уровня, структурное и объектно□ ориентированное программирова□ ние. - способы построения и примене□ ния логических выражений в реа□ лизации условных операторов и циклов; - технологии построения алгорит□ мов для решения практических за□ дач; - комбинаторные алгоритмы для решения задач в области програм□ мирования; - базовые структуры данных; - способы представления данных в виде структур объектов и интер□ фейсов; - принципы представления спис□ ков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комбинатор□ ных задач; - алгоритмы построения и поиска данных на деревьях и графах; - способы документирования про□ грамм с использованием коммен□ тариев и мета-данных; - технологии тестирования и от□ладки программ в средах разра□ ботки программ; - принципы оформления и структу□ рирования программного кода; - правила математической логики, для составления логических выра□ жений

					в алгоритмах программ; - состав и принципы функциониро вания программно-аппаратных средств защиты информации; - принципы формирования поли тики информационной безопасно сти организации; - источники угроз информационной безопасности в компьютерных си стемах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязви мостей информационных систем, методы оценки рисков информаци онных систем, методы и средства проектирования технологически безопасного программного обеспе чения; - источники угроз информационной безопасности в компьютерных си стемах и сетях, основные виды уязвимостей ПО, принципы работы средств статического и динамиче ского анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста тического и динамического ана лиза программ, методы проведе ния экспертизы исходного кода; - принципы функционирования программных средств криптогра фической защиты информации. Уметь: - объяснять основополагающие принципы создания и развития ар хитектуры компьютерных систем; - выполнять работы по установке, настройке и обслуживанию техни ческих компьютерных средств, тре бующие знания их архитектуры и системы команд; - составлять алгоритмы решения практических задач, грамотно вы бирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовывать алгоритмы решения задач на языке высокого уровня; - строить математические модели для алгоритмов задач в области программирования; - разрабатывать и реализовывать алгоритмы решения задач поиска, сортировки, работы со стеками и очередью, деревьями и графами; - оценивать вычислительную слож ность алгоритмов; - конфигурировать программно-ап паратные средства защиты инфор мации инфраструктуры и конечных систем; - проводить разработку политики информационной безопасности для различных вариантов

					построе□ ния защищенных информационных систем; определять классы защищенности автоматизированных систем и средств вычислительной техники; обосновывать требования к защи□ щенным системам обработки ин□ формации и проводить оценку эф□ фективности их функционирова□ ния; - составлять задание по безопас□ ности и профиль защиты при со□ здании защищенных систем обра□ ботки информации; обосновывать требования к защищенным систе□ мам обработки информации и про□ водить оценку эффективности их функционирования; - проводить классификацию уязви□ мостей информационных систем и моделирование угроз безопасно□ сти в компьютерных системах с учетом мер по их предотвраще□ нию; - применять на практике получен□ ные знания и навыки для проверки работоспособности ПО и его ана□ лиза на наличие уязвимостей (экс□ пертиза исходного кода, статиче□ ский и динамический анализ, фай□ ззингтестирование); - применять на практике получен□ ные знания и навыки для анализа ПО на наличие уязвимостей. Владеть: - навыками самостоятельной ра□ боты с компьютером, программи□ рования на машинно-ориентиро□ ванном языке; - базовой подготовкой в области программирования для решения практических задач в области ин□ формационных систем и техноло□ гий; - навыками разработки программ; - навыками разработки, документи□ рования, тестирования и отладки программ; - навыками документирования про□ граммного кода в виде коммента□ риев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной политики без□ опасности объекта защиты для ти□ повых решений и требований; - практическими навыками приме□ нения стандартов информацион□ ной безопасности при создании за□ щищенных систем обработки ин□ формации; - навыками использования инстру□ ментальных интеллектуальных си□ стем для обоснования требований и оценки защищенности систем об□ работки информации; - практическими навыками исполь□ зования инструментальных средств для моделирования

					угроз безопасности в компьютерных си□стемах с учетом мер по их предот□вращению и проектирования тех□нологически безопасного про□граммного обеспечения; - практическими навыками анализа исходного кода на предмет нали□чия уязвимостей, навыками ис□пользования специализированных утилит статического и динамиче□ского анализа кода; - специализированными инстру□ментами и практическими навы□ками анализа ПО на наличие уяз□вимостей; - практическими навыками разра□ботки, использования (известных криптографических библиотек) и тестирования специализированных алгоритмов и ПО, реализующих криптографические методы и алго□ритмы.
				Б2.О.04(Пд) Производственная практика (преддипломная)	Знать: - фундаментальные принципы фоннеймановской архитек□туры ЭВМ;- структуру фоннеймановского процессора и организацию си□стемы команд ЭВМ; - принципы обмена информа□цией с внешними устрой□ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно□сти ЭВМ; - классификацию современных компьютерных систем и архи□тектуру их основных типов; - определения и понимать суть таких понятий как алгоритм, типы и структуры данных, управление памятью, про□грамма, компилятор и т.п. - алгоритмы поиска и обра□ботки данных в массивах и файлах; - формы и способы представ□ления данных в программах; - области и особенности при□менения языков программиро□вания высокого уровня; - язык программирования вы□сокого уровня, структурное и объектно-ориентированное программирование. - способы построения и приме□нения логических выражений в реализации условных операто□ров и циклов; - технологии построения алго□ритмов для решения практиче□ских задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; -

					алгоритмы решений комбина□торных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей инфор□мационных систем, методы оценки рисков информацион□ных систем, методы и сред-ства проектирования техноло□гически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирования программных средств крипто□графической защиты инфор□мации. Уметь:- объяснять основополагаю□щие принципы создания и раз□вития архитектуры компьютер□ных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого

					уровня; - строить математические мо□ дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□ вать алгоритмы решения за□ дач поиска, сортировки, ра□ боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□ мно-аппаратные средства за□ щиты информации инфра□ структуры и конечных систем; - проводить разработку поли□ тики информационной без□ опасности для различных ва□ риантов построения защищен□ ных информационных систем; определять классы защищен□ ности автоматизированных си- стем и средств вычислитель□ ной техники; обосновывать требования к защищенным си□ стемам обработки информа□ ции и проводить оценку эф□ фективности их функциониро□ вания; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информационных систем и моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с компьютером, про□ граммирования на машинно□ ориентированном языке; - базовой подготовкой в обла□ сти программирования для ре□ шения практических задач в области информационных си□ стем и технологий; - навыками разработки про□ грамм; - навыками разработки, доку□ ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде ком□ ментариев; - навыками тестирование и от□ ладки программ; - навыками формирования и настройки локальной

					политики безопасности объекта защиты для типовых решений и требо ваний; - практическими навыками применения стандартов ин формационной безопасности при создании защищенных си стем обработки информации; - навыками использования ин струментальных интеллекту альных систем для обоснова ния требований и оценки за щищенности систем обработки информации; - практическими навыками ис пользования инструменталь ных средств для моделирова ния угроз безопасности в ком пьютерных системах с учетом мер по их предотвращению и проектирования технологиче ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования спе циализированных утилит ста тического и динамического анализа кода; - специализированными ин струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками раз работки, использования (из вестных криптографических библиотек) и тестирования специализированных алгорит мов и ПО, реализующих крип тографические методы и алго ритмы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - фундаментальные принципы фоннеймановской архитек туры ЭВМ; - структуру фоннеймановского процессора и организацию си стемы команд ЭВМ; - принципы обмена информа цией с внешними устрой ствами и управления памятью ЭВМ; - фундаментальные принципы повышения производительно сти ЭВМ; - классификацию современ ных компьютерных систем и архитектуру их основных ти пов; - определения и понимать суть таких понятий как алго ритм, типы и структуры дан ных, управление памятью, программа, компилятор и т.п.; - алгоритмы поиска и обра ботки данных в массивах и файлах; - формы и способы представ ления данных в программах; - области и особенности при менения языков программиро вания высокого уровня; - язык программирования вы сокого уровня, структурное и объектно-ориентированное

					программирование. - способы построения и при□менения логических выраже□ний в реализации условных операторов и циклов- технологии построения алго□ритмов для решения практи□ческих задач; - комбинаторные алгоритмы для решения задач в области программирования; - базовые структуры данных; - способы представления дан□ных в виде структур объектов и интерфейсов; - принципы представления списков, деревьев, графов; - основные алгоритмы поиска и сортировки данных; - алгоритмы решений комби□наторных задач; - алгоритмы построения и по□иска данных на деревьях и графах; - способы документирования программ с использованием комментариев и мета-данных; - технологии тестирования и отладки программ в средах разработки программ; - принципы оформления и структурирования программ□ного кода; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ; - состав и принципы функцио□нирования программно-аппа□ратных средств защиты ин□формации; - принципы формирования по□литики информационной без□опасности организации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - объяснять основополагаю□щие принципы создания и раз□вития

					архитектуры компью□терных систем; - выполнять работы по уста□новке, настройке и обслужива□нию технических компьютер□ных средств, требующие зна□ния их архитектуры и системы команд; - составлять алгоритмы реше□ния практических задач, гра□мотно выбирать инструменты для решения задач; - принципы отладки программ; - работать в интегрированной среде разработки программ на языке высокого уровня; - разрабатывать и реализовы□вать алгоритмы решения за□дач на языке высокого уровня; - строить математические мо□дели для алгоритмов задач в области программирования; - разрабатывать и реализовы□вать алгоритмы решения за□дач поиска, сортировки, ра□боты со стеками и очередью, деревьями и графами; - оценивать вычислительную сложность алгоритмов; - конфигурировать програм□мно-аппаратные средства за□щиты информации инфра□структуры и конечных систем; - проводить разработку поли□тики информационной без□опасности для различных ва□риантов построения защищен□ных информационных систем; определять классы защищен□ности автоматизированных систем и средств вычисли□тельной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - навыками самостоятельной работы с

					компьютером, про□граммирования на машинно□ориентированном языке; - базовой подготовкой в обла□сти программирования для ре□шения практических задач в области информационных си□стем и технологий; - навыками разработки про□грамм; - навыками разработки, доку□ментирования, тестирования и отладки программ; - навыками документирования программного кода в виде комментариев; - навыками тестирование и от□ладки программ; - навыками формирования и настройки локальной поли□тики безопасности объекта за□щиты для типовых решений и требований; - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
	ОПК-14	Способен проектировать базы данных, администрировать системы управления	ОПК-14.1. Знает характеристики и типы систем баз данных.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа

		базами данных в соответствии с требованиями по защите информации;			данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
			ОПК-14.2. Знает основные языки запросов.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
			ОПК-14.3. Знает физическую организацию баз данных и принципы (основы) их защиты.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей

			ОПК-14.4. Умеет проектировать реляционные базы данных и осуществлять нормализацию отношений при проектировании реляционной базы данных.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - понятие защищенной си□стемы баз данных, этапы и методы проектирования защи□щенных систем баз данных, модели представления ин□формации на концептуаль□ном, логическом и физиче□ском уровнях, нормальные формы баз данных и алго□ритмы их построения, крите□рии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компь□ютерных систем, методы обеспечения конфиденциаль□ности, целостности и доступ□ности в системах баз данных, возможности языка SQL (TransactSQL) при обеспече□нии целостности и конфиден□циальности информации в си□стемах баз данных;- этапы и методы проектиро□вания защищенных систем с базами данных, методы обес□печения конфиденциальности, целостности и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ. Уметь: - разрабатывать функцио□нальную и информационную модели защищенной системы баз данных, включая концеп□туальную, логическую и физи- ческую модели; разрабаты□вать нормализованную схему базы данных; - применять методы защиты информации в системах управления

					базами данных; - осуществлять проектирова□ ние и реализацию защищен□ ных систем баз данных с ис□ пользованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, построе□ ния нормализованных баз данных, навыками разработки функциональной и информа□ ционной моделей системы баз данных с использованием ин□ струментальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения це□ лостности и конфиденциаль□ ности СУБД;- навыками работы с инстру□ ментальными средствами проектирования баз данных, системами управления ба□ зами данных, средствами обеспечения целостности и конфиденциальности СУБД.
			ОПК-14.5. Умеет настраивать и применять современные системы управления базами данных.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - понятие защищенной си□ стемы баз данных, этапы и методы проектирования защи□ щенных систем баз данных, модели представления ин□ формации на концептуаль□ ном, логическом и физиче□ ском уровнях, нормальные формы баз данных и алго□ ритмы их построения, крите□ рии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компь□ ютерных

					систем, методы обеспечения конфиденциаль□ ности, целостности и доступ□ ности в системах баз данных, возможности языка SQL (TransactSQL) при обеспече□ нии целостности и конфиден□ циальнсти информации в си□ стемах баз данных; - этапы и методы проектиро□ вания защищенных систем с базами данных, методы обес□ печения конфиденциальности, целостности и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ. Уметь: - разрабатывать функцио□ нальную и информационную модели защищенной системы баз данных, включая концеп□ туальную, логическую и физи- ческую модели; разрабаты□ вать нормализованную схему базы данных; - применять методы защиты информации в системах управления базами данных; - осуществлять проектирова□ ние и реализацию защищен□ ных систем баз данных с ис□ пользованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, постро□ ния нормализованных баз данных, навыками разработки функциональной и информа□ ционной моделей системы баз данных с использованием ин□ струмнтальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения це□ лостности и конфиденциаль□ ности СУБД;- навыками работы с инстру□ ментальными средствами проектирования баз данных, системами управления ба□ зами данных, средствами обеспечения целостности и конфиденциальности СУБД.
			ОПК-14.6. Владеет методикой и навыками составления запросов для поиска информации в базах данных.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы

					установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - понятие защищенной си□ стемы баз данных, этапы и методы проектирования защи□ щенных систем баз данных, модели представления ин□ формации на концептуаль□ ном, логическом и физиче□ ском уровнях, нормальные формы баз данных и алго□ ритмы их построения, крите□ рии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компь□ ютерных систем, методы обеспечения конфиденциаль□ ности, целостности и доступ□ ности в системах баз данных, возможности языка SQL (TransactSQL) при обеспече□ нии целостности и конфиден□ циальности информации в си□ стемах баз данных; - этапы и методы проектиро□ вания защищенных систем с базами данных, методы обес□ печения конфиденциальности, целостности и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ. Уметь: - разрабатывать функцио□ нальную и информационную модели защищенной системы баз данных, включая концеп□ туальную, логическую и физи- ческую модели; разрабаты□ вать нормализованную схему базы данных; - применять методы защиты информации в системах управления базами данных; - осуществлять проектирова□ ние и реализацию защищен□ ных систем баз данных с ис□ пользованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, постро□ ния нормализованных баз данных, навыками

					разработки функциональной и информа□ционной моделей системы баз данных с использованием ин□струментальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения це□лостности и конфиденциаль□ности СУБД; - навыками работы с инстру□ментальными средствами проектирования баз данных, системами управления ба□зами данных, средствами обеспечения целостности и конфиденциальности СУБД.
			ОПК-14.7. Знает основные критерии защищенности баз данных и методы оценивания механизмов защиты.	Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных

					БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
			ОПК-14.8. Знает механизмы обеспечения конфиденциальности, целостности и высокой доступности баз данных.	Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.

			ОПК-14.9. Знает особенности применения криптографической защиты в СУБД.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
				Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты

					защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
			ОПК-14.10. Знает этапы проектирования системы защиты в СУБД.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
				Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту

					содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
			ОПК-14.11. Умеет пользоваться средствами защиты, предоставляемыми СУБД.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе встроенных механизмов аутентификации и ролей
				Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты

					информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - понятие защищенной си□стемы баз данных, этапы и методы проектирования защи□щенных систем баз данных, модели представления ин□формации на концептуаль□ном, логическом и физиче□ском уровнях, нормальные формы баз данных и алго□ритмы их построения, крите□рии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компь□ютерных

					систем, методы обеспечения конфиденциаль□ ности, целостности и доступ□ ности в системах баз данных, возможности языка SQL (TransactSQL) при обеспече□ нии целостности и конфиден□ циальности информации в си□ стемах баз данных; - этапы и методы проектиро□ вания защищенных систем с базами данных, методы обес□ печения конфиденциальности, целостности и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ. Уметь: - разрабатывать функцио□ нальную и информационную модели защищенной системы баз данных, включая концеп□ туальную, логическую и физи- ческую модели; разрабаты□ вать нормализованную схему базы данных; - применять методы защиты информации в системах управления базами данных; - осуществлять проектирова□ ние и реализацию защищен□ ных систем баз данных с ис□ пользованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, постро□ ения нормализованных баз данных, навыками разработки функциональной и информа□ ционной моделей системы баз данных с использованием ин□ струментальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения це□ лостности и конфиденциаль□ ности СУБД; - навыками работы с инстру□ ментальными средствами проектирования баз данных, системами управления ба□ зами данных, средствами обеспечения целостности и конфиденциальности СУБД.
			ОПК-14.12. Умеет создавать дополнительные средства защиты баз данных.	Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД

					для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - понятие защищенной си□стемы баз данных, этапы и методы проектирования защи□щенных систем баз данных, модели представления ин□формации на концептуаль□ном, логическом и физиче□ском уровнях, нормальные формы баз данных и алго□ритмы их построения, крите□рии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компь□ютерных систем, методы обеспечения конфиденциаль□ности, целостности и доступ□ности в системах баз данных, возможности языка SQL (TransactSQL) при обеспече□нии целостности и

					конфиден□ циальности информации в си□ стемах баз данных;- этапы и методы проектиро□ вания защищенных систем с базами данных, методы обес□ печения конфиденциальности, целостности и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ. Уметь: - разрабатывать функцио□ нальную и информационную модели защищенной системы баз данных, включая концеп□ туальную, логическую и физи- ческую модели; разрабаты□ вать нормализованную схему базы данных; - применять методы защиты информации в системах управления базами данных; - осуществлять проектирова□ ние и реализацию защищен□ ных систем баз данных с ис□ пользованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, построе□ ния нормализованных баз данных, навыками разработки функциональной и информа□ ционной моделей системы баз данных с использованием ин□ струментальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения це□ лостности и конфиденциаль□ ности СУБД;- навыками работы с инстру□ ментальными средствами проектирования баз данных, системами управления ба□ зами данных, средствами обеспечения целостности и конфиденциальности СУБД.
			ОПК-14.13. Умеет проводить анализ и оценивание механизмов защиты баз данных.	Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности

					реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - понятие защищенной си□стемы баз данных, этапы и методы проектирования защи□щенных систем баз данных, модели представления ин□формации на концептуаль□ном, логическом и физиче□ском уровнях, нормальные формы баз данных и алго□ритмы их построения, крите□рии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компь□ютерных систем, методы обеспечения конфиденциаль□ности, целостности и доступ□ности в системах баз данных, возможности языка SQL (TransactSQL) при обеспече□нии целостности и конфиден□циальности информации в си□стемах баз данных;- этапы и методы проектиро□вания защищенных систем с базами данных, методы обес□печения конфиденциальности, целостности

					и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической ло□ гики, для составления логиче□ ских выражений в алгоритмах программ. Уметь: - разрабатывать функцио□ нальную и информационную модели защищенной системы баз данных, включая концеп□ туальную, логическую и физи- ческую модели; разрабаты□ вать нормализованную схему базы данных; - применять методы защиты информации в системах управления базами данных; - осуществлять проектирова□ ние и реализацию защищен□ ных систем баз данных с ис□ пользованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, построе□ ния нормализованных баз данных, навыками разработки функциональной и информа□ ционной моделей системы баз данных с использованием ин□ струментальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения це□ лостности и конфиденциаль□ ности СУБД;- навыками работы с инстру□ ментальными средствами проектирования баз данных, системами управления ба□ зами данных, средствами обеспечения целостности и конфиденциальности СУБД.
			ОПК-14.14. Владеет методикой и навыками использования средств защиты, предоставляемых СУБД.	Б1.О.38 Системы управления базами данных	Знание основных принципов проектирования баз данных с использованием современных инструментальных средств. Умение создавать прикладные системы для быстрого и надежного поиска информации в БД. Владение типовыми навыками решения профессиональных и исследовательских задач в области анализа данных и организации транзакций. Знание основные принципы установки и конфигурирования СУБД. Умение разрабатывать надежную и безопасную схему хранения и обработки данных, исключающую аномалии, взаимные блокировки и нарушения целостности данных, и удовлетворяющую требованиям компьютерной безопасности. Владение навыками администрирования и конфигурирования СУБД на основе

					встроенных механизмов аутентификации и ролей
				Б1.О.43 Основы построения защищенных баз данных	Знать: основные принципы проектирования защищенных баз данных с использованием программно-аппаратных средств защиты информации и средства криптографической защиты информации; основные принципы построения подсистем информационной безопасности в сетях, использующих корпоративные БД; жизненный цикл разработки приложений БД для заданной предметной области и систем защиты данных в СУБД; механизмы аутентификации серверов и пользователей БД; основные методы и подходы к оцениванию эффективности реализации систем защиты информации и действующих политик безопасности в защищенных БД. Уметь: выполнять резервное копирование данных, осуществлять криптографическую защиту содержимого таблиц БД; управлять соединениями с базой данных, реализовывать защиту от взаимных блокировок; управлять транзакциями, распознавать блокировки; моделировать основные угрозы и тестировать защиту от них; создавать прикладные системы для автоматизации CRUD операций БД; разрабатывать и использовать алгоритмы работы с данными, удовлетворяющие требованиям компьютерной безопасности. управлять пользователями, ролями, привилегиями, реализовывать резервное копирование данных; документировать структуру и компоненты защищенной БД, клиентской и серверной части приложения, составлять инструкции и диаграммы развертывания. Владеть навыками: решения профессиональных и исследовательских задач в области анализа данных и организации транзакций; безопасного проектирования и администрирования БД; построения безопасных БД на основе встроенных в СУБД механизмов и ролей; применения современных эффективных систем и подходов защиты информации и политик безопасности в компьютерных системах с защищенными БД.
				Б2.О.06(П) Производственная практика по получению профессиональны	Знать: - понятие защищенной си□стемы баз данных, этапы и методы проектирования защи□щенных систем баз данных, модели представления ин□формации на концептуаль□ном,

				х умений и навыков в области профессиональной деятельности	логическом и физиче□ском уровнях, нормальные формы баз данных и алго□ритмы их построения, крите□рии защищенных баз данных, общие принципы построения систем управления базами данных (СУБД); - модели безопасности компь□ютерных систем, методы обеспечения конфиденциаль□ности, целостности и доступ□ности в системах баз данных, возможности языка SQL (TransactSQL) при обеспече□нии целостности и конфиден□циальности информации в си□стемах баз данных; - этапы и методы проектиро□вания защищенных систем с базами данных, методы обес□печения конфиденциальности, целостности и доступности информации в системах баз данных и их реализацию в конкретных СУБД; - правила математической ло□гики, для составления логиче□ских выражений в алгоритмах программ. Уметь: - разрабатывать функцио□нальную и информационную модели защищенной системы баз данных, включая концеп□туальную, логическую и физи- ческую модели; разрабаты□вать нормализованную схему базы данных; - применять методы защиты информации в системах управления базами данных; - осуществлять проектирова□ние и реализацию защищен□ных систем баз данных с ис□пользованием современных СУБД; - оценивать вычислительную сложность алгоритмов. Владеть: - навыками структурного и объектно-ориентированного проектирования защищенных систем баз данных, постро□ения нормализованных баз данных, навыками разработки функциональной и информа□ционной моделей системы баз данных с использованием ин□струментальных средств; - навыками работы с СУБД, инструментами разработчика и администратора баз данных, средствами обеспечения це□лостности и конфиденциаль□ности СУБД; - навыками работы с инстру□ментальными средствами проектирования баз данных, системами управления ба□зами данных, средствами обеспечения целостности и конфиденциальности СУБД.
	ОПК-15	Способен администриров	ОПК-15.1. Знает архитектуру основных	Б1.О.22 Аппаратные средства вычислительной	Знает особенности аппаратной реализации ВТ различных классов: суперкомпьютеры, универсальные и управляющие ЭВМ.

		ать компьютерные сети и контролироват ь корректность их функционирования;	типов современных компьютерных систем.	техники	Проектирование сети крупной фирмы (подбор сетевого оборудования, требуемого для создания сети организации)
				Б1.О.34 Компьютерные сети	
			ОПК-15.2. Знает основы организации и построения компьютерных сетей.	Б1.О.34 Компьютерные сети	
			ОПК-15.3. Знает эталонную модель взаимодействия открытых систем.	Б1.О.34 Компьютерные сети	
			ОПК-15.4. Знает функции, принципы действия и алгоритмы работы сетевого оборудования.	Б1.О.34 Компьютерные сети	
			ОПК-15.5. Умеет реализовывать приложения для сетевых интерфейсов на нескольких современных программно-аппаратных платформах.	Б1.О.34 Компьютерные сети	
				Б2.О.06(П) Производственная практика по получению профессиональны х умений и навыков в области профессиональной деятельности	Знать: - полномочную и дискрецион□ ную политики доступом; - архитектуру, функции и спо□ собы внедрения в инфра□ структуру криптографической защиты информации. Уметь: - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами выбора типов и то□ пологий сетевого экранирова□ ния;- навыками развертывания и настройки программно-аппа□ ратных средств защиты ин□ формации.
			ОПК-15.6. Умеет осуществлять проектирование и оптимизацию функционирования компьютерных сетей.	Б1.О.34 Компьютерные сети	
				Б2.О.06(П) Производственная практика по получению профессиональны х умений и навыков в области профессиональной деятельности	Знать: - полномочную и дискрецион□ ную политики доступом; - архитектуру, функции и спо□ собы внедрения в инфра□ структуру криптографической защиты информации. Уметь: - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами выбора типов и то□ пологий сетевого экранирова□ ния;- навыками развертывания и настройки программно-аппа□ ратных средств защиты ин□ формации.
			ОПК-15.7. Владеет	Б1.О.34 Компьютерные	

			навыками администрирования компьютерных сетей.	сети	
				Б1.О.42 Основы построения защищенных компьютерных сетей	владеть: навыками управления сетевым оборудованием
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - полномочную и дискрецион□ ную политики доступом; - архитектуру, функции и спо□ собы внедрения в инфра□ структуру криптографической защиты информации. Уметь: - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами выбора типов и то□ пологий сетевого экранирова□ ния;- навыками развертывания и настройки программно-аппа□ ратных средств защиты ин□ формации.
			ОПК-15.8. Владеет навыками работы с сетевым оборудованием и сетевым программным обеспечением.	Б1.О.34 Компьютерные сети	
				Б1.О.42 Основы построения защищенных компьютерных сетей	владеть: навыками управления сетевым оборудованием и сетевыми ОС
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и

					администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - полномочную и дискрецион□ ную политики доступом; - архитектуру, функции и спо□ собы внедрения в инфра□ структуру криптографической защиты информации. Уметь: - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами выбора типов и то□ пологий сетевого экранирова□ ния; - навыками развертывания и настройки программно-аппа□ ратных средств защиты ин□ формации.
	ОПК-16	Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;	ОПК-16.1. Знает средства и методы хранения и передачи аутентификационной информации в компьютерных системах и сетях.	Б1.О.42 Основы построения защищенных компьютерных сетей	знать: технологии удаленного доступа с использованием распределенной и централизованной проверками подлинности
			ОПК-16.2. Знает механизмы реализации атак в сетях TCP/IP.	Б1.О.42 Основы построения защищенных компьютерных сетей	знать: типовые уязвимости 2 и 3 уровней
			ОПК-16.3. Знает основные протоколы идентификации и аутентификации абонентов сети.	Б1.О.42 Основы построения защищенных компьютерных сетей	знать:метода проверки подлинности при удаленом доступе и с с использованием ААА
			ОПК-16.4. Знает защитные механизмы и средства обеспечения сетевой безопасности.	Б1.О.42 Основы построения защищенных компьютерных сетей	знать: принцип и реализации сетевого карантина

			ОПК-16.5. Знает средства и методы предотвращения и обнаружения вторжений.	Б1.О.42 Основы построения защищенных компьютерных сетей	знать: основы технологий DPI/IPS/IDS
			ОПК-16.6. Умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе.	Б1.О.42 Основы построения защищенных компьютерных сетей	уметь: конфигурировать групповые политики, связанные с реализацией процедур безопасности в ОС
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза□ имодействия открытых си□ стем; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - планировать и устанавли□ вать инфраструктуры откры□ тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; -

					настраивать основные типы телекоммуникационного обо рудования IP сетей;- основными пакетами, приме няемыми для расчётов и мо делирования в телекоммуни кациях; - практическими навыками применения современных криптографических алгорит мов и протоколов; - практическими навыками ра боты с известными криптогра фическими библиотеками; - методами обеспечения за щиты данных на этапе пере дачи в IP-сетях; - методами выбора типов и то пологий сетевого экранирова ния;- навыками развертывания и настройки программно-аппа ратных средств защиты ин формации.
			ОПК-16.7. Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях.	Б1.О.42 Основы построения защищенных компьютерных сетей	уметь: конфигурировать сетевые экраны типа "пакетный фильтр"; систему ViPNet IDS
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза имодействия открытых си стем; - основные принципы класси фикации и количественных характеристик технических ка налов утечки информации; - основные способы и сред ства защиты информации от утечки по техническим кана лам и контроля эффективно сти защиты информации; - основы принципов организа ции защиты информации от утечки по техническим кана лам на объектах информати зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче ской защиты информации. Уметь: - классифицировать функцио нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си стем; - настраивать основные типы телекоммуникационного обо рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации

					от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - планировать и устанавли□ вать инфраструктуры откры□ тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей;- основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - методами обеспечения за□ щиты данных на этапе пере□ дачи в IP-сетях; - методами выбора типов и то□ пологий сетевого экранирова□ ния;- навыками развертывания и настройки программно-аппа□ ратных средств защиты ин□ формации.
			ОПК-16.8. Умеет осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.	Б1.О.42 Основы построения защищенных компьютерных сетей	уметь: создавать и конфигурировать защищенные сети на основе технологий VipNet, Континент, IPsec/VPN
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое

					программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза□ имодействия открытых си□ стем; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - планировать и устанавли□ вать

					инфраструктуры откры□тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей;- основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; - практическими навыками применения современных криптографических алгорит□мов и протоколов;- практическими навыками ра□боты с известными криптогра□фическими библиотеками; - методами обеспечения за□щиты данных на этапе пере□дачи в IP-сетях; - методами выбора типов и то□пологий сетевого экранирова□ния;- навыками развертывания и настройки программно-аппа□ратных средств защиты ин□формации.
			ОПК-16.9. Владеет навыками настройки межсетевых экранов.	Б1.О.42 Основы построения защищенных компьютерных сетей	владеть: навыками конфигурирования L2-L7 экранов
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального

					назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза□ имодействия открытых си□ стем; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - планировать и устанавли□ вать инфраструктуры откры□ тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: -

					методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо рудования IP сетей;- основными пакетами, приме няемыми для расчётов и мо делирования в телекоммуни кациях; - практическими навыками применения современных криптографических алгорит мов и протоколов; - практическими навыками ра боты с известными криптогра фическими библиотеками; - методами обеспечения за щиты данных на этапе пере дачи в IP-сетях; - методами выбора типов и то пологий сетевого экранирова ния;- навыками развертывания и настройки программно-аппа ратных средств защиты ин формации.
			ОПК-16.10. Владеет методиками анализа сетевого трафика.	Б1.О.42 Основы построения защищенных компьютерных сетей	владеть: навыками перехвата и анализа сетевого трафика
				Б1.О.50 Инсталляция и настройка программного обеспечения	Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Умение производить установку, наладку, тестирование и обслуживание современного программного обеспечения специального назначения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение. Владение навыками наладки и администрирования программного обеспечения специального назначения, включая операционные системы. Знание методов восстановления работоспособности операционных систем и

					программ специального назначения при возникновении нештатных ситуаций. Умение восстанавливать работоспособность операционных систем и программ специального назначения при возникновении нештатных ситуаций. Владение навыками обеспечения повышения надёжности функционирования программного обеспечения специального назначения с позиции администратора системы.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза□ имодействия открытых си□ стем; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - планировать и устанавли□ вать инфраструктуры откры□ тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного

					обо рудования IP сетей;- основными пакетами, приме няемыми для расчётов и мо делирования в телекоммуни кациях; - практическими навыками применения современных криптографических алгорит мов и протоколов; - практическими навыками ра боты с известными криптогра фическими библиотеками; - методами обеспечения за щиты данных на этапе пере дачи в IP-сетях; - методами выбора типов и то пологий сетевого экранирова ния;- навыками развертывания и настройки программно-аппа ратных средств защиты ин формации.
			ОПК-16.11. Знает основные виды деструктивных воздействий на программные продукты.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты,

					средства криптографической защиты информации
			ОПК-16.12. Умеет выявлять действие вредоносных программ, и определять характер их воздействия.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза□ имодействия открытых си□ стем; - основные принципы класси□ фикации и количественных характеристик технических

				профессиональной деятельности	ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - планировать и устанавли□ вать инфраструктуры откры□ тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей;- основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - методами обеспечения за□ щиты данных на этапе пере□ дачи в IP-сетях; - методами выбора типов и то□ пологий сетевого экранирова□ ния; - навыками развертывания и настройки программно-аппа□ ратных средств защиты ин□ формации.

			ОПК-16.13. Знает современные методы анализа программных решений по обеспечению защищенности компьютерных систем.	Б1.О.44 Защита программ и данных	Знание видов деструктивных действий программных продуктов, современных подходов к формированию моделей политик безопасности Умение определить признаки, свидетельствующие о наличии вредоносных программ, и определить характер их действия. Владение методами определения вредоносных программ и современными инструментальными средствами борьбы с вредоносными программами. Знание современных методов анализа проектных решений по обеспечению защищенности компьютерных систем, рынка современных антивирусных программных продуктов. Умение применять современные методы анализа проектных решений по обеспечению защищенности компьютерных систем. Владение современными методами анализа проектных решений по обеспечению защищенности компьютерных систем. Знание современных программно-аппаратных средств обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации. Умение применять современные программно-аппаратные средства обеспечения информационной безопасности компьютерных систем. Владение современными программно□ аппаратными средствами обеспечения информационной безопасности компьютерных систем, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
			ОПК-16.14. Умеет производить оценку технического состояния аппаратных средств защиты информации.	Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы

					основных блоков современных средств за□щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ций владеть: навыками восстановле□ния штатного режима работы технических средств защиты ин□ формации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза□имодействия открытых си□стем; - основные принципы класси□фикации и количественных характеристик технических ка□налов утечки информации; - основные способы и сред□ства защиты информации от утечки по техническим кана□лам и контроля эффективно□сти защиты информации; - основы принципов организа□ции защиты информации от утечки по техническим кана□лам на объектах информати□зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче□ской защиты информации. Уметь: - классифицировать функцио□нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□стем; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто□графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ническим каналам и контроля эффективности защиты ин□формации; - планировать и устанавли□вать инфраструктуры откры□тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□рудования IP сетей; - основными пакетами, приме□няемыми для расчётов и мо□делирования в телекоммуни□кациях; -

					практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ ботыс известными криптогра□ фическими библиотеками; - методами обеспечения за□ щиты данных на этапе пере□ дачи в IP-сетях; - методами выбора типов и то□ пологий сетевого экранирова□ ния; - навыками развертывания и настройки программно-аппа□ ратных средств защитыин□ формации.
			ОПК-16.15. Знает методологию применения технических средств диагностики состояния устройств защиты информации.	Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации
			ОПК-16.16. Умеет выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций.	Б1.О.52 Теория радиотехнических систем	знать: фундаментальные зако□ номерности, связанные с получе□ нием сигналов и их передачей по каналам связи, обработкой и преобразованием в информаци□ онных системах при обеспечении защиты информации. уметь: производить оценку тех□ нического состояния аппаратных средств защиты информации владеть: навыками применения технических средств для диагно□ стики состояния устройств защи□ ты информации знать: функциональное назначе□ ние и принципы работы основных блоков современных средств за□ щиты информации уметь: выполнять работы по вос□ становлению работоспособности средств защиты информации при возникновении нештатных ситуа□ ций владеть: навыками восстановле□ ния штатного режима работы технических средств защиты ин□ формации

				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - принципы построения сетей связи и передачи информа□ ции; - принципы взаимодействия телекоммуникационных си- стем согласно принципам вза□ имодействия открытых си□ стем; - основные принципы класси□ фикации и количественных характеристик технических ка□ налов утечки информации; - основные способы и сред□ ства защиты информации от утечки по техническим кана□ лам и контроля эффективно□ сти защиты информации; - основы принципов организа□ ции защиты информации от утечки по техническим кана□ лам на объектах информати□ зации; - - принципы и детали работы IPsec, VPN, ViPNet, АПКШ Континент. - методы и средства техниче□ ской защиты информации. Уметь: - классифицировать функцио□ нальность элементов сетей связи и передачи информации по семиуровневой модели взаимодействия открытых си□ стем; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - устанавливать, настраивать и использовать на практике специализированные крипто□ графические программные средства (криптографические библиотеки OpenSSL, cryptopp и пр.); - применять математические модели для оценки стойкости СКЗИ; - определять необходимые способы и средства защиты информации от утечки по тех□ ническим каналам и контроля эффективности защиты ин□ формации; - планировать и устанавли□ вать инфраструктуры откры□ тых ключей, VPN-решения; - конфигурировать сетевые экраны 2-7 уровней. Владеть: - методами моделирования телекоммуникационных сетей; - настраивать основные типы телекоммуникационного обо□ рудования IP сетей; - основными пакетами, приме□ няемыми для расчётов и мо□ делирования в телекоммуни□ кациях; - практическими навыками применения современных криптографических алгорит□ мов и протоколов; - практическими навыками ра□ боты с известными криптогра□ фическими библиотеками; - методами обеспечения за□ щиты данных на этапе пере□ дачи в IP-сетях; - методами выбора типов и то□ пологий

					сетевого экранирова□ ния;- навыками развертывания и настройки программно-аппа□ ратных средств защиты ин□ формации.
	ОПК-17	Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма.	ОПК-17.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире.	Б1.О.02 История России	Знать основные историче□ ские факты, даты, события и имена исторических деяте□ лей России; основные про□ цессы отечественной исто□ рии в контексте мировой ис□ тории
			ОПК-17.2. Знает ключевые события истории России и мира, выдающихся деятелей России.	Б1.О.02 История России	Знать основные историче□ ские факты, даты, события и имена исторических деяте□ лей России; основные про□ цессы отечественной исто□ рии в контексте мировой ис□ тории
			ОПК-17.3. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий.	Б1.О.02 История России	Уметь критически восприни□ мать, анализировать и оцени□ вать историческую информа□ цию, факты и механизмы ис□ торических изменен
			ОПК-17.4. Умеет формулировать и аргументировано отстаивать собственную позицию по различным проблемам истории России, опираясь на принципы историзма и научной объективности.	Б1.О.02 История России	Уметь критически восприни□ мать, анализировать и оцени□ вать историческую информа□ цию, факты и механизмы ис□ торических изменени
	ОПК-1.1	Способен проводить анализ защищенности и находить уязвимости компьютерной	ОПК-1.1.1. Знает принципы построения защищенных компьютерных систем и сетей.	Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем	Знать: принципы построения защищенных компьютерных систем и сетей, этапы со□ здания защищенных компьютерных си□ стем, стандарты информационной без□ опасности и руководящие документы ФСТЭК России (Гостехкомиссии России), модели безопасности компьютерных си□ стем, методы оценки защищенности ком□ пьютерных систем, методы проектирова□ ния

		системы			защищенных компьютерных систем. Уметь: определять классы защищенности автоматизирванных систем и средств вы□числительной техники; обосновывать тре□бования к защищенным системам обра□ботки информации и проводить оценку эффективности их функционирования. Владеть: практическими навыками приме□нения стандартов информационной без□опасности при создании защищенных си□стем обработки информации; навыками использования инструментальных для обоснования требований и оценки защи□щенности систем обработки информаци
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требо□ваний и оценки защищенности систем обработки информа□ции; порядок сертификации защищенных систем обра□ботки информации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - определять классы защи□щенности автоматизирован□ных систем и средств вычис□лительной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании

					защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.1.2. Знает требования основных стандартов по оценке защищенности	Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем	Знать: требования стандартов информа□ционной безопасности и руководящих до□кументы ФСТЭК России (Гостехкомиссии России по оценке защищенности компью□терных систем и сетей.

			компьютерных систем и сетей.		Уметь: составлять задание по безопасно сти и профиль защиты при создании за щищенных систем обработки информации; обосновывать требования к защищенным системам обработки информации и прово дить оценку эффективности их функцио нирования. Владеть: практическими навыками приме нения стандартов информационной без опасности при определении уровня ин формационной безопасности и соответ ствие профилю защиты; навыками исполь зования инструментальных интеллекту альных систем для обоснования требова ний и оценки защищенности систем обра ботки информации.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требо ваний и оценки защищенности систем обработки информа ции; порядок сертификации защищенных систем обра ботки информации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин формационных систем, ме тоды оценки рисков информа ционных систем, методы и средства проектирования тех нологически безопасного про граммного обеспечения; - источники угроз информаци онной безопасности в компью терных системах и сетях, ос новные виды уязвимостей ПО, принципы работы средств ста тического и динамического анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина мического анализа программ, методы проведения экспер тизы исходного кода; - принципы функционирова ния программных средств криптографической защиты информации. Уметь: - определять классы защи щенности автоматизирован ных систем и средств вычис лительной техники; обоснова вать требования к защищен ным системам обработки ин формации и проводить оценку эффективности их функциони рования; - составлять

					задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.1.3. Умеет определять уровень	Б1.О.55.03 Методы и стандарты оценки защищенности	Знать: требования стандартов информа□ционной безопасности (Единые критерии безопасности информационных техноло□гий).

			защищенности и доверия программно-аппаратных средств защиты информации.	компьютерных систем	Уметь; определять уровень защищенности и доверия программно-аппаратных средств защиты информации. Владеть: практическими навыками ис□ пользования инструментальных интеллек□ туальных систем для определения уровня защищенности и доверия программно□ аппаратных средств защиты информации
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требо□ ваний и оценки защищенности систем обработки информа□ ции; порядок сертификации защищенных систем обра□ ботки информации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - определять классы защи□ щенности автоматизирован□ ных систем и средств вычис□ лительной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных

					систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - практическими навыками применения стандартов ин□формационной безопасности при создании защищенных си□стем обработки информации; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.1.4. Умеет классифицировать информационные системы по требованиям защиты информации.	Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем	Знать: стандарты информационной без□опасности и руководящие документы ФСТЭК России (Гостехкомиссии России). Уметь; проводить классификацию инфор□мационные системы по требованиям за□щиты информации Владеть: практическими навыками клас□сификации автоматизированных систем, средств вычислительной техники, межсе□тевых экранов, средств антивирусной за□щиты, систем обнаружения вторжений по

					требованиям защиты информации.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требо□ваний и оценки защищенности систем обработки информа□ции; порядок сертификации защищенных систем обра□ботки информации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - определять классы защи□щенности автоматизирован□ных систем и средств вычис□лительной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический

					анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.1.5. Умеет определять угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе.	Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем	Знать: источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей информационных систем, формальные модели безопасности ком□ пьютерных систем, методы оценки рисков информационных систем Уметь; проводить классификацию уязви□ мостей информационных систем и моде□ лирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению Владеть: практическими навыками ис□ пользования инструментальных средств для моделирование угроз безопасности в компьютерных системах с учетом мер по их предотвращению.

				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требо ваний и оценки защищенности систем обработки информа ции; порядок сертификации защищенных систем обра ботки информации; - источники угроз информаци онной безопасности в компью терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин формационных систем, ме тоды оценки рисков информа ционных систем, методы и средства проектирования тех нологически безопасного про граммного обеспечения; - источники угроз информаци онной безопасности в компью терных системах и сетях, ос новные виды уязвимостей ПО, принципы работы средств ста тического и динамического анализа кода, методы устра нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина мического анализа программ, методы проведения экспер тизы исходного кода; - принципы функционирова ния программных средств криптографической защиты информации. Уметь: - определять классы защи щенности автоматизирован ных систем и средств вычис лительной техники; обосновы вать требования к защищен ным системам обработки ин формации и проводить оценку эффективности их функциони рования; - составлять задание по без опасности и профиль защиты при создании защищенных си стем обработки информации; обосновывать требования к защищенным системам обра ботки информации и прово дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион ных систем и моделирование угроз безопасности в компью терных системах с учетом мер по их предотвращению; - применять на практике полу ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис ходного кода, статический и динамический анализ, фай ззингтестирование); - применять на практике

					полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.1.6. Умеет выполнять анализ компьютерной системы с целью определения уровня защищенности и доверия.	Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем	знать: стандарты информационной без□ опасности и руководящие документы ФСТЭК России (Гостехкомиссии России), формальные модели безопасности, мето□ ды обоснования требований и оценки за□ щищенности систем обработки информа□ ции. уметь: определять классы защищенности автоматизированных систем и средств вы□ числительной техники; проводить анализ задания по безопасности и профиля защи□ ты при анализе защищенных систем обра□ ботки информации. владеть:. Владеть практическими навы□ ками применения стандартов информаци□ онной безопасности при анализе защи□ щенных систем обработки информации; навыками использования инструменталь□ ных интеллектуальных систем для анали□ за

					требований к защищенности компью□терных систем и оценки эффективности их функционирования
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требо□ваний и оценки защищенности систем обработки информа□ции; порядок сертификации защищенных систем обра□ботки информации; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - определять классы защи□щенности автоматизирован□ных систем и средств вычис□лительной техники; обосновы□вать требования к защищен□ным системам обработки ин□формации и проводить оценку эффективности их функциони□рования; - составлять задание по без□опасности и профиль защиты при создании защищенных си□стем обработки информации; обосновывать требования к защищенным системам обра□ботки информации и прово□дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей

					(экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.1.7. Умеет проводить теоретические исследования уровней защищенности и доверия компьютерных систем и сетей.	Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем	знать: этапы создания защищенных ком□ пьютерных систем и сетей; формальные модели безопасности компьютерных си□ стем; методы и средства проектирования технологически безопасного программного обеспечения; методы обоснования требо□ ваний и оценки защищенности систем об□ работки информации. уметь: проводить анализ формальных моделей безопасности; оценку требований к защищенным компьютерным системам и оценку эффективности их функционирова□ ния. владеть: практическими навыками ис□ пользования инструментальных интеллек□ туальных систем для оценки требований к защищенности компьютерных систем и эффективности их

					функционирования; практическими навыками использования CASE-средств при анализе проектных ре□ шений по обеспечению защищенности компьютерных систем.
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - стандарты информационной безопасности и руководящие документы ФСТЭК России (Гостехкомиссии России); - методы обоснования требо□ ваний и оценки защищенности систем обработки информа□ ции; порядок сертификации защищенных систем обра□ ботки информации; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - определять классы защи□ щенности автоматизирован□ ных систем и средств вычис□ лительной техники; обосновы□ вать требования к защищен□ ным системам обработки ин□ формации и проводить оценку эффективности их функциони□ рования; - составлять задание по без□ опасности и профиль защиты при создании защищенных си□ стем обработки информации; обосновывать требования к защищенным системам обра□ ботки информации и прово□ дить оценку эффективности их функционирования; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки

					работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - практическими навыками применения стандартов ин□ формационной безопасности при создании защищенных си□ стем обработки информации; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
	ОПК-1.2	Способен оценивать корректность программных реализаций алгоритмов защиты информации	ОПК-1.2.1. Знает основные средства и методы защиты программного обеспечения от анализа и нарушения целостности.	Б1.О.55.02 Алгоритмы кодирования и сжатия информации	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основные понятия и методы дискретной математики, кото□ рые используются для постро□ ения моделей и конструирова□ ния алгоритмов; - основные понятия, принципы и подходы к кодированию, пе□ редаче и обработке информа□ ции; - основные численные методы решения математических за□ дач, методы оценки и кон□ троля погрешностей; - источники угроз информаци□ онной безопасности в компью□ терных системах и

					сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - реализовывать методы дис□ кретной математики на ЭВМ; - переводить числа между различными системами счис□ ления; - рассчитывать степень избы□ точности кода и оценивать возможности его сжатия; - реализовывать численные методы на ЭВМ; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - методами построения пре□ фиксных кодов для оптималь□ ного кодирования данных; - навыками квалифицирован□ ного выбора и адаптации су□ ществующих методов прибли□ женного решения математиче□ ских задач; - разработки при□ кладных программ; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для

					моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками испо□льзова□ ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.2.2. Знает теоретические основы устранения избыточности данных.	Б1.О.55.02 Алгоритмы кодирования и сжатия информации	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основные понятия и методы дискретной математики, кото□рые используются для постро□ения моделей и конструирова□ ния алгоритмов; - основные понятия, принципы и подходы к кодированию, пе□редаче и обработке информа□ции; - основные численные методы решения математических за□дач, методы оценки и кон□троля погрешностей; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств

					криптографической защиты информации. Уметь: - реализовывать методы дис□кретной математики на ЭВМ; - переводить числа между различными системами счис□ления; - рассчитывать степень избы□точности кода и оценивать возможности его сжатия; - реализовывать численные методы на ЭВМ; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - методами построения пре□фиксных кодов для оптималь□ного кодирования данных; - навыками квалифицирован□ного выбора и адаптации су□ществующих методов прибли□женного решения математиче□ских задач, разработки при□кладных программ; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.

			ОПК-1.2.3. Знает основные алгоритмы кодирования данных и сжатия текстовой, графической, аудио- и видеоинформации.	Б1.О.55.02 Алгоритмы кодирования и сжатия информации	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основные понятия и методы дискретной математики, кото□рые используются для постро□ения моделей и конструирова□ния алгоритмов; - основные понятия, принципы и подходы к кодированию, пе□редаче и обработке информа□ции;- основные численные методы решения математических за□дач, методы оценки и кон□троля погрешностей; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - реализовывать методы дис□кретной математики на ЭВМ; - переводить числа между различными системами счис□ления; - рассчитывать степень избы□точности кода и оценивать возможности его сжатия; - реализовывать численные методы на ЭВМ; - проводить классификацию уязвимостей информацион□ных систем и моделирование угроз безопасности в компью□терных системах с учетом мер по их предотвращению; - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ,

					фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - методами построения пре□ фиксных кодов для оптималь□ ного кодирования данных; - навыками квалифицирован□ ного выбора и адаптации су□ ществующих методов прибли□ женного решения математиче□ ских задач, разработки при□ кладных программ; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.2.4. Умеет проводить анализ программ и алгоритмов сжатия данных на предмет соответствия требованиям защиты информации.	Б1.О.55.02 Алгоритмы кодирования и сжатия информации	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основные понятия и методы дискретной математики, кото□ рые используются для постро□ ения моделей и конструирова□ ния алгоритмов; - основные понятия, принципы и подходы к кодированию, пе□ редаче и обработке информа□ ции;- основные численные методы решения математических за□ дач, методы оценки и кон□ троля погрешностей; - источники угроз информаци□ онной безопасности в компью□ терных системах и

					сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - реализовывать методы дис□ кретной математики на ЭВМ; - переводить числа между различными системами счис□ ления; - рассчитывать степень избы□ точности кода и оценивать возможности его сжатия; - реализовывать численные методы на ЭВМ; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ зинг тестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - методами построения пре□ фиксных кодов для оптималь□ ного кодирования данных; - навыками квалифицирован□ ного выбора и адаптации су□ ществующих методов прибли□ женного решения математиче□ ских задач, разработки при□ кладных программ; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для

					моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
			ОПК-1.2.5. Умеет применять средства и методы анализа программных реализаций для поиска уязвимостей.	Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основные понятия и методы дискретной математики, кото□рые используются для постро□ения моделей и конструирова□ния алгоритмов; - основные понятия, принципы и подходы к кодированию, пе□редаче и обработке информа□ции; - основные численные методы решения математических за□дач, методы оценки и кон□троля погрешностей; - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода; - принципы функционирова□ния программных средств криптографической защиты информации. Уметь: - реализовывать методы дис□кретной математики на ЭВМ; - переводить числа

					между различными системами счис□ ления; - рассчитывать степень избы□ точности кода и оценивать возможности его сжатия; - реализовывать численные методы на ЭВМ; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - методами построения пре□ фиксных кодов для оптималь□ ного кодирования данных; - навыками квалифицирован□ ного выбора и адаптации су□ ществующих методов прибли□ женного решения математиче□ ских задач, разработки при□ кладных программ; - навыками использования ин□ струментальных интеллекту□ альных систем для обоснова□ ния требований и оценки за□ щищенности систем обра□ ботки информации; - практическими навыками ис□ пользования инструменталь□ ных средств для моделирова□ ния угроз безопасности в ком□ пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□ стей, навыками использова□ ния специализированных ути□ лит статического и динамиче□ ского анализа кода; - специализированными ин□ струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ ских библиотек) и тестирова□ ния специализированных ал□ горитмов и ПО, реализующих криптографические методы и алгоритмы.

			ОПК-1.2.6. Знает основные типы уязвимостей программного обеспечения.	Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - основные понятия и методы дискретной математики, кото□ рые используются для постро□ ения моделей и конструирова□ ния алгоритмов; - основные понятия, принципы и подходы к кодированию, пе□ редаче и обработке информа□ ции;- основные численные методы решения математических за□ дач, методы оценки и кон□ троля погрешностей; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□ формационных систем, ме□ тоды оценки рисков информа□ ционных систем, методы и средства проектирования тех□ нологически безопасного про□ граммного обеспечения; - источники угроз информаци□ онной безопасности в компью□ терных системах и сетях, ос□ новные виды уязвимостей ПО, принципы работы средств ста□ тического и динамического анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□ мического анализа программ, методы проведения экспер□ тизы исходного кода; - принципы функционирова□ ния программных средств криптографической защиты информации. Уметь: - реализовывать методы дис□ кретной математики на ЭВМ; - переводить числа между различными системами счис□ ления; - рассчитывать степень избы□ точности кода и оценивать возможности его сжатия; - реализовывать численные методы на ЭВМ; - проводить классификацию уязвимостей информацион□ ных систем и моделирование угроз безопасности в компью□ терных системах с учетом мер по их предотвращению; - применять на практике полу□ ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ ходного кода, статический и динамический анализ, фай□ ззингтестирование); - применять на практике полу□ ченные знания и навыки для анализа ПО на наличие уязви□ мостей. Владеть: - методами построения пре□ фиксных кодов для оптималь□ ного кодирования данных; - навыками

					квалифицирован□ного выбора и адаптации су□ществующих методов прибли□женного решения математиче□ских задач, разработки при□кладных программ; - навыками использования ин□струментальных интеллекту□альных систем для обоснова□ния требований и оценки за□щищенности систем обра□ботки информации; - практическими навыками ис□пользования инструменталь□ных средств для моделирова□ния угроз безопасности в ком□пьютерных системах с учетом мер по их предотвращению и проектирования технологиче□ски безопасного программного обеспечения; - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы.
	ОПК-1.3	Способен проводить тестирование и использовать средства верификации механизмов защиты информации	ОПК-1.3.1. Знает основные способы и средства верификации программ.	Б1.О.55.01 Методы верификации	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения

					экспер□тизы исходного кода Уметь: - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы
			ОПК-1.3.2. Знает основные способы тестирования средств защиты информации с использованием средств верификации программ.	Б1.О.55.01 Методы верификации	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамического анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода Уметь: - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные

					знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы
			ОПК-1.3.3. Умеет применять основные методы верификации программ и алгоритмов на предмет соответствия требованиям защиты информации.	Б1.О.55.01 Методы верификации	
				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Знать: - источники угроз информаци□онной безопасности в компью□терных системах и сетях и меры по их предотвращению, стандарты по классификации и описанию уязвимостей ин□формационных систем, ме□тоды оценки рисков информа□ционных систем, методы и средства проектирования тех□нологически безопасного про□граммного обеспечения; - источники угроз информаци□онной безопасности в компью□терных системах и сетях, ос□новные виды уязвимостей ПО, принципы работы средств ста□тического и динамическою анализа кода, методы устра□нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы статического и дина□мического анализа программ, методы проведения экспер□тизы исходного кода Уметь: - применять на практике полу□ченные знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза ис□ходного кода, статический и динамический анализ, фай□ззингтестирование); - применять на практике полу□ченные знания и навыки для анализа ПО на наличие уязви□мостей. Владеть: - практическими навыками анализа исходного кода на предмет наличия уязвимо□стей, навыками использова□ния специализированных ути□лит статического и динамиче□ского

					анализа кода; - специализированными ин□струментами и практическими навыками анализа ПО на наличие уязвимостей; - практическими навыками разработки, использования (известных криптографиче□ских библиотек) и тестирова□ния специализированных ал□горитмов и ПО, реализующих криптографические методы и алгоритмы

— профессиональные компетенции:

Тип задач профессиональной деятельности	Код	Формулировка компетенции	Код и формулировка индикатора достижения компетенции	Планируемые результаты освоения соответствующих дисциплин (модулей), практик[3]	
				Дисциплина	Результаты
	ПК-1	Способен проводить анализ требований к программному обеспечению, выполнять работы по проектированию программного обеспечения	ПК-1.1. Знает методы разработки программного обеспечения и технологии программирования.	Б2.В.01(П) Производственная практика (технологическая)	Знать: основные программные средства и технологии программирования, ис□пользуемые при формировании ком□плекса мер по обеспечению инфор□мационной безопасности предприя□тия (организации).
			ПК-1.2. Знает применяемые математические методы и алгоритмы функционирования для компонентов программных средств.	Б1.В.01 Стеганография и цифровые водяные знаки	Знать принципы защиты авторских прав на цифровые объекты интеллектуальной собственности с использованием технологий создания цифровых водяных знаков;
				Б1.В.02 Моделирование систем	
				Б1.В.03 Технологии защищенного документооборота и блокчейн	Знать: программные компоненты и особен□ности реализации электронной подписи и средств криптозащиты информации Уметь: проводить анализ безопасности компьютерных систем, использующих сред□ства электронной подписи Владеть: навыками построения и анализа безопасности информационных систем ис□пользующих электронную подпись

[3] Заполняются в соответствии с рабочими программами дисциплин (модулей), практик (без учета элективных и факультативных дисциплин (модулей))

				Б2.В.01(П) Производственная практика (технологическая)	Знать: - принципы формирования ком□плекса мер по обеспечению инфор□мационной безопасности предприя□тия (организации).
			ПК-1.3. Умеет применять технологии обработки данных, анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.	Б1.В.01 Стеганография и цифровые водяные знаки	Уметь применять на практике теоретические знания для реализации стеганографического скрытия информации в файлы распространенных форматов;
				Б1.В.02 Моделирование систем	
				Б1.В.03 Технологии защищенного документооборота и блокчейн	Знать: роль и особенности применения ме□тодов и средств криптозащиты информации в современных компьютерных системах Уметь: производить установку, наладку, те□стирование и обслуживание современных средств криптографической защиты инфор□мации Владеть: практическими навыками развер□тывания удостоверяющего центра для реа□лизации технологий с использованием ква□лифицированной электронной подписи
				Б2.В.01(П) Производственная практика (технологическая)	Уметь: - проводить синтез и анализ алго□ритмов обработки информации для решения конкретных практических задач, использовать математиче□ские методы в интересах аналитиче□ской и численной оценки основных показателей эффективности алго□ритмов анализа данных и машин□ного обучения; - проводить разработку простейших компьютерных моделей. Владеть: - методами выполнения типовых расчетов и моделирования процес□сов с применением компьютерной техники, проведение эксперимен□тальных исследований системы за□щиты информации; - практическими навыками разра□ботки и применения алгоритмов и технологий обработки информации в части анализа данных и машин□ного обучения.
	ПК-2	Способен проводить исследования на всех этапах жизненного	ПК-2.1. Знает методы и средства планирования и организации исследований и разработок.	Б1.В.02 Моделирование систем	
				Б1.В.04 Методология экспериментальных исследований и испытаний	Знать: базовые понятия теории эксперимента; основные принципы и приемы извлечения информации об объекте в процессе проведения эксперимента; базовые элементы методов

		цикла программных средств в профессиональной деятельности			планирования эксперимента. Уметь: формировать математическую модель объекта экспериментальных исследований с минимальным количеством переменных; формировать план эксперимента. Владеть практическими навыками: разработки математических моделей объекта эксперимента, планирования эксперимента, разработки рабочих методик эксперимента
				Б2.В.01(П) Производственная практика (технологическая)	Знать: - этапы разработки компьютерных моделей систем, применяемые при этом технологии структурно-функци□ онального и объектного визуального моделирования, технологии органи□ зации и проведения статистического компьютерного моделирования ком□ пьютерных систем.
			ПК-2.2. Знает методы проведения экспериментов и наблюдений, обобщения и обработки информации, полученной в ходе исследований.	Б1.В.02 Моделирование систем	
				Б1.В.04 Методология экспериментальных исследований и испытаний	Знать: основы методов обработки результатов эксперимента с позиций детерминистского и статистического подходов; основополагающие стандарты в области разработки отчетных документов. Уметь: выбирать технические средства экспериментальных исследований; проводить синтез алгоритмов формирования линейных, квазилинейных и нелинейных оценок измеряемых в ходе эксперимента значений физических величин, оптимальных в смысле заданного критерия; строить точечные и интервальные оценки результата эксперимента, представлять его в стандартном виде; проводить анализ результатов эксперимента с использованием методов линейного регрессионного и корреляционного анализа; Владеть практическими навыками: обработки и анализа результатов эксперимента; применения компьютерных технологий в экспериментальных исследованиях
				Б2.В.01(П) Производственная практика (технологическая)	Знать: - типовые математические схемы, используемые при построении мо□ делей элементов систем и их взаи□ модействия в виде блок-схем, струк□ турных схем и стандартных описа□ ний к ним, основные способы алго□ ритмизации математических моде□ лей систем, технологии организации и

					проведения имитационного экспе□ римента.
			ПК-2.3. Планирует стадии исследования или разработки в рамках поставленной задачи, выбирает или формирует программную среду для компьютерного моделирования и проведения экспериментов.	Б1.В.02 Моделирование систем	
				Б1.В.04 Методология экспериментальных исследований и испытаний	Знать: основные принципы и приемы извлечения информации об объекте в процессе проведения компьютерного эксперимента. Уметь: формировать математическую модель объекта компьютерного эксперимента; выбирать программную среду для проведения эксперимента и обработки его результатов; формировать план эксперимента, проводить его декомпозицию на отдельные этапы. Владеть практическими навыками: разработки математических моделей объекта, планирования компьютерного эксперимента.
				Б2.В.01(П) Производственная практика (технологическая)	Уметь: - использовать стандартное про□ граммное обеспечение для решения задач профессиональной деятель□ ности; - работать с измерительной аппара□ турой для контроля и изучения от□ дельных характеристик процессов, приборов, устройств, программного обеспечения информационных си□ стем для решения задач обеспече□ ния информационной безопасности
			ПК-2.4. Использует стандартное и оригинальное программное обеспечение, проводит компьютерный эксперимент, составляет его описание и формулирует выводы.	Б1.В.02 Моделирование систем	
				Б1.В.04 Методология экспериментальных исследований и испытаний	Владеть практическими навыками: использования стандартного и оригинального программного обеспечения для проведения и обработки данных компьютерного эксперимента, анализа и интерпретации результатов компьютерного эксперимента, их сопоставления с данными реального эксперимента и теоретическими выводами.
				Б2.В.01(П) Производственная практика (технологическая)	Уметь: - использовать стандартное про□ граммное обеспечение для решения задач профессиональной деятель□ ности. Владеть: - методами оценки информацион□ ных рисков; - основными методами алгоритмиза□ ции математических моделей си□ стем, технологиями организации и проведения имитационного экспери□ мента.

	ПК-3	Способен проводить анализ безопасности программных средств в компьютерных системах	ПК-3.1. Знает основные типы уязвимостей программного обеспечения и возможные пути их устранения.	Б1.В.05 Анализ уязвимостей программного обеспечения	Знает основные виды уязвимостей ПО, проводить анализ типы уязвимостей принципы работы средств статического и безопасности программного динамического анализа кода, методы программных средств в обеспечения и устранения уязвимостей. компьютерных системах возможные пути их Умеет применять на практике полученные устранения знания и навыки для проверки работоспособности ПО и его анализа на наличие уязвимостей (экспертиза исходного кода, статический и динамический анализ, файззинг□ тестирование). Владеет практическими навыками анализа исходного кода на предмет наличия уязвимостей, навыками использования специализированных утилит статического и динамического анализа кода.
				Б2.В.01(П) Производственная практика (технологическая)	Знать: - источники угроз информационной безопасности в компьютерных си□ стемах и сетях и меры по их предот□ вращению, стандарты по классифи□ кации и описанию уязвимостей ин□ формационных систем, методы оценки рисков информационных си□ стем, методы и средства проектиро□ вания технологически безопасного программного обеспечения; - источники угроз информационной безопасности в компьютерных си□ стемах и сетях, основные виды уяз□ вимостей ПО, принципы работы средств статического и динамиче□ ского анализа кода, методы устра□ нения уязвимостей; - известные методы анализа ПО на наличие уязвимостей, методы ста□ тического и динамического анализа программ, методы проведения экс□ пертизы исходного кода; - принципы функционирования про□ граммных средств криптографиче□ ской защиты информации.
			ПК-3.2. Знает современные технологии защиты электронного документооборота, технологии защиты объектов электронного контента от	Б1.В.01 Стеганография и цифровые водяные знаки	Знать основные теоретические и практические аспекты стеганографического скрытия информации; современные методы и средства защиты конфиденциальной информации, принципы организации скрытых каналов передачи информации, уязвимости современных алгоритмов компьютерной стеганографии; меры противодействия

			несанкционированного использования.		стеганографическому скрытию, принципы стегоанализа
				Б1.В.03 Технологии защищенного документооборота и блокчейн	Знать: требования нормативных докумен тов, методы анализа информационной без опасности при проектировании и эксплуата ции информационных систем при использо вании средств электронной подписи Уметь: анализировать и разрабатывать мо дели угроз для различных объектов защиты при использовании средств электронной подписи Владеть: практическими навыками форми рования требований безопасности инфор мации для различных классов и уровней за щищенности информационных систем
				Б2.В.01(П) Производственная практика (технологическая)	Знать - основные теоретические и практи ческие аспекты стеганографиче ского скрытия информации; - современные методы и средства защиты конфиденциальной инфор мации, принципы организации скры тых каналов передачи информации, принципы защиты авторских прав на цифровые объекты интеллектуаль ной собственности с использова нием технологий создания цифро вых водяных знаков; - методы и средства контроля эф фективности технической защиты информации.
			ПК-3.3. Умеет анализировать программные средства на наличия уязвимостей.	Б1.В.05 Анализ уязвимостей программного обеспечения	Знает известные методы анализа ПО на проводить анализ анализировать наличие уязвимостей, методы безопасности программные средства статического и динамического анализа программных средств в на наличия уязвимостей программ, методы проведения экспертизы компьютерных системах исходного кода. Умеет применять на практике полученные знания и навыки для анализа ПО на наличие уязвимостей. Владеет специализированными инструментами и практическими навыками анализа ПО на наличие уязвимостей.
				Б2.В.01(П) Производственная практика (технологическая)	Уметь: - проводить анализ стеганографиче ской стойкости и пропускной способ ности стеганографических каналов передачи информации для опти мального выбора контейнеров, алго ритмов стегоскрытия и алгоритмов создания цифровых водяных знаков

			ПК-3.4. Умеет анализировать возможности использования современных технологий защиты данных и объектов электронного контента.	Б1.В.01 Стеганография и цифровые водяные знаки	Уметь проводить анализ стеганографической стойкости и пропускной способности стеганографических каналов передачи информации для оптимального выбора контейнеров, алгоритмов стегоскрытия и алгоритмов создания цифровых водяных знаков.
				Б1.В.03 Технологии защищенного документооборота и блокчейн	Знать: базовые понятия, требования нор□ мативных документов, методы анализа ин□ формационной безопасности при проекти□ровании и эксплуатации информационных систем при использовании средств элек□ тронной подписи Уметь: анализировать и разрабатывать мо□ дели угроз для различных вариантов по□ строения защищенных информационных си□ стем при использовании электронной под□ писи Владеть: практическими навыками форми□ рования требований безопасности инфор□ мации для различных классов и уровней за□ щищенности информационных систем
				Б2.В.01(П) Производственная практика (технологическая)	Уметь: - проводить анализ стеганографиче□ ской стойкости и пропускной способ□ ности стеганографических каналов передачи информации для опти□ мального выбора контейнеров, алго□ ритмов стегоскрытия и алгоритмов создания цифровых водяных знаков.

В Приложении 10.1 приведен календарный график освоения элементов образовательной программы, в Приложении 10.2 – календарный график формирования компетенций.

На основе рабочих программ (фондов оценочных средств) дисциплин (модулей), практик, ГИА (ИА) образовательной программы сформированы комплексы заданий (включающие тестовые задания, расчетные задачи, ситуационные, практико-ориентированные задачи / мини-кейсы и темы для написания эссе для оценки сформированности компетенций у обучающегося. Задания фонда оценочных средств по образовательной программе размещены на Образовательном портале «Электронный университет ВГУ» *https://edu.vsu.ru/question/category.php?courseid=13780*

Критерии и шкалы оценивания:

Для оценивания выполнения заданий используется балльная шкала:

1) тестовые задания:

– средний уровень сложности (в формулировке задания перечислены все варианты ответа *(на Образовательном портале «Электронный университет ВГУ» реализованы с помощью вопросов следующих типов: множественный выбор, верно/неверно, на соответствие, все или ничего)*):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ, в том числе частично.

– повышенный уровень сложности (в формулировке задания отсутствуют варианты ответа *(на Образовательном портале «Электронный университет ВГУ» реализованы с помощью вопросов следующих типов: короткий ответ, числовой ответ)*):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ, в том числе частично.

2) расчетные задачи, ситуационные, практико-ориентированные задачи / мини-кейсы *(на Образовательном портале «Электронный университет ВГУ» реализованы с помощью вопросов типа эссе)*:

– средний уровень сложности:

- 5 баллов – задача решена верно (получен правильный ответ, обоснован (аргументирован) ход решения);
- 2 балла – решение задачи содержит незначительные ошибки, но приведен правильный ход рассуждений, или получен верный ответ, но отсутствует обоснование хода ее решения, или задача решена не полностью, но получены промежуточные результаты, отражающие правильность хода решения задачи, или, в случае если задание состоит из решения нескольких подзадач, 50% которых решены верно;
- 0 баллов – задача не решена или решение неверно (ход решения ошибочен или содержи грубые ошибки, значительно влияющие на дальнейшее изучение задачи).

– повышенный уровень сложности:

- 10 баллов – задача решена верно (получен правильный ответ, обоснован (аргументирован) ход решения);
- 5 баллов – решение задачи содержит незначительные ошибки, но приведен правильный ход рассуждений, или получен верный ответ, но отсутствует обоснование хода ее решения, или задача решена не полностью, но получены промежуточные результаты, отражающие правильность хода решения задачи;
- 0 баллов – задача не решена или решение неверно (ход решения ошибочен или содержи грубые ошибки, значительно влияющие на дальнейшее изучение задачи).

3) эссе *(на Образовательном портале «Электронный университет ВГУ» реализованы с помощью вопросов типа эссе)*:

- 10 баллов – содержание эссе соответствует заявленной теме, а также не менее 6 нижеуказанным показателям;

- 8 баллов – содержание эссе соответствует заявленной теме, а также не менее 4 нижеуказанным показателям, частично не менее 3 показателям;
- 5 баллов – содержание эссе соответствует заявленной теме, а также частично не менее 6 показателям;
- 2 балла – содержание эссе соответствует заявленной теме, а также частично не менее 4 показателям;
- 0 баллов – содержание эссе не соответствует заявленной теме или более чем 3 показателям.

Показатели оценивания:
- полнота раскрытия темы;
- наличие в работе позиции ее автора;
- аргументированность выдвинутого тезиса работы;
- четкость, логичность, смысловое единство изложения;
- обоснованность выводов;
- грамотность изложения:
- специализированный показатель.

Отметьте корректный перечень групп процессов управления проектом, выделяемых в стандарте PMBoK.

A) Планирование, Выполнение, Проверка, Воздействие

B) Инициация, Планирование, Исполнение, Мониторинг и контроль, Закрытие

C) Анализ, Проектирование, Кодирование, Тестирование, Эксплуатация и сопровождение

D) Начало проекта, Инициация проекта, Руководство проектом, Управление границей стадии, Контроль стадии, Управление поставкой продуктов, Закрытие проекта

ANSWER: B

Что из перечисленного характеризует итеративный ЖЦ проекта?

A) Разработка ведётся этапами-итерациями на основе получения регулярной обратной связи от заказчика, поставка готовых к использованию результатов осуществляется по итогам проведения всех итераций.

B) Разработка ведётся этапами-итерациями на основе получения регулярной обратной связи от заказчика, поставка готовых к использованию результатов осуществляется каждую итерацию.

C) Разработка ведётся поэтапно на основе продуманного на начальном этапе плана, поставка готовых к использованию результатов осуществляется на заключительном этапе.

ANSWER: A

Как называется организационная структура предприятия, основанная на принципе двойного подчинения исполнителей, когда сотрудник подчиняется руководителю своего отдела и руководителю проекта?

A) Матричная

B) Функциональная

C) Проектная

D) Горизонтальная

ANSWER: A

Два и больше взаимосвязанных проекта, нацеленных на достижение результата(-ов), которые невозможно достичь, организовав управление каждым проектом отдельно - это...

A) Портфель проектов

B) Область знания

C) Программа проектов
D) Группа процессов
ANSWER: C

Найдите угол между векторами \(\overline p = -5\overline a - 2 \overline b \) и \(\overline q = 3 \overline a + 7 \overline b \), если \(\overline a \) и \(\overline b \) взаимно перпендикулярные орты.
A) π/6
B) π/4
C) π/3
D) 3π/4
ANSWER: D

В декартовой прямоугольной системе координат на плоскости заданы координаты точки _M_(4,1) и уравнение прямой _L_ \(4x - y + 3 = 0. \) Найдите уравнение прямой, проходящей через точку _M_ перпендикулярно прямой _L_.
A) \(y = x-3 \)
B) \(x-2y+9=0 \)
C) \(x+4y-8=0 \)
D) \(2x - 3y = 0 \)
ANSWER: C

Каноническое уравнение гиперболы, у которой действительная полуось a = 4, а мнимая полуось b = 3, в декартовой прямоугольной системе координат имеет вид
A) \(\frac{x}{4} - \frac{y}{3} = 1 \)
B) \(\frac{x^2}{4} + \frac{y^2}{3} = 1 \)
C) \(\frac{x^2}{16} + \frac{y^2}{9} = 1 \)
D) \(\frac{x^2}{16} - \frac{y^2}{9} = 1 \)
ANSWER: D

Какие из точек \(A(2; \sqrt[]{3}) \), \(B(0;1) \), \(C(- \frac{2}{ \sqrt[]{3}} ;\frac{2} { \sqrt[]{3}}) \) лежат на гиперболе \(x^{2}-y^{2}=1 \) \(? \)
A) A
B) B
C) C
ANSWER: A

Какие из прямых \((AB):x-y=0, (BC):2x+5y-3=0 \) и \((AC):2x+2y+3=0 \) перпендикулярны?
A) (AB) и (BC)
B) (AB) и (AC)
C) (BC) и (AC)
ANSWER: B

Какие из векторов \(\overrightarrow{a}(1,0,0), \overrightarrow{b}(1,-3,1) \) и \(\overrightarrow{c}(0,3,5) \) перпендикулярны?
A) \(\overrightarrow{a}\) и \(\overrightarrow{c}\)
B) \(\overrightarrow{a}\) и \(\overrightarrow{b}\)
C) \(\overrightarrow{b}\) и \(\overrightarrow{c}\)
ANSWER: A

Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на гиперболе \(x^{2}- \frac{y^{2}}{3} =1 ?\)
A) A
B) B
C) C
ANSWER: A

Даны уравнения сторон треугольника \((AB):5x-3y-15=0, (BC):x+5y-3=0, \; и \; (AC):3x+y+5=0. \) Найти координаты точки A.
A) (0,-5)

B) (0,5)
C) (5,0)
ANSWER: A
Определить угловой коэффициент прямой \(y = -3x-5. \)
A) -3
B) 3
C) 4
ANSWER: A
Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на эллипсе \(x^{2} + y^{2}=1 ? \)
A) A
B) B
C) C
ANSWER: B
Чему равен косинус угла между векторами \(\overrightarrow{a}=(1,2,-3) \) и \(\overrightarrow{b} = (2, -3, 1)? \)
A) 1
B) 0.5
C) -0.5
ANSWER: C
Чему равен угол между векторами \(\overrightarrow{a}=(1,0,0) \) и \(\overrightarrow{b}=(0,-3,1)? \)
A) \(90^{\circ } \)
B) \(0^{\circ } \)
C) \(60^{\circ } \)
ANSWER: A
Какие из прямых \((AB):x-y=0, (BC):2x+5y-3=0 \) и \((AC):2x-2y+3=0 \) параллельны?
A) (AB) и (BC)
B) (AB) и (AC)
C) (BC) и (AC)
ANSWER: B
Найдите угол между векторами \(\overline p = -5\overline a - 2 \overline b \) и \(\overline q = 3 \overline a + 7 \overline b \), если \(\overline a \) и \(\overline b \) взаимно перпендикулярные орты.
A) π/6
B) π/4
C) π/3
D) 3π/4
ANSWER: D
В декартовой прямоугольной системе координат на плоскости заданы координаты точки _M_(4,1) и уравнение прямой _L_ \(4x - y + 3 = 0. \) Найдите уравнение прямой, проходящей через точку _M_ перпендикулярно прямой _L_.
A) \(y = x-3 \)
B) \(x-2y+9=0 \)
C) \(x+4y-8=0 \)
D) \(2x - 3y = 0 \)
ANSWER: C
Каноническое уравнение гиперболы, у которой действительная полуось a = 4, а мнимая полуось b = 3, в декартовой прямоугольной системе координат имеет вид
A) \(\frac{x}{4} - \frac{y}{3} = 1 \)
B) \(\frac{x^2}{4} + \frac{y^2}{3} = 1 \)
C) \(\frac{x^2}{16} + \frac{y^2}{9} = 1 \)

D) \(\frac{x^2}{16} - \frac{y^2}{9} = 1 \)
ANSWER: D
Какие из точек \(A(2; \sqrt[]{3}) \), \(B(0;1) \), \(C(- \frac{2}{ \sqrt[]{3}} ;\frac{2} { \sqrt[]{3}}) \) лежат на гиперболе \(x^{2}-y^{2}=1 \) \(? \)
A) A
B) B
C) C
ANSWER: A
Какие из прямых \((AB):x-y=0, (BC):2x+5y-3=0 \) и \((AC):2x+2y+3=0 \) перпендикулярны?
A) (AB) и (BC)
B) (AB) и (AC)
C) (BC) и (AC)
ANSWER: B
Какие из векторов \(\overrightarrow{a}(1,0,0), \overrightarrow{b}(1,-3,1) \) и \(\overrightarrow{c}(0,3,5) \) перпендикулярны?
A) \(\overrightarrow{a}\) и \(\overrightarrow{c}\)
B) \(\overrightarrow{a}\) и \(\overrightarrow{b}\)
C) \(\overrightarrow{b}\) и \(\overrightarrow{c}\)
ANSWER: A
Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на гиперболе \(x^{2}- \frac{y^{2}}{3} =1 ?\)
A) A
B) B
C) C
ANSWER: A
Даны уравнения сторон треугольника \((AB):5x-3y-15=0, (BC):x+5y-3=0, \; и \; (AC):3x+y+5=0. \) Найти координаты точки A.
A) (0,-5)
B) (0,5)
C) (5,0)
ANSWER: A
Определить угловой коэффициент прямой \(y = -3x-5. \)
A) -3
B) 3
C) 4
ANSWER: A
Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на эллипсе \(x^{2} + y^{2}=1 ? \)
A) A
B) B
C) C
ANSWER: B
Чему равен косинус угла между векторами \(\overrightarrow{a}=(1,2,-3) \) и \(\overrightarrow{b} = (2, -3, 1)? \)
A) 1
B) 0.5
C) -0.5
ANSWER: C
Найдите угол между векторами \(\overline p = -5\overline a - 2 \overline b \) и \(\overline q = 3 \overline a + 7 \overline b \), если \(\overline a \) и \(\overline b \) взаимно перпендикулярные орты.
A) π/6
B) π/4

C) π/3
D) 3π/4
ANSWER: D
Чему равен угол между векторами \(\overrightarrow{a}=(1,0,0) \) и \(\overrightarrow{b}=(0,-3,1)? \)
A) \(90^{\circ } \)
B) \(0^{\circ } \)
C) \(60^{\circ } \)
ANSWER: A
В декартовой прямоугольной системе координат на плоскости заданы координаты точки _M_(4,1) и уравнение прямой _L_ \(4x - y + 3 = 0. \) Найдите уравнение прямой, проходящей через точку _M_ перпендикулярно прямой _L_.
A) \(y = x-3 \)
B) \(x-2y+9=0 \)
C) \(x+4y-8=0 \)
D) \(2x - 3y = 0 \)
ANSWER: C
Какие из прямых \((AB):x-y=0, (BC):2x+5y-3=0 \) и \((AC):2x-2y+3=0 \) параллельны?
A) (AB) и (BC)
B) (AB) и (AC)
C) (BC) и (AC)
ANSWER: B
Каноническое уравнение гиперболы, у которой действительная полуось a = 4, а мнимая полуось b = 3, в декартовой прямоугольной системе координат имеет вид
A) \(\frac{x}{4} - \frac{y}{3} = 1 \)
B) \(\frac{x^2}{4} + \frac{y^2}{3} = 1 \)
C) \(\frac{x^2}{16} + \frac{y^2}{9} = 1 \)
D) \(\frac{x^2}{16} - \frac{y^2}{9} = 1 \)
ANSWER: D
Какие из точек \(A(2; \sqrt[]{3}) \), \(B(0;1) \), \(C(- \frac{2}{ \sqrt[]{3}} ;\frac{2} { \sqrt[]{3}}) \) лежат на гиперболе \(x^{2}-y^{2}=1 \) \(? \)
A) A
B) B
C) C
ANSWER: A
Какие из прямых \((AB):x-y=0, (BC):2x+5y-3=0 \) и \((AC):2x+2y+3=0 \) перпендикулярны?
A) (AB) и (BC)
B) (AB) и (AC)
C) (BC) и (AC)
ANSWER: B
Какие из векторов \(\overrightarrow{a}(1,0,0), \overrightarrow{b}(1,-3,1) \) и \(\overrightarrow{c}(0,3,5) \) перпендикулярны?
A) \(\overrightarrow{a}\) и \(\overrightarrow{c}\)
B) \(\overrightarrow{a}\) и \(\overrightarrow{b}\)
C) \(\overrightarrow{b}\) и \(\overrightarrow{c}\)
ANSWER: A
Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на гиперболе \(x^{2}- \frac{y^{2}}{3} =1 ?\)
A) A
B) B
C) C

ANSWER: A

Даны уравнения сторон треугольника \((AB):5x-3y-15=0, (BC):x+5y-3=0, \; и \; (AC):3x+y+5=0. \) Найти координаты точки A.

A) (0,-5)

B) (0,5)

C) (5,0)

ANSWER: A

Определить угловой коэффициент прямой \(y = -3x-5. \)

A) -3

B) 3

C) 4

ANSWER: A

Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на эллипсе \(x^{2} + y^{2}=1 ? \)

A) A

B) B

C) C

ANSWER: B

Чему равен косинус угла между векторами \(\overrightarrow{a}=(1,2,-3) \) и \(\overrightarrow{b} = (2, -3, 1)? \)

A) 1

B) 0.5

C) -0.5

ANSWER: C

Чему равен угол между векторами \(\overrightarrow{a}=(1,0,0) \) и \(\overrightarrow{b}=(0,-3,1)? \)

A) \(90^{\circ } \)

B) \(0^{\circ } \)

C) \(60^{\circ } \)

ANSWER: A

Какие из прямых \((AB):x-y=0, (BC):2x+5y-3=0 \) и \((AC):2x-2y+3=0 \) параллельны?

A) (AB) и (BC)

B) (AB) и (AC)

C) (BC) и (AC)

ANSWER: B

Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на параболе \(y^{2}=x+1 ? \)

A) A

B) B

C) C

ANSWER: B

Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на параболе \(y^{2}=x+1 ? \)

A) A

B) B

C) C

ANSWER: B

Какие из точек \(A(-\frac{2}{ \sqrt[]{3} } ; 1), B(0;-1), C(\frac{2}{ \sqrt[]{3} }, \frac{2}{ \sqrt[]{3} }) \) лежат на параболе \(y^{2}=x+1 ? \)

A) A

B) B

C) C

ANSWER: B

Разложите дробь \(\frac{4x^2 + 2}{x^3 + x} \) на сумму простейших дробей над полем _R._

A) \(\frac{4}{x^2+1} + \frac{2}{x^3+x} \)

B) \(\frac{2}{x} + \frac{2x}{x^2+1} \)

C) \(\frac{2}{x} + \frac{2}{x^2+1} \)

D) \(\frac{2}{x} + \frac{1}{x+1} + \frac{1}{x-1} \)

ANSWER: B

В пространстве _R3_ 1) для любых векторов _x = (x1, x2, x3), y = (y1, y2, y3) _задано скалярное произведение _(x, y) = x1y1 + x2y2 + x3y3_, 2) заданы четыре вектора _e = (1, 1, 3), f = (2, 1, -1), g = (-1, 2, 0), h = (4, -7, 1)._ Среди векторов _e, f, g, h_ найдите ортогональный базис пространства.

A) _e, f, g_

B) _e, f, h_

C) _e, g, h_

D) _f, g, h_

ANSWER: B

Чему равно произведение матриц \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \) и \(B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \) ?

A) \(\begin{pmatrix} -1 & 4 \\ -1 & 8 \end{pmatrix} \)

B) \(\begin{pmatrix} -1 & 4 \\ -1 & 5 \end{pmatrix} \)

C) \(\begin{pmatrix} 0 & 4 \\ -1 & 8 \end{pmatrix} \)

ANSWER: A

Чему равно сумма матриц \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \) и \(B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \) ?

A) \(\begin{pmatrix} 2 & 2 \\ 2 & 8 \end{pmatrix} \)

B) \(\begin{pmatrix} 2 & 2 \\ 2 & 6 \end{pmatrix} \)

C) \(\begin{pmatrix} 0 & 4 \\ -1 & 8 \end{pmatrix} \)

ANSWER: B

Чему равен определитель матрицы \(\begin{vmatrix} 1 & 2 & 4\\ 0 & 1 & 1\\ 0 & 2 & 8 \end{vmatrix} \) ?

A) 6

B) 1

C) 5

ANSWER: A

Чему равен определитель матрицы \(\begin{vmatrix} 1 & 0 & -5\\ 0 & 1 & 3\\ 0 & 2 & 8 \end{vmatrix} \) ?

A) 2

B) 1

C) 5

ANSWER: A

Найти матрицу, обратную матрице \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}. \)

A) \(A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

B) \(A^{-1} = \begin{pmatrix} -1 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

C) \(A^{-1} = \begin{pmatrix} -2 & 1 \\ - \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

ANSWER: A

Для матрицы \(\begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix} \) найдите обратную матрицу.

A) \(\begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \)

B) \(\begin{pmatrix} 1/2 & 1 \\ 1/4 & 1/3 \end{pmatrix} \)

C) \(\begin{pmatrix} 3 & -4 \\ -1 & 2 \end{pmatrix} \)

D) \(\begin{pmatrix} 3/2 & -2 \\ -1/2 & 1 \end{pmatrix} \)

ANSWER: D

Разложите дробь \(\frac{4x^2 + 2}{x^3 + x} \) на сумму простейших дробей над полем _R._

A) \(\frac{4}{x^2+1} + \frac{2}{x^3+x} \)

B) \(\frac{2}{x} + \frac{2x}{x^2+1} \)

C) \(\frac{2}{x} + \frac{2}{x^2+1} \)

D) \(\frac{2}{x} + \frac{1}{x+1} + \frac{1}{x-1} \)

ANSWER: B

В пространстве _R3_ 1) для любых векторов _x = (x1, x2, x3), y = (y1, y2, y3) _задано скалярное произведение _(x, y) = x1y1 + x2y2 + x3y3_, 2) заданы четыре вектора _e = (1, 1, 3), f = (2, 1, -1), g = (-1, 2, 0), h = (4, -7, 1)._ Среди векторов _e, f, g, h_ найдите ортогональный базис пространства.

A) _e, f, g_

B) _e, f, h_

C) _e, g, h_

D) _f, g, h_

ANSWER: B

Чему равно произведение матриц \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \) и \(B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \) ?

A) \(\begin{pmatrix} -1 & 4 \\ -1 & 8 \end{pmatrix} \)

B) \(\begin{pmatrix} -1 & 4 \\ -1 & 5 \end{pmatrix} \)

C) \(\begin{pmatrix} 0 & 4 \\ -1 & 8 \end{pmatrix} \)

ANSWER: A

Чему равно сумма матриц \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \) и \(B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \) ?

A) \(\begin{pmatrix} 2 & 2 \\ 2 & 8 \end{pmatrix} \)

B) \(\begin{pmatrix} 2 & 2 \\ 2 & 6 \end{pmatrix} \)

C) \(\begin{pmatrix} 0 & 4 \\ -1 & 8 \end{pmatrix} \)

ANSWER: B

Чему равен определитель матрицы \(\begin{vmatrix} 1 & 2 & 4\\ 0 & 1 & 1\\ 0 & 2 & 8 \end{vmatrix} \) ?

A) 6

B) 1

C) 5

ANSWER: A

Чему равен определитель матрицы \(\begin{vmatrix} 1 & 0 & -5\\ 0 & 1 & 3\\ 0 & 2 & 8 \end{vmatrix} \) ?

A) 2

B) 1

C) 5

ANSWER: A

Найти матрицу, обратную матрице \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}. \)

A) \(A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

B) \(A^{-1} = \begin{pmatrix} -1 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

C) \(A^{-1} = \begin{pmatrix} -2 & 1 \\ - \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

ANSWER: A

Для матрицы \(\begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix} \) найдите обратную матрицу.

A) \(\begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \)

B) \(\begin{pmatrix} 1/2 & 1 \\ 1/4 & 1/3 \end{pmatrix} \)

C) \(\begin{pmatrix} 3 & -4 \\ -1 & 2 \end{pmatrix} \)

D) \(\begin{pmatrix} 3/2 & -2 \\ -1/2 & 1 \end{pmatrix} \)

ANSWER: D

Разложите дробь \(\frac{4x^2 + 2}{x^3 + x} \) на сумму простейших дробей над полем _R._

A) \(\frac{4}{x^2+1} + \frac{2}{x^3+x} \)

B) \(\frac{2}{x} + \frac{2x}{x^2+1} \)

C) \(\frac{2}{x} + \frac{2}{x^2+1} \)

D) \(\frac{2}{x} + \frac{1}{x+1} + \frac{1}{x-1} \)

ANSWER: B

В пространстве _R3_ 1) для любых векторов _x = (x1, x2, x3), y = (y1, y2, y3) _задано скалярное произведение _(x, y) = x1y1 + x2y2 + x3y3_, 2) заданы четыре вектора _e = (1, 1, 3), f = (2, 1, -1), g = (-1, 2, 0), h = (4, -7, 1)._ Среди векторов _e, f, g, h_ найдите ортогональный базис пространства.

A) _e, f, g_

B) _e, f, h_

C) _e, g, h_

D) _f, g, h_

ANSWER: B

Чему равно произведение матриц \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \) и \(B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \) ?

A) \(\begin{pmatrix} -1 & 4 \\ -1 & 8 \end{pmatrix} \)

B) \(\begin{pmatrix} -1 & 4 \\ -1 & 5 \end{pmatrix} \)

C) \(\begin{pmatrix} 0 & 4 \\ -1 & 8 \end{pmatrix} \)

ANSWER: A

Чему равно сумма матриц \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \) и \(B = \begin{pmatrix} 1 & 0 \\ -1 & 2 \end{pmatrix} \) ?

A) \(\begin{pmatrix} 2 & 2 \\ 2 & 8 \end{pmatrix} \)

B) \(\begin{pmatrix} 2 & 2 \\ 2 & 6 \end{pmatrix} \)

C) \(\begin{pmatrix} 0 & 4 \\ -1 & 8 \end{pmatrix} \)

ANSWER: B

Чему равен определитель матрицы \(\begin{vmatrix} 1 & 2 & 4\\ 0 & 1 & 1\\ 0 & 2 & 8 \end{vmatrix} \) ?

A) 6

B) 1

C) 5

ANSWER: A

Чему равен определитель матрицы \(\begin{vmatrix} 1 & 0 & -5\\ 0 & 1 & 3\\ 0 & 2 & 8 \end{vmatrix} \) ?

A) 2

B) 1

C) 5

ANSWER: A

Найти матрицу, обратную матрице \(A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}. \)

A) \(A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

B) \(A^{-1} = \begin{pmatrix} -1 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

C) \(A^{-1} = \begin{pmatrix} -2 & 1 \\ - \frac{3}{2} & -\frac{1}{2} \end{pmatrix} \)

ANSWER: A

Для матрицы \(\begin{pmatrix} 2 & 4 \\ 1 & 3 \end{pmatrix} \) найдите обратную матрицу.

A) \(\begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix} \)

B) \(\begin{pmatrix} 1/2 & 1 \\ 1/4 & 1/3 \end{pmatrix} \)

C) \(\begin{pmatrix} 3 & -4 \\ -1 & 2 \end{pmatrix} \)

D) \(\begin{pmatrix} 3/2 & -2 \\ -1/2 & 1 \end{pmatrix} \)

ANSWER: D

Выберите верный ответДля того, чтобы возрастающая числовая последовательность сходилась, необходимо и достаточно, чтобы она была … .

A) ограниченным сверху
B) конечна
C) монотонна
D) ограничена снизу
ANSWER: A

Выберите верный ответФункция \(\alpha (x) \) имеет в точке a более высокий порядок малости, чем функция \(\beta (x) \), если

A) \(lim_{x \rightarrow a} \frac{ \alpha (x)}{ \beta (x) } =0 \)
B) \(lim_{x \rightarrow a} \frac{ \beta (x)}{ \alpha (x) } =0 \)
C) \(lim_{x \rightarrow a} \frac{ \alpha (x)}{ \beta (x) } =1 \)
D) \(lim_{x \rightarrow a} \frac{ \beta (x)}{ \alpha (x) } =5 \)
ANSWER: A

Выберите верный ответ\(lim_{x \rightarrow 0} \frac{sin(x)}{x} = ... \) .

A) 1
B) 0
C) не существует
D) \(\pi \)
ANSWER: A

Выберите верный ответФункция f(x) называется непрерывной в точке a, если для любой сходящейся к пределу a последовательности \(\lbrace{x_{n}}\rbrace \) значений ее аргументов соответствующая последовательность значений функции \(\lbrace{f(x_{n})}\rbrace \) сходится к ... .

A) f(a)
B) 0
C) a
D) f(0)
ANSWER: A

Выберите верный ответФункция f(x) называется ... на множестве X, если \(\forall (x_{1} , x_{2} \in X : x_{1} < x_{2}) [f(x_{1}) < f(x_{2})] \)

A) ограниченной сверху
B) возрастающей
C) сходящейся
D) непрерывной
ANSWER: B

Выберите верный ответПусть функция f имеет производную в точке \(x_{0} \), а функция g имеет производную в точке \(y_{0}=f(x_{0}) \). Тогда существует \((g(f(x_{0})))' \) и \((g(f(x_{0})))'= \)... .

A) \(g'(f(x_{0})) \cdot f'(x_{0}) \)
B) \(\frac{g'(f(x_{0}))}{ f'(x_{0})} \)
C) \(g'(f(x_{0})) \cdot f(x_{0}) \)
D) \(g'(f(x_{0})) + f'(x_{0}) \)
ANSWER: A

Выберите верный ответФункция f(x) называется ... на множестве X, если \(\exists (M \in \mathbb{R}) \forall (x \in X) [f(x) \leq M] \)

A) ограниченной сверху
B) сходящейся
C) монотонной
D) непрерывной
ANSWER: A

Выберите верный ответЕсли F(x) - первообразная функции f(x) на промежутке X, то функция ..., где C - произвольная постоянная, также является первообразной функции f(x) на промежутке X.

A) \(F(x)+C \)

B) \(F(x) \cdot C \)

C) \(\frac{F(x)}{C} \)

D) \(\frac{C}{F(x)} \)

ANSWER: A

Выберите верный ответОперация нахождения неопределенного интеграла называется ... .

A) интегрированием

B) аппроксимацией

C) дифференцированием

D) интегрализацией

ANSWER: A

Выберите правильный вариант ответа:Пусть функция \(f (x) \) определена на отрезке \([a;b] \) \((a<b) \). Рассмотрим разбиение \((T, \xi) \) этого отрезка с отмеченными точками (\(T= \lbrace{x_{0}, x_{1}, x_{2}, ... , x_{n-1}, x_{n}\rbrace } \) такое, что \(a=x_{0}<x_{1}<x_{2}<...< x_{n-1}<x_{n}=b , \Delta x_{i}=x_{i} - x_{i-1}, i=1,2, ... , n \)) и соответствующую интегральную сумму Римана функции \(f (x) \) \(S (f, (T, \xi)) = \sum _{i=1}^{n}{f (\xi _{i}) \Delta x_{i} } \) .Функция \(f (x) \), определенная на отрезке \([a;b] \), называется интегрируемой по Риману на \([a;b] \), если

A) \(\exists (J) \forall (\epsilon >0) \exists (\delta >0) \forall ((T, \xi): d(T)< \delta) [\left| S(f,(T, \xi))-J \right| < \epsilon] \)

B) \(\exists (c \in (a;b)) \exists (J) \forall (\epsilon >0) \exists (\delta >0) \forall (x: 0<\left| x-c \right| < \delta) [\left| f(x)-J \right| < \epsilon] \)

C) \(\forall (J) \exists (\epsilon >0) \forall (\delta >0) \exists ((T, \xi): d(T)< \delta) [\left| S(f,(T, \xi))-J \right| < \epsilon] \)

D) \(\forall (c \in (a;b)) \forall (J) \exists (\epsilon >0) \forall (\delta >0) \exists (x: \left| x-c \right| < \delta) [\left| f(x)-J \right| < \epsilon] \)

ANSWER: A

Выберите правильный вариант ответа:Если функция \(f(x) \) интегрируема на \([a;b] \) по Риману, то она ... на \([a;b] \) .

A) сохраняет свой знак

B) монотонна

C) дифференцируема

D) ограничена

ANSWER: D

Выберите правильный вариант ответа:Теорема о среднем значении. Пусть функции \(f(x) \) и \(\phi (x) \) определены и интегрируемы на отрезке \([a;b] \), на котором функция \(\phi (x) \) ... . Тогда при некотором \(\mu \in [m;M] \), где \(m=inf_{x \in [a;b]} f(x) \), \(M=sup_{x \in [a;b]} f(x) \), имеет место равенство \(\int_{a}^{b}{(\phi f)(x) dx} = \mu \int_{a}^{b}{g(x) dx} \) .

A) сохраняет свой знак

B) монотонна

C) дифференцируема

D) ограничена

ANSWER: A

Выберите правильный ответ:Непрерывную функцию \(F(x) \) называют ... на отрезке \([a;b] \), если функция \(F(x) \) имеет во всех точках отрезка \([a;b] \), за исключением конечного множества \(X \subset [a;b] \), производную, причем в этих точках \(F'(x)=f(x) \)

A) обобщенной первообразной функции \(f(x) \)

B) монотонной
C) интегрируемой
D) квадрируемой
ANSWER: A

Выберите правильный вариант ответа:Пусть функции \(u(x) \) и \(v(x) \) непрерывны и дифференцируемы на отрезке \([a;b] \), то справедливо равенство ...
A) \(\int_{a}^{b}{u(x) v'(x)dx} = (u(x) v(x)) |_{a}^{b} - \int_{a}^{b}{u'(x) v(x)dx} \)
B) \(\int_{a}^{b}{u(x) v'(x)dx} = (u(x) v(x)) |_{a}^{b} - \int_{a}^{b}{u(x) v'(x)dx} \)
C) \(\int_{a}^{b}{u'(x) v'(x)dx} = (u(x) v(x)) |_{a}^{b} + \int_{a}^{b}{u(x) v(x)dx} \)
D) \(\int_{a}^{b}{u(x) v(x)dx} = - (u(x) v(x)) |_{a}^{b} + \int_{a}^{b}{u'(x) v'(x)dx} \)
E) \(\int_{a}^{b}{u(x) v'(x)dx} = (u'(x) v(x)) |_{a}^{b} - \int_{a}^{b}{u'(x) v(x)dx} \)
F) \(\int_{a}^{b}{u(x) v'(x)dx} = (u(x) v'(x)) |_{a}^{b} + \int_{a}^{b}{u'(x) v(x)dx} \)
ANSWER: A

Выбрать правильный вариант ответа:Если кривая, задаваемая уравнением \(y=f(x) \) при \(x \in [a;b] \), является гладкой, то она спрямляема и ее длина \(l \) определяется равенством
A) \(l= \int_{a}^{b}{ \sqrt{1+(f'(x))^{2}}dx } \)
B) \(l= \int_{a}^{b}{f(x)dx} \)
C) \(l= \pi \int_{a}^{b}{f^{2} (x)dx} \)
D) \(l= \int_{0}^{2 \pi }{f'(x)dx} \)
ANSWER: A

Выбрать правильный вариант ответа:Если функция \(f(x) \) неотрицательна на \([a;b) \), то для сходимости несобственного интеграла \(\int_{a}^{b}{f(x)dx} \) необходимо и достаточно, чтобы все интегралы \(\int_{a}^{c}{f(x)dx} \), \(a \leq c <b \), были ... .
A) ограниченными по совокупности
B) монотонными на \([a;b] \)
C) определены
D) интегрируемы
ANSWER: A

Выберите правильный вариант ответа:Если \(f(x) \leq g(x) \) для всех \(x \in [a;b) \), то говорят, что функция \(g(x) \) ... функцию \(f(x) \) .
A) мажорирует
B) определяет
C) дифференцирует
D) квадрирует
ANSWER: A

Выберите правильный вариант ответа (знак):Пусть \(\sum_{k=1}^{ \infty }{p_{k}} \) и \(\sum_{k=1}^{ \infty }{p'_{k}} \) - два ряда с неотрицательными членами, и пусть для всех номеров \(k \) справедливо: \(p_{k} ... p'_{k} \). Тогда сходимость ряда \(\sum_{k=1}^{ \infty }{p'_{k}} \) влечет за собой сходимость ряда \(\sum_{k=1}^{ \infty }{p_{k}} \), а расходимость ряда \(\sum_{k=1}^{ \infty }{p_{k}} \) влечет за собой расходимость ряда \(\sum_{k=1}^{ \infty }{p'_{k}} \)
A) \(\leq \)
B) \(\geq \)
C) \(= \)
D) \(< \)
E) \(> \)
ANSWER: A

Выберите правильный вариант ответа (знак):Пусть \(\sum_{k=1}^{ \infty }{p_{k}} \) и \(\sum_{k=1}^{ \infty }{p'_{k}} \) - два ряда со строго положительными членами, и пусть для всех номеров \(k \) справедливо: \(\dfrac{p_{k+1}}{p_{k}} ... \dfrac{p'_{k+1}}{p'_{k}} \). Тогда сходимость ряда \(\sum_{k=1}^{ \infty }{p'_{k}} \) влечет за собой сходимость ряда \(\sum_{k=1}^{ \infty }{p_{k}} \), а расходимость ряда \(\sum_{k=1}^{ \infty }{p_{k}} \) влечет за собой расходимость ряда \(\sum_{k=1}^{ \infty }{p'_{k}} \)

A) \(\leq \)

B) \(\geq \)

C) \(= \)

D) \(< \)

E) \(> \)

ANSWER: A

Выберите верный ответЕсли выполнено утверждение\(\exists (m \in \mathbb {R}) \forall (x \in X) [x \geq m] \)множество X является

A) ограниченным снизу

B) конечным

C) монотонным

D) полным

ANSWER: A

Выберите правильный вариант ответа:Ряд \(\sum_{k=1}^{ \infty }{u_{k}} \) называется абсолютно сходящимся, если сходится ряд ... .

A) \(\sum_{k=1}^{ \infty }{\left| u_{k} \right| } \)

B) \(\sum_{k=1}^{ \infty }{(-u_{k})^{k}} \)

C) \(\sum_{k=1}^{ \infty }{(-1)^{u_{k}}} \)

D) \(\sum_{k=1}^{ \infty }{\dfrac{1}{u_{k}}} \)

ANSWER: A

Выберите правильный вариант ответа:Пусть дан ряд \(\sum_{k=1}^{ \infty }{u_{k}} \)

A) из абсолютной сходимости ряда следует его обычная сходимость

B) из обычной сходимости ряда следует его абсолютная сходимость

C) понятия абсолютной сходимости и обычной сходимости эквивалентны

ANSWER: A

Выберите правильный вариант ответа:Если модули членов знакочередующегося ряда \(\sum_{k=1}^{ \infty }{(-1)^{k-1} p_{k}} \), где \(p_{k} >0 \) , образуют ... бесконечно малую последовательность, то этот ряд сходится.

A) невозрастающую / убывающую

B) неубывающую / возрастающую

C) постоянную

ANSWER: A

Выберите правильный вариант ответа:Ряд \(\sum_{k=1}^{ \infty }{\dfrac{(-1)^{k-1}}{k}} \)

A) условно сходится

B) абсолютно сходится

C) расходится

ANSWER: A

Выберите правильный вариант ответа:Последовательность \(\lbrace{f_{n} (x)}\rbrace \) функций, определенных на множестве X, равномерно сходится на этом множестве к функции f(x) в том и только в том случае, когда \(lim_{n \rightarrow \infty } sup_{X} |f_{n} (x) - f(x) | = \) ... .

A) 0

B) 1

C) \(\infty \)
D) не существует
ANSWER: A

Выберите правильный вариант ответа (знак):Для любых трех точек \(M' \), \(M'' \) и \(M''' \) \(N \)-мерного евклидова пространства справедливо соотношение \(\rho (M',M''') ... \rho (M',M'') + \rho (M'',M''') \)
A) \(\leq \)
B) \(\geq \)
C) =
ANSWER: A

Выберите правильный вариант ответа (знак):Последовательность \(\lbrace{M_{n}}\rbrace \) точек \(N \)-мерного евклидова пространства \(R^{N} \) называется ..., если \(\forall (\epsilon >0) \exists (n_{0} \in \mathbb{N}) \forall (n, p \in \mathbb{N} : n_{0} \geq n) [\rho (M_{n+p} , M_{N}) < \epsilon] \) .
A) фундаментальной (последовательностью Коши)
B) убывающей
C) подпоследовательностью последовательности 1; 2; ...; n; ...
D) конечной
ANSWER: A

Выберите правильный вариант ответа:Пусть на плоскости Oxy задача спрямляемая кривая L=AB без точек самопересечения и участков самоналягания, параметризуемая при помощи уравнений \(x= \phi (x) , y= \psi (t) , a \leq t \leq b \) .Пусть функция f(x,y) определена и непрерывна вдоль кривой L=AB. Разобьем отрезок [a; b] на n частичных отрезков точками \(a=t_{0} < t_{1} < t_{2} < ... < t_{n} = b \). Каждому значению \(t_{k} \) соответствует точка \(M_{k} (x_{k}, y_{k}) \in L \), где \(x_{k} = \phi (t_{k}) , y_{k} = \psi (t_{k}) \) . Поэтому указанному разбиению кривой L на частичные дуги \(M_{0} M_{1} , M_{1} M_{2} , ... , M_{n-1} M_{n} \) . Выберем на каждой частичной дуге любую точку \(N_{k} (\xi _{k} , \eta _{k}) \in M_{k-1} M_{k} \). Тогда существует значение \(\tau _{k} \in [t_{k-1} ; t_{k}] \) такое, что \(\xi _{k} = \phi (\tau _{k}) , \eta _{k} = \psi (\tau _{k}) \). Обозначим \(\Delta t_{k} = t_{k} - t_{k-1}, \Delta x_{k} = x_{k} - x_{k-1}, \Delta y_{k} = y_{k} - y_{k-1}, \Delta l_{k} \) - длина частичной дуги \(M_{k-1} M_{k} \).Криволинейным интегралом 1-го рода от функции f(x,y) по дуге L=AB называется предел интегральной суммы \(\sigma \) при стремлении к нулю длины наибольшей частичной дуги \(\Delta l_{k} \), где \(\sigma = \) ... .
A) \(\sum_{i=1}^{n}{f(\xi _{k}, \ } \eta _{k}) \Delta l_{k} \)
B) \(\sum_{i=1}^{n}{f(\xi _{k}, \ } \eta _{k}) \Delta x_{k} \)
C) \(\sum_{i=1}^{n}{f(\xi _{k}, \ } \eta _{k}) \Delta y_{k} \)
D) \(\sum_{i=1}^{n}{f(\xi _{k}, \ } \eta _{k}) \Delta x_{k} + \sum_{i=1}^{n}{f(\xi _{k}, \ } \eta _{k}) \Delta y_{k} \)
ANSWER: A

Выберите правильный вариант ответа:Если множество измеримо по Жордану, то оно ... .
A) ограничено
B) конечно
C) счетно
D) неограниченно
ANSWER: A

Выберите правильный вариант ответа:Если множество ограничено, то его верхняя и нижняя меры ... .
A) конечны
B) бесконечны
C) отрицательны
D) равны

ANSWER: A

Выберите правильный вариант ответа:Прямоугольник \(R=[a \leq x \leq b] \times [c \leq y \leq d] \) разбит на \(np \) частичных прямоугольников \(R_{kl} = [x_{k-1} \leq x \leq x_{k}] \times [y_{l-1} \leq y \leq y_{l}] , k=1, 2, ... , n, l=1, 2, ... , p \) . Величина равная ... называется диаметром разбиения.

A) наибольшему из диаметров всех частичных прямоугольников \(R_{kl} \)

B) наименьшему из диаметров всех частичных прямоугольников \(R_{kl} \)

C) среднему арифметическому диаметров всех частичных прямоугольников \(R_{kl} \)

D) среднему геометрическому диаметров всех частичных прямоугольников \(R_{kl} \)

E) сумме диаметров всех частичных прямоугольников \(R_{kl} \)

ANSWER: A

Выберите правильный вариант ответа:Функция \(f(x,y) \) определена на прямоугольнике \(R=[a \leq x \leq b] \times [c \leq y \leq d] \), который разбит на \(np \) частичных прямоугольников \(R_{kl} = [x_{k-1} \leq x \leq x_{k}] \times [y_{l-1} \leq y \leq y_{l}] , k=1, 2, ... , n, l=1, 2, ... , p \) . На каждом частичном прямоугольнике \(R_{kl} \) выбрана произвольная точка \((\xi _{k} , \eta _{l}) \) и составлена интегральная сумма \(\sigma = \sum_{k=1}^{n}{ \sum_{l=1}^{p}{f(\xi _{k} , \eta _{l}) \Delta R_{kl} } } \), где \(\Delta R_{kl} = \Delta x_{k} \cdot \Delta y_{l} , \Delta x_{k} = x_{k} - x_{k-1} , \Delta y_{l} = y_{l} - y_{l-1} \). Функция \(f(x,y) \) называется … на прямоугольнике \(R \), если для этой функции существует на прямоугольнике \(R \) конечный предел \(I \) ее интегральных сумм \(\sigma \) при стремлении к нулю диаметра разбиения прямоугольника \(R \).

A) интегрируемой

B) дифференцируемой

C) непрерывной

D) монотонной

ANSWER: A

Выберите правильный вариант ответа (знак):Если обе функции \(f(x,y) \) и \(g(x,y) \) интегрируемы в области \(D \) и всюду в этой области \(f(x,y) \leq g(x,y) \), то \(\iint_{D}{f(x,y)dxdy} ... \iint_{D}{g(x,y)dxdy} \).

A) \(\leq \)

B) \(\geq \)

C) \(= \)

ANSWER: A

Выберите правильный вариант ответа:Если функция \(f(x,y) \) интегрируема в области \(D \) и если область \(D \) при помощи кривой \(\Gamma \) площади нуль разбивается на две не имеющие общих внутренних точек области \(D_{1} \) и \(D_{2} \) , причем \(\iint_{D}{f(x,y)dxdy} =\) ... .

A) \(\iint_{D_{1}}{f(x,y)dxdy} + \iint_{D_{2}}{f(x,y)dxdy} \)

B) \(\iint_{D_{1}}{f(x,y)dxdy} \cdot \iint_{D_{2}}{f(x,y)dxdy} \)

C) \(\iint_{D_{1}}{f(x,y)dxdy} - \iint_{D_{2}}{f(x,y)dxdy} \)

D) \(\iint_{D_{1} \cap D_{2}}{f(x,y)dxdy} \)

ANSWER: A

Выберите правильный вариант ответа:Если преобразование \(x= \phi (\xi , \eta) \), \(y= \psi (\xi , \eta) \) переводят область \(D' \) в область \(D \) и являются взаимно однозначными, и если функции \(\phi (\xi , \eta) \) и \(\psi (\xi , \eta) \) имеют в области \(D' \) непрерывные частные производные первого порядка и отличный от нуля Вронскиан, то для двойного интеграла \(\iint_{D}{f(x,y)dxdy} \) справедлива следующая формула замены переменной \(\iint_{D}{f(x,y)dxdy} =\) ... .

A) \(\iint_{D'}{f(\phi (\xi , \eta), \psi (\xi , \eta)) |\frac{\partial \phi }{\partial \xi } \cdot \frac{\partial \psi }{\partial \eta } - \frac{\partial \phi }{\partial \eta } \cdot \frac{\partial \psi }{\partial \xi } | d \xi d \eta } \)

B) \(\iint_{D}{f(\phi (\xi , \eta), \psi (\xi , \eta)) |\frac{\partial \phi }{\partial \xi } \cdot \frac{\partial \psi }{\partial \eta } + \frac{\partial \phi }{\partial \eta } \cdot \frac{\partial \psi }{\partial \xi } | d \xi d \eta } \)

C) \(\iint_{D'}{f(\phi (\xi , \eta), \psi (\xi , \eta)) |\frac{\partial \phi }{\partial \xi } \cdot \frac{\partial \psi }{\partial \eta } + \frac{\partial \phi }{\partial \eta } \cdot \frac{\partial \psi }{\partial \xi } | d \xi d \eta } \)

D) \(\iint_{D'}{f(\phi (\xi , \eta), \psi (\xi , \eta)) |\frac{\partial \phi }{\partial \xi } \cdot \frac{\partial \psi }{\partial \xi } - \frac{\partial \phi }{\partial \eta } \cdot \frac{\partial \psi }{\partial \eta } | d \xi d \eta } \)

ANSWER: A

Выберите верный ответЕсли выполнено условие\(\forall (M| (M \in \mathbb {R}) \wedge (M>0)) \exists (n_{0} \in \mathbb {N}) \forall (n| (n \in \mathbb {N}) \wedge (n \geq n_{0})) [|x_{n}| > M] \)числовая последовательность \(\lbrace{x_{i}}\rbrace \) называется

A) бесконечно большой

B) сходящейся

C) знакопеременной

D) предельной

ANSWER: A

Выберите верный ответЕсли выполнено условие\(\exists (M \in \mathbb {R}) \forall (i \in \mathbb {N}) [x_{i} \leq M] \)числовая последовательность \(\lbrace{x_{i}}\rbrace \) называется

A) ограниченной сверху

B) сходящейся

C) монотонной

D) предельной

ANSWER: A

К источникам угроз безопасности информации относятся:

A) нарушитель

B) вредоносная программа

C) программно-аппаратная (аппаратная) закладка

D) все перечисленное.

ANSWER: D

Какая функция решается подсистемой регистрации событий безопасности информации?

A) идентификация и аутентификация пользователей, являющихся работниками оператора

B) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

C) сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

ANSWER: C

В ходе анализа защищенности информационной системы реализуются

A) обновление базы данных признаков вредоносных компьютерных программ (вирусов);

B) выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

C) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

D) контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

E) функции б), в), г)

F) все функции

ANSWER: E

Принятие решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется

A) оператором информационной системы

B) владельцем информационной системы

C) федеральным органом исполнительной власти

ANSWER: B

При обеспечении защиты на этапе эксплуатации осуществляются

A) управление (администрирование) системой защиты информации информационной системы

B) выявление инцидентов и реагирование на них

C) управление конфигурацией информационной системы и ее системы защиты информации

D) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе

E) все перечисленное

ANSWER: E

Какой вид не относится к стратегиям защиты информации в компьютерной сети?

A) стратегия периметровой защиты

B) стратегия отступления

C) стратегия пресечения

D) стратегия адаптивной защиты

ANSWER: B

Какой вид не относится к стратегиям защиты информации в компьютерной сети?

A) стратегия периметровой защиты

B) стратегия отступления

C) стратегия пресечения

D) стратегия адаптивной защиты

ANSWER: B

Недостаток (слабость) информационной системы – это:

A) ошибки в программном обеспечении

B) ошибки в параметрах настройки

C) ошибки технологии обработки (передачи) информации

D) все перечисленное

ANSWER: D

Сколько всего классов защищенности автоматизированных систем?

A) 3

B) 6

C) 9

D) 12

ANSWER: C

Сколько всего классов защиты государственных информационных систем?

A) 3

B) 6

C) 9

D) 12

ANSWER: A

Сколько всего классов защиты средств вычислительной техники?
A) 3
B) 6
C) 9
D) 12
ANSWER: B
Уязвимость характеризуется:
A) слабостью
B) недостатком
C) слабостью и (или) недостатком
D) условиями и факторами
ANSWER: C
Угроза характеризуется
A) слабостью
B) недостатком
C) слабостью и (или) недостатком
D) условиями и факторами
ANSWER: D
ERP – система это:
A) система управления ресурсами предприятия
B) система регистрации событий безопасности информации
C) система управления инцидентами безопасности информации
D) система управления доступом
ANSWER: A
Какие функции не выполняет подсистема идентификации и аутентификации:
A) идентификация и аутентификация пользователей, являющихся работниками оператора
B) идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
C) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
D) ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
ANSWER: D
Какие функции не выполняет подсистема управления доступом?
A) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
B) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
C) реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
D) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
E) правильный ответ отсутствует
ANSWER: B
Что такое защита информации?
A) Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

B) Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физиче-ского, духовного и интеллектуального развития, а также защи-та информации, обеспечивающая личную безопасность

C) Деятельность, направленная на предотвращение НСД к информации

D) Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию

ANSWER: D

Концептуальная комплексность включает:

A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы

B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла

C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства

D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода

ANSWER: D

Техническая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных ипрограммно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: A

Физическая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: C

Правовая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: D

Криптографическая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: B

Способ защиты информации – это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) заранее намеченный результат защиты информации

C) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации

D) порядок и правила применения определенных принципов и средств защиты информации

ANSWER: D

Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

A) несанкционированный доступ к информации, вредительские программы, ошибки при разработке компьютерной системы

B) электромагнитные излучения и наводки, несанкционированная модификация структур компьютерной системы

C) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала

D) технические каналы утечки информации

ANSWER: C

Замысел защиты информации – это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) деятельность по обеспечению защиты информации не криптографическими методами от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию

C) совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация

D) реализация конституционных прав человека и гражданина на до-ступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность

ANSWER: A

Технический канал утечки информации – это:

A) совокупность объекта разведки, средства разведки, среды распространения сигнала

B) возможность доступа к информации с нарушением правил разграничения доступа

C) совокупность ресурсов автоматизированной системы и человека

D) возможность доступа к информации с помощью штатных средств автоматизированной системы

ANSWER: A

Несанкционированный доступ (НСД) к информации – это:

A) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)

B) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств

C) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа

D) совокупность объекта разведки, средства разведки, среды распространения сигнала

ANSWER: A

Безопасность информации – это:

A) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)

B) состояние защищенности информации (данных) при котором обеспечивается ее (их) конфиденциальность, доступность и целостность

C) реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физиче-ского, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность

D) деятельность, направленная на предотвращение НСД к информации
ANSWER: B
Структурная комплексность включает:
A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы
B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла
C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства
D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода
ANSWER: C
Временная комплексность включает:
A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы
B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла
C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства
D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода
ANSWER: B
Целевая комплексность включает:
A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы
B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла
C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства
D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода
ANSWER: A
Произведение z1z2, если z1=5+2i, z2=1-2i равно
A) 10-8i
B) 9-7i
C) 9-8i
D) 9-9i
ANSWER: C
Установите соответствие между матричным уравнением и формулой для его решения. Уравнение AX=BРешение
A) X=A-1B
B) X=ATB
C) X=BA-1
D) X=B-1A
ANSWER: A
Установите соответствие между матричным уравнением и формулой для его решения. Уравнение XA=BРешение
A) X=A-1B
B) X=ATB
C) X=BA-1
D) X=B-1A

ANSWER: C

Установите соответствие между отображением и его свойствами.Отображение y=cos⁡xСвойства:

A) Инъективная, сюръективная, биективная

B) Не инъективная, не сюръективная

C) Инъективная, не сюръективная

ANSWER: B

Установите соответствие между отображением и его свойствами.Отображение y=2x+3Свойства:

A) Инъективная, сюръективная, биективная

B) Не инъективная, не сюръективная

C) Инъективная, не сюръективная

ANSWER: A

Установите соответствие между отображением и его свойствами.Отображение y=5+exСвойства:

A) Инъективная, сюръективная, биективная

B) Не инъективная, не сюръективная

C) Инъективная, не сюръективная

ANSWER: C

Укажите, что не нужно задавать при введении исчисления высказывания

A) Алфавит

B) Правила образования формул

C) Аксиомы

D) Правила доказательства

E) Правила действия с кванторами

ANSWER: E

Какую функцию _f_(_x_,_y_) вычисляет нормальная схема подстановок* 1 → 11 *11* →.

A) f(x,y)=2y

B) f(x,y)=x+2y

C) f(x,y)=x+y+2

ANSWER: B

Установите соответствие между значением аргумента и значением функции, вычисляемой машиной Тьюринга, заданной следующей схемой 1λq1q2λRq21Lq2q1λRqz1EАргумент 1111Значение функции:

A) 1

B) 11

ANSWER: B

Установите соответствие между значением аргумента и значением функции, вычисляемой машиной Тьюринга, заданной следующей схемой 1λq1q2λRq21Lq2q1λRqz1EАргумент 1111111Значение функции:

A) 1

B) 11

ANSWER: A

Установите соответствие между названием тезиса и его описанием.Название тезиса:Тезис ЧёрчаОписание тезиса:

A) Согласно этому тезису, всякая вычислимая в интуитивном смысле функция, вычислима с помощью некоторой машины, названной в честь автора данного тезиса. Его невозможно доказать.

B) Согласно этому тезису класс функций, вычислимых с помощью алгоритмов в широком интуитивном смысле, совпадает с классом частично рекурсивных функций. Данный тезис не может быть строго доказан, но считается справедливым.

C) Согласно этому принципу, всякая вычислимая в интуитивном смысле функция, вычислима с помощью нормального алгоритма над конечным алфавитом A. Математически доказать этот принцип невозможно.

ANSWER: B

Установите соответствие между названием тезиса и его описанием.Название тезиса:Тезис ТьюрингаОписание тезиса:

A) Согласно этому тезису, всякая вычислимая в интуитивном смысле функция, вычислима с помощью некоторой машины, названной в честь автора данного тезиса. Его невозможно доказать

B) Согласно этому тезису класс функций, вычислимых с помощью алгоритмов в широком интуитивном смысле, совпадает с классом частично рекурсивных функций. Данный тезис не может быть строго доказан, но считается справедливым.

C) Согласно этому принципу, всякая вычислимая в интуитивном смысле функция, вычислима с помощью нормального алгоритма над конечным алфавитом A. Математически доказать этот принцип невозможно.

ANSWER: A

Установите соответствие между названием тезиса и его описанием.Название тезиса:Тезис МарковаОписание тезиса:

A) Согласно этому тезису, всякая вычислимая в интуитивном смысле функция, вычислима с помощью некоторой машины, названной в честь автора данного тезиса. Его невозможно доказать.

B) Согласно этому тезису класс функций, вычислимых с помощью алгоритмов в широком интуитивном смысле, совпадает с классом частично рекурсивных функций. Данный тезис не может быть строго доказан, но считается справедливым.

C) Согласно этому принципу, всякая вычислимая в интуитивном смысле функция, вычислима с помощью нормального алгоритма над конечным алфавитом A. Математически доказать этот принцип невозможно.

ANSWER: C

Дана формула алгебры логики Определите, какой из формул алгебры логики она равносильна. Выберите правильный ответ.

A)

B)

C)

D) $z\rightarrow(x\vee y)$

ANSWER: B

Дана функции алгебры логики найдите ее совершенную дизъюнктивную нормальную форму (СДНФ). Выберите правильный ответ.

A)

B)

C)

D) $x\wedge y\wedge z$

ANSWER: A

На множестве заданы бинарные отношения:Какое из этих отношений является рефлексивным? Выберите правильный вариант ответа:

A) отношение R1

B) отношение R2

C) отношение R3

D) отношение R3 и R2

ANSWER: A

На множестве заданы бинарные отношенияКакое из этих отношений является симметричным? Выберите правильный вариант ответа:

A) отношение R1

B) отношение R2
C) отношение R3
D) отношение R3 и R2
ANSWER: B
Отношение эквивалентности обладает свойствами:
A) рефлексивность, симметричность, транзитивность
B) рефлексивность, антисимметричность, транзитивность
C) антирефлексивность, асимметричность, транзитивность
D) взаимная однозначность, асимметричность, транзитивность
ANSWER: A
К какому типу принадлежит уравнение y'+y=xy3?
A) линейное
B) Бернулли
C) в полных дифференциалах
D) риккати
ANSWER: B
К какому типу принадлежит уравнение (sin(x)+y)dy + (ycos(x)-x2)dx=0?
A) с разделяющимися переменными
B) линейное
C) однородное
D) в полных дифференциалах
ANSWER: D
К какому типу принадлежит уравнение x3 y''' - x2 y'' + 2xy' - 2y = x3?
A) уравнение третьего порядка с постоянными коэффициентами
B) уравнение третьего порядка с переменными коэффициентами
C) уравнение Эйлера
ANSWER: B
Укажите частное решение дифференциального уравнения xy'=1
A) y=_ln_|x|+c
B) y=_ln_|x+c|
C) y=_ln_|x|
D) y=cex
E) y=2_ln_|x|
F) y=_ln_|x+1|
ANSWER: C
Уравнение λ2-2λ+1 является характеристическим уравнением дифференциального уравнения
A) y''-2y'+1=0
B) y''-2y'+y=0
C) y''-2y'=0
D) y'''-2y''-y=x
ANSWER: B
Что такое префиксный код?
A) Это код фиксированной длины
B) Это код, в котором никакое кодовое слово не совпадает с начальной частью какого-то другого кодового слова
C) Это код, в котором никакое кодовое слово не совпадает с завершением какого-то другого кодового слова
ANSWER: B
Выберите правильное значение расстояния Хэмминга для следующего двоичного кодового набора:0101100000010001101001001111011010100011100100100010100111001111101001110100
A) 12

B) 11
C) 10
D) 13
E) 14
ANSWER: A
В результате сложения со знаком двух двоичных 11-разрядных чисел 11101101000111110101 01имели место следующие переносы относительно старшего разряда:
A) Входящий и исходящий вместе
B) Только входящий
C) Только исходящий
D) Не было переносов вообще
E) Больше двух переносов
ANSWER: A
Как называется возможность скрыть детали реализации?
A) Инкапсуляция
B) Наследование
C) Полиморфизм
ANSWER: A
При наследовании:
A) Данные производному классу наследуются от базового класса
B) Методы производному классу наследуются от базового класса
C) Данные и методы производному классу наследуются от базового класса
ANSWER: C
Методы класса это:
A) правила, как работать с объектами класса
B) функции-члены класса, могут быть статическими или динамическими
C) динамические функции-члены класса
D) статические функции-члены класса
ANSWER: B
Можно ли в языке программирование c# не использовать блок get в реализации свойства?
A) можно
B) нельзя
C) можно, но с точки зрения корректности разработки — это неправильно
ANSWER: C
Как получить ссылку на текущий экземпляр класса внутри самого класса?
A) с помощью соответствующей переменной или параметра метода
B) с помощью ключевого слова super
C) с помощью ключевого слова this
D) с помощью ключевого слова value
E) с помощью ключевого слова base
ANSWER: C
Верно ли, что если метод использует открытые члены класса, то он должен быть открытым?
A) да
B) нет
ANSWER: B
верно ли написана реализация класса на языке программирования c#?class A{ public abstract void DoIt() { }}
A) да
B) нет

ANSWER: B

Возможно ли перекрытие абстрактных методов класса в производном классе?

A) да

B) нет

ANSWER: A

Обязательно ли перекрытие абстрактных методов класса в производном классе?

A) да

B) нет

ANSWER: B

Как удалить объект в программе, написанной на языке C#?

A) вызвать деструктор

B) с помощью оператора delete

C) удалять объект в программе не нужно, он будет удалён сборщиком мусора

D) присвоить переменной значение null

ANSWER: C

Возможно ли множественное наследование в языке программирования C#?

A) множественное наследование в языке C# не поддерживается

B) множественное наследование в языке C# возможно только для интерфейсов

ANSWER: B

Какие утверждения верны для массивов в языке Java?

A) Размер массива может быть изменен после его создания.

B) Индексация элементов в массиве начинается с 1.

C) Все элементы в конкретном массиве должны быть одного типа (или наследоваться от одного типа).

D) В одной программе могут использоваться массивы только для одного типа данных.

ANSWER: C

Почему для конкатенации множества строк в языке Java следует использовать StringBuilder (выберите верные утверждения)?

A) Конкатенация строк оператором «+» не предусмотрена.

B) При конкатенации строк с помощью оператором «+» результат всегда печатается в консоль (стандартный поток вывода – stdout).

C) Конкатенация строк оператором «+» приводит к созданию множества экземпляров строк и многократному копированию данных.

D) Строки не являются ссылочным типом данных.

ANSWER: C

Строгая типизация предполагает (выберите верные утверждения)?

A) Все используемые в функции переменные должны объявляться строго до остального кода функции.

B) При компиляции программы весь код (все операции) проверяется на совместимость или возможность преобразования типов, несовместимость считается ошибкой.

C) В программе нельзя определить несколько функций с одинаковым именем.

D) Язык программирования обязательно должен быть объектно-ориентированным.

ANSWER: B

Что возвращает функция, приведенная ниже:

A) последнее положительное значение в массиве

B) максимальное значение в массиве
C) минимальное значение после первого положительного значения в массиве
D) минимальное положительное значение в массиве
ANSWER: D
Кто является инициатором записи данных Cookie?
A) Веб-сервер
B) Клиентское приложение
C) Данные Cookie всегда сохраняются автоматически
D) Это может быть кто угодно
ANSWER: A
В какой части ответа сервера содержится запрашиваемый клиентом веб-ресурс?
A) В теле ответа сервера
B) В заголовке ответа сервера
C) В строке состояния ответа сервера
ANSWER: A
К какому классу языков относятся языки сценариев с точки зрения поддержки типизации переменных?
A) К типизированным языкам
B) К нетипизированным языкам
C) Это зависит от конкретного языка сценариев
ANSWER: B
Алгоритм состоит из 2-х последовательно выполняемых частей. Вычислительная сложность первой части алгоритма – O(n2), второй – O(n). Какова вычислительная сложность всего алгоритма?
A) O(n)
B) O(n2)
C) O(n3)
D) Для определения вычислительной сложности всего алгоритма недостаточно данных
ANSWER: B
Где может формироваться пара ключей при создании сертификата в PKI ?
A) на смарт-карте
B) на стороне удостоверяющего центра
C) на стороне корневого удостоверяющего центра
D) на стороне CRL
E) на стороне AIA
ANSWER: A
Где может формироваться пара ключей при создании сертификата в PKI ?
A) на смарт-карте
B) на стороне удостоверяющего центра
C) на стороне корневого удостоверяющего центра
D) на стороне CRL
E) на стороне AIA
ANSWER: A
Компоненты VPN (как системы удаленного доступа) обычно включают:
A) NYS
B) YP
C) AAA
D) WPA
E) AIA

ANSWER: C

Компоненты VPN (как системы удаленного доступа) обычно включают:

A) NYS

B) YP

C) AAA

D) WPA

E) AIA

ANSWER: C

В ходе конфигурирования ViPNet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация локальной сети ViPNet и добавлено новое рабочее место (АП). Какие ключи потребуются (без учёта ключей защиты ключей) для обработки исходящего зашифрованного сообщения с этого нового АП?

A) ключи ЭП, ключи АП

B) ключи ЭП, ключи АП, ключи пользователя

C) ключи ЭП, ключи АП, межсетевой мастер-ключ

D) ключи АП, ключи пользователя

E) ключи ЭП, ключи пользователя

ANSWER: A

В ходе конфигурирования ViPNet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация локальной сети ViPNet и добавлено новое рабочее место (АП). Какие ключи потребуются (без учёта ключей защиты ключей) для обработки исходящего зашифрованного сообщения с этого нового АП?

A) ключи ЭП, ключи АП

B) ключи ЭП, ключи АП, ключи пользователя

C) ключи ЭП, ключи АП, межсетевой мастер-ключ

D) ключи АП, ключи пользователя

E) ключи ЭП, ключи пользователя

ANSWER: A

Назовите тип(ы) УЦ, приемлемые для получения сертификатов для веб-сервера компании.

A) Standalone, Enterprise

B) Root, Subordinate

C) Public

D) Private

ANSWER: C

Назовите тип(ы) УЦ, приемлемые для получения сертификатов для веб-сервера компании.

A) Standalone, Enterprise

B) Root, Subordinate

C) Public

D) Private

ANSWER: C

Назовите тип(ы) УЦ, приемлемыедля получения сертификатов для смарткарт пользователей VPN.

A) Standalone, Enterprise

B) Root, Subordinate

C) Public

D) Private

ANSWER: D

Назовите тип(ы) УЦ, приемлемыедля получения сертификатов для смарткарт пользователей VPN.

A) Standalone, Enterprise

B) Root, Subordinate
C) Public
D) Private
ANSWER: D
Мощность какого множества модели ХРУ больше: субъектов или объектов ?
A) субъектов
B) объектов
ANSWER: B
Какая ролевая модель реализует статическое разделение обязанностей?
A) модель с иерархической организацией ролей
B) модель с ограничениями на одновременное использование ролей в одном сеансе
C) модель со взаимоисключающими ролями
ANSWER: C
Какими понятиями замещается понятие «субъект» в ролевой модели?
A) объект
B) пользователь
C) сущность
D) роль
ANSWER: B
Что означает правило управления доступом user в ролевой модели?
A) для каждого сеанса определяет пользователя, который осуществляет этот сеанс работы с системой
B) для каждого сеанса задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе
C) для каждого сеанса определяет набор ролей, которые могут быть одновременно доступны пользователю в этом сеансе
ANSWER: A
Какая ролевая модель реализует динамическое разделение обязанностей?
A) модель с иерархической организацией ролей
B) модель с ограничениями на одновременное использование ролей в одном сеансе
C) модель со взаимоисключающими ролями
ANSWER: B
К какому классу моделей безопасности относится модель Take-Grant?
A) дискреционные модели безопасности
B) мандатные модели безопасности
C) ролевые модели безопасности
ANSWER: A
К какому классу моделей безопасности относится модель типизированной матрицы доступа?
A) дискреционные модели безопасности
B) мандатные модели безопасности
C) ролевые модели безопасности
ANSWER: A
К какому классу моделей безопасности относится модель Белла-ЛаПадулы?
A) дискреционные модели безопасности
B) мандатные модели безопасности
C) ролевые модели безопасности
ANSWER: B

К какому классу моделей безопасности относится модель безопасности переходов?

A) дискреционные модели безопасности

B) мандатные модели безопасности

C) ролевые модели безопасности

ANSWER: B

Сколько примитивных (элементарных) операций используется в классической модели ХРУ?

A) 4

B) 6

C) 5

D) 7

ANSWER: B

К какому классу операций относится операция Create классической модели ХРУ?

A) монотонная

B) немонотонная

ANSWER: A

Сколько основных множеств использует ролевая модель для описания системы?

A) 5

B) 4

C) 3

D) 7

ANSWER: B

В каком случае задача проверки безопасности системы ХРУ является разрешимой?

A) система команд не содержит элементарных операций «удалить» и «уничтожить»

B) команды являются монооперационными

C) команды системы являются одноусловными и монотонными

ANSWER: C

Сколько функций уровня безопасности используется в модели безопасности переходов?

A) 3

B) 2

C) 1

ANSWER: B

Состояние в модели Белла-ЛаПадулы называется безопасным по чтению, если

A) уровень безопасности субъекта не ниже уровня безопасности объекта

B) уровень безопасности объекта не ниже уровня безопасности субъекта

ANSWER: A

Система ХРУ называется монооперационной, если

A) система команд не содержит элементарных операций «удалить» и «уничтожить»

B) каждая команда системы содержит одну элементарную операцию

C) команды системы являются одноусловными

ANSWER: B

Удовлетворяет ли функция перехода Z-системы ограничениям основной теоремы безопасности Белла-ЛаПадулы?

A) да

B) нет

ANSWER: A

Ячейка матрицы доступа модели XPY является

A) строкой

B) множеством

C) числом

ANSWER: B

Какое дополнительное отношение на множестве ролей вводится в ролевой модели с иерархической организацией ролей?

A) отношение строгого порядка

B) отношение эквивалентности

C) отношение толерантности

D) отношение нестрогого порядка

ANSWER: D

Какое количество базовых представлений включают в себя модели безопасности?

A) 4

B) 6

C) 7

D) 5

ANSWER: B

Существует ли алгоритм проверки безопасности произвольной системы XPY?

A) да

B) нет

ANSWER: B

Возможности (capabilities) потоков в Linux позволяют

A) Разделить возможности суперпользователя на несколько отдельных возможностей, которые могут быть разрешены независимо на уровне потока

B) Ограничить использование потоком процессорного времени

C) Разрешить прямой доступ к объектам ядра

ANSWER: A

В MS Windows под термином олицетворение (impersonation) понимают

A) Возможность выполнения потока в контексте безопасности, отличном от контекста безопасности своего процесса

B) Возможность идентифицировать владельца потока

C) Возможность удаленного запуска потока с использованием механизма RPC

ANSWER: A

Контроль учетных записей (User Account Control, UAC) в MS Windows реализует

A) Механизм защиты от вредоносных программ

B) Ограничение срока действия учетной записи

C) Контроль уровеня доверия к учетной записи

ANSWER: A

При одновременном присутствии в списке контроля доступа разрешающей и запрещающей записи по одному и тому же виду доступа для одного и того же субъекта доступа в современных реализациях ОС MS Windows

A) Запрещающая запись имеет приоритет

B) Разрешающая запись имеет приоритет

C) Поведение системы не определено

ANSWER: A

В UNIX-подлобных системах Sticky-bit (атрибут T) установленный для каталога имеет следующее действие

A) Не оказывает никакого действия для каталогов в современных реализациях операционных систем

B) Для новых файлов группой-владельцем становится группа-владелец каталога

C) Пользователь может удалять из каталога только файлы, которыми он владеет

D) Файлы из каталога нельзя объявить исполняемыми

ANSWER: C

В UNIX-подобных системах при вычислении хэша пароля используется дополнительный открытый ключ (соль), применение которого обеспечивает

A) Генерацию разного хэша для одинаковых паролей

B) Увеличение числа вариантов пароля

ANSWER: A

В UNIX-подобных системах атрибут разрешение исполнения (x) применительно к каталогу разрешает

A) Получить список имен файлов из каталога

B) Создавать файлы в каталоге

C) Удалять файлы в каталоге

D) Переходить в каталог

ANSWER: D

Для проверки подлинности данных, полученных через открытый канал или хранимых в ненадежном хранилище, может быть использован алгоритм

A) HMAC – hash-based message authentication code

B) HOTP – HMAC-Based One-Time Password Algorithm

C) TOTP – Time-based One-Time Password Algorithm

ANSWER: A

Политика безопасности это

A) Набор правил, регламентирующих порядок хранения и обработки информации

B) Перечень требуемых программ технической защиты информации и их настроек

C) Список ограничений на действия пользователей

ANSWER: A

Встроенный программный межсетевой экран в Linux и MS Windows обеспечивает

A) Фильтрацию сетевого трафика в соответствии с заданными правилами для предотвращения возможности использования злоумышленником уязвимостей сетевых протоколов и программного обеспечения

B) Шифрование и контроль целостности пакетов в сетевом трафике для защиты от подмены данных

ANSWER: A

Оценочный уровень доверия 1 обеспечивает

A) Минимальный уровень доверия, который подтверждает только наличие в составе ОС некоторых средств защиты

B) Уровень доверия от невысокого до умеренного, достигаемый при отсутствии доступа к полной документации по разработке ОС, основанный на анализе структуры ОС с использованием полученной от разработчика ОС дополнительной информации.

C) Умеренный уровень доверия, основанный на всестороннем методическом исследовании функций безопасности и процесса разработки ОС

D) Уровень доверия от умеренного до высокого в отношении уже существующей ОС общего назначения, основанный на всестороннем методическом тестировании и проверке реализации функций безопасности

ОС, на уверенности в правильном использовании типовых методов при проектирования ОС.

E) Высокий уровень доверия для разрабатываемой ОС, основанный на использовании полуформальных методов при проектировании и тестировании ОС.

F) Уверенность в безопасности ОС при работе в условиях высокого риска, где ценность защищаемых данных оправдывает дополнительные затраты, основанную на использовании полуформальных методов при верификации и тестировании ОС

G) Уверенность в безопасности ОС при работе в условиях чрезвычайно высокого риска, где высокая ценность защищаемых данных оправдывает повышенные затраты, основанную на использовании формальных методов при верификации и тестировании ОС

ANSWER: A

Оценочный уровень доверия 4 (Наиболее высокий уровень доверия, достижимый при оценке существующих ОС общего назначения, так как боле высокий уровень доверия требует вмешательства в разработку ОС) обеспечивает

A) Некоторую уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией (в процессе реализации не были внесены неучтенные изменения)

B) Уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией

C) Высокую уверенность в том, что подсистема безопасности ОС реализована в соответствии с предъявляемыми требованиями

ANSWER: B

Каких типов процессоров (по виду набора команд) НЕ существует?

A) CISC

B) RISC

C) MISC

D) VLIW

E) MPLA

ANSWER: E

Что такое порог срабатывания?

A) напряжение, примерно равное 1,3...1,4 В

B) уровень выходного напряжения

C) уровень входного напряжения, выше которого сигнал воспринимается как единица, а ниже — как нуль

ANSWER: C

Что такое аналоговый сигнал?

A) это сигнал, который может принимать любые значения в определенных пределах

B) это сигнал, несущий в себе какую-то информацию

C) это сигнал, приходящий на электронную систему извне и искажающий полезный

ANSWER: A

Какие устройства называются аналоговыми?

A) устройства, работающие только с аналоговыми сигналами

B) устройства, аналогичные друг другу

C) устройства, преобразующие физические величины в напряжение или ток

ANSWER: A

Выберите утверждение, характеризующее связь температуры процессора и тротлинга:

A) Прямой взаимосвязи между температурой и тротлингом не существует

B) Чем выше температура, тем больше тротлинг

C) Чем ниже температура, тем меньше тротлинг

ANSWER: B

Выберите правильное утверждение, характеризующее функционал контроллера прерываний наиболее полно. Контроллер прерываний это…

A) микросхема или встроенный блок процессора, отвечающий за возможность последовательной обработки запросов на прерывание от разных устройств

B) особый вид часов реального времени, синхронизирующий обмен контроллеров данными

C) специальное устройство, перезагружающее СВТ при «зависании»

D) обработчик сигналов от устройств ввода/вывода

ANSWER: A

Какой функционал НЕ реализуется в математических сопроцессорах?

A) аппаратный функционал, реализующий взятие прямого и обратного преобразования Фурье

B) выполнение операций с плавающей точкой

C) перезагрузка СВТ при «зависании»

D) решение задач численными методами

ANSWER: C

Какими из перечисленных особенностей НЕ обладают процессоры архитектуры CISC:

A) нефиксированное значение длины команды

B) фиксированное значение длины команды

C) арифметические действия кодируются в одной команде

D) небольшое число регистров, каждый из которых выполняет строго определённую функцию

ANSWER: B

Какими из перечисленных особенностей НЕ обладают процессоры архитектуры CISC:

A) нефиксированное значение длины команды

B) фиксированное значение длины команды

C) арифметические действия кодируются в одной команде

D) небольшое число регистров, каждый из которых выполняет строго определённую функцию

ANSWER: B

Какой функционал реализуется в классических (не гибридных) видеопроцессорах (GPU)?

A) синхронизация генерации звука и процесса наложения текстур не модель

B) расчет реалистичной физики

C) рендер изображения и его вывод на интерактивное устройство отображения

D) выполнение арифметических операций с матрицами

ANSWER: C

Выберите пункт, нарушающий стандартную очередность операций BIOS:

A) выполнение тестирования оборудования компьютера

B) чтение настроек из энергонезависимого ПЗУ

C) обновление ядра операционной системы

D) применение настроек

E) поиск и загрузка в оперативную память кода загрузчика

F) передача управления загрузчику

ANSWER: C
Операция AND это:
A) операция логического умножения
B) операция отрицания
C) операция логического сложения
D) операция отрицания равнозначности
ANSWER: A
ЧТО ОЗНАЧАЕТ ШЕСТЬ КОРОТКИХ СИГНАЛОВ?
A) Ошибок не обнаружено, ПК исправен
B) Проблемы с блоком питания
C) Неисправность оперативной памяти
D) Неисправность контроллера клавиатуры
ANSWER: D
КАТАЛОГ /ETC СОДЕРЖИТ
A) Загрузочные файлы
B) Файлы пользователей
C) Конфигурационные файлы
D) Файлы устройств
E) Исполняемые файлы
F) Каталоги для монтирования временных файловых систем
ANSWER: C
КАТАЛОГ /MNT СОДЕРЖИТ
A) Загрузочные файлы
B) Файлы пользователей
C) Конфигурационные файлы
D) Файлы устройств
E) Исполняемые файлы
F) Каталоги для монтирования временных файловых систем
ANSWER: F
КАТАЛОГ /BIN СОДЕРЖИТ
A) Загрузочные файлы
B) Файлы пользователей
C) Конфигурационные файлы
D) Файлы устройств
E) Исполняемые файлы
ANSWER: E
КАТАЛОГ /SBIN СОДЕРЖИТ
A) Конфигурационные файлы
B) Файлы пользователей
C) Системные исполняемые файлы
D) Файлы устройств
E) Загрузочные файлы
F) Каталоги для монтирования временных файловых систем
ANSWER: C
ФАЙЛ /ETC/LILO.CONF СОДЕРЖИТ
A) Параметры настройки видеосистемы
B) Параметры начальной загрузки
C) Меню начальной загрузки
D) Путь к ядру операционной системы
ANSWER: B
ЧТОБЫ ИЗМЕНИТЬ РАЗМЕР ФАЙЛА ПОДКАЧКИ В WINDOWS, НЕОБХОДИМО РЕДАКТИРОВАТЬ ПАРАМЕТРЫ:
A) Загрузка и восстановление
B) Быстродействие

C) Переменные среды
D) Профили пользователей
ANSWER: B

С ЧЕМ ОБЫЧНО СВЯЗАНО ВОЗНИКАЮЩЕЕ В ПРОЦЕССЕ ДЛИТЕЛЬНОЙ ЭКСПЛУАТАЦИИ УВЕЛИЧЕНИЕ ВРЕМЕНИ ОТВЕТА ОС WINDOWS:
A) С необходимостью очистки системного блока от пыли
B) С ростом размера системного реестра
C) С уменьшением объема свободного места на системном диске
ANSWER: B

КАК НАЗЫВАЕТСЯ ТЕХНОЛОГИЯ УПРАВЛЕНИЯ РАСПРЕДЕЛЕННЫМИ СИСТЕМАМИ ОТ CISCO SYSTEMS, COMPAQ COMPUTER, INTEL И MICROSOFT , ПОЗВОЛЯЮЩАЯ РЕШАТЬ ТАКИЕ ЗАДАЧИ КАК УПРАВЛЕНИЕ ОС WINDOWS, УПРАВЛЕНИЕ РЕСУРСАМИ И СЛУЖБАМИ СЕТИ, МОНИТОРИНГ СОСТОЯНИЯ СИСТЕМЫ В РЕАЛЬНОМ ВРЕМЕНИ:
A) CIM (Common Information Model)
B) WBEM (Web-Based Enterprise Management)
C) WMI (Windows Management Instrumentation)
ANSWER: C

НА ОСНОВЕ КАКОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ БЫЛА РАЗРАБОТАНА СИСТЕМА ANDROID:
A) Linux
B) MiniX
C) Windows iOS
ANSWER: A

КАК НАЗЫВАЕТСЯ РЕЖИМ ИСПОЛЬЗОВАНИЯ ANDROID-СИСТЕМЫ С МАКСИМАЛЬНЫМИ ПРАВАМИ (АНАЛОГ АДМИНИСТРАТОРА WINDOWS):
A) Суперпользователь
B) Root-Home пользователь Android
C) user
D) Up-User
ANSWER: A

ЧТО НЕ ЯВЛЯЕТСЯ ХАРАКТЕРНОЙ ЧЕРТОЙ RISC-АРХИТЕКТУРЫ:
A) Использование компиляторов, оптимизирующих работу конвейера машинных команд
B) В состав процессора включают расширенный набор регистров
C) Серьезное внимание должно быть уделено командам условного перехода
D) В процессорах можно использовать сокращенный набор команд
ANSWER: C

КАКАЯ АРХИТЕКТУРА ОС ИМЕЕТ ТАКОЙ НЕДОСТАТОК, КАК СНИЖЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ ПО СРАВНЕНИЮ С РЕАЛЬНЫМ КОМПЬЮТЕРОМ, И, КАК ПРАВИЛО, ОНИ ОЧЕНЬ ГРОМОЗДКИ
A) Монолитное ядро
B) Многоуровневая ОС
C) Смешанная ОС
D) Виртуальная машина
ANSWER: D

КАКОЙ ИЗ ВНЕШНИХ ИНТЕРФЕЙСОВ ОБЛАДАЕТ ПЕРВОНАЧАЛЬНОЙ СКОРОСТЬЮ 850 МБИТ/С:
A) Параллельный порт (LPT)
B) Fire Wire
C) Последовательный порт (RS 323)
D) Fire Wire 800
E) USB 2.0

ANSWER: D

ОСНОВНЫМ ПРИЗНАКОМ КАКИХ СИСТЕМ ЯВЛЯЕТСЯ НАЛИЧИЕ ВЕКТОРНО-КОНВЕЙЕРНЫХ ПРОЦЕССОРОВ?

A) PVP-систем

B) NUMA-систем

C) SMP-систем

ANSWER: A

ПРЕИМУЩЕСТВА АРХИТЕКТУРЫ МИКРОЯДРА ОПЕРАЦИОННОЙ СИСТЕМЫ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО

A) Повышается скорость работы приложений

B) Эффективнее расходуются ресурсы системы

C) Ядро становится более надежное

ANSWER: C

АЛГОРИТМ ВЫБОРКИ ПО ТРЕБОВАНИЮ С КЛАСТЕРИЗАЦИЕЙ ПОЗВОЛЯЕТ

A) Загрузить требуемую в данный момент страницу и не загружать расположенные рядом с ней

B) Загрузить требуемую в данный момент страницу и расположенные рядом с ней

C) Загрузить требуемую в данный момент страницу

D) Упреждающе загружать страницу, которая потребуется в ближайшее время

E) Упреждающе загружать

ANSWER: B

КОМАНДА ОС UNIX: PS

A) Отображает содержимое текущего каталога

B) Позволяет завершить выполняющийся процесс

C) Отображает перечень запущенных процессов

D) Позволяет создать символическую связь

ANSWER: C

ВЕТВЬ РЕЕСТРА - HKEY_CLASSES_ROOT СОДЕРЖИТ

A) Информацию об аппаратных средствах компьютера

B) Ассоциации по типам файлов и данные по ярлыкам

C) Информацию об программном обеспечении

D) Информацию о пользователях

ANSWER: B

ВЕТВЬ РЕЕСТРА - HKEY_CURRENT_CONFIG СОДЕРЖИТ

A) Информацию о текущем аппаратном профиле

B) Информацию об программном обеспечении

C) Информацию о пользователях

D) Ассоциации по типам файлов и данные по ярлыкам

ANSWER: A

Сетевой стандарт FDDI использует метод доступа:

A) с передачей маркера

B) по приоритету запроса

C) множественный доступ с контролем несущей и обнаружением коллизий

D) множественный доступ с контролем несущей и предотвращением коллизий

ANSWER: A

Сетевой стандарт FDDI имеет топологию:

A) звезда

B) шина

C) кольцо

D) точка-точка
E) инфраструктура
ANSWER: C
Сетевой стандарт Gigabit Ethernet 1000 Base T использует метод доступа:
A) с передачей маркера
B) по приоритету запроса
C) множественный доступ с контролем несущей и обнаружением коллизий
D) множественный доступ с контролем несущей и предотвращением коллизий
ANSWER: C
Сетевой стандарт Gigabit Ethernet 1000 Base T имеет топологию:
A) звезда
B) шина
C) кольцо
D) точка-точка
E) инфраструктура
ANSWER: A
Сетевой стандарт Gigabit Ethernet 1000 Base T имеет кабель:
A) оптоволоконный
B) неэкранированная витая пара
C) коаксиальный
ANSWER: B
Сетевое устройство Repieter выполняет функцию
A) усиление сигнала
B) объединение компьютеров
C) объединение участков сетей
D) определение маршрутов передачи данных
E) объединение сетей с разными стандартами
ANSWER: A
Протокол IPX/SPX работает на основе
A) IP-адресов
B) IPX-адресов
C) MAC-адресов
D) имен
ANSWER: C
Для проверки работоспособности компьютерной сети на основе протокола TCP/IP служит программа:
A) ping
B) ipconfig
C) netstat
ANSWER: A
В таблице IP-маршрутизации используется адрес 0.0.0.0
A) для адресации пакетов по умолчанию
B) для адресации групповой рассылки
C) для адресации локальной сети
D) для адресации широковещательных пакетов
E) для адресации самого компьютера (обратный адрес)
ANSWER: A
Какой уровень OSI отвечает за доставку?
A) прикладной
B) представлений
C) сеансовый
D) транспортный

E) сетевой
F) канальный
G) физический
ANSWER: D
На каком уровне работает сетевое устройство router?
A) прикладной
B) представлений
C) сеансовый
D) транспортный
E) сетевой
F) канальный
G) физический
ANSWER: E
Заголовок канального уровня в пакете содержит:
A) IP адрес
B) MAC адрес
C) Номер порта
ANSWER: B
Где может формироваться пара ключей при создании сертификата в PKI ?
A) на смарт-карте
B) на стороне удостоверяющего центра
C) на стороне корневого удостоверяющего центра
D) на стороне CRL
E) на стороне AIA
ANSWER: A
Компоненты VPN (как системы удаленного доступа) обычно включают:
A) NYS
B) YP
C) AAA
D) WPA
E) AIA
ANSWER: C
В ходе конфигурирования ViPNet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация локальной сети ViPNet и добавлено новое рабочее место (АП). Какие ключи потребуются (без учёта ключей защиты ключей) для обработки исходящего зашифрованного сообщения с этого нового АП?
A) ключи ЭП, ключи АП
B) ключи ЭП, ключи АП, ключи пользователя
C) ключи ЭП, ключи АП, межсетевой мастер-ключ
D) ключи АП, ключи пользователя
E) ключи ЭП, ключи пользователя
ANSWER: A
Назовите тип(ы) УЦ, приемлемые для получения сертификатов для веб-сервера компании.
A) Standalone, Enterprise
B) Root, Subordinate
C) Public
D) Private
ANSWER: C
Назовите тип(ы) УЦ, приемлемыедля получения сертификатов для смарткарт пользователей VPN.
A) Standalone, Enterprise

B) Root, Subordinate
C) Public
D) Private
ANSWER: D

Выберите правильный вариант ответа:Что являлось основой политической системы Древней Греции?
A) полисы
B) номы
C) фемы
D) коммуны
ANSWER: A

Выберите правильный вариант ответа:Что из перечисленного было характерно для славянофилов в России XIX века?
A) идеализация истории допетровской Руси
B) идеализация капиталистического общества
C) стремление к возрождению старообрядчества
D) стремление к возрождению традиционных языческих культов
ANSWER: A

Выберите правильный вариант ответа:В какой стране к середине XIX века завершился промышленный переворот?
A) Англия
B) Германия
C) Россия
D) Франция
ANSWER: A

Выберите правильный вариант ответа:Какая из перечисленных реформ произошла в России в 1860-1870-х годах?
A) земская реформа
B) Столыпинская аграрная реформа
C) учреждение первых министерств
D) секуляризация церковных земель
ANSWER: A

Выберите правильный вариант ответа:Декрет о земле, принятый на II Всероссийском съезде Советов отменял … .
A) право частной собственности на землю
B) крепостное право
C) продразвёртку
D) крестьянскую общину
ANSWER: A

Выберите правильный вариант ответа:Кто в годы гражданской войны возглавлял в России Добровольческую армию?
A) Деникин А.И.
B) Брусилов А.А.
C) Каменев С.С.
D) Власов А.А.
ANSWER: A

Выберите правильный вариант ответа:Продовольственная диктатура, введенная в годы «военного коммунизма» предусматривала … .
A) принудительное изъятие излишков сельхозпродукции
B) создание колхозов
C) введение натурального сельскохозяйственного налога
D) ликвидацию помещичьих хозяйств
ANSWER: A

Выберите правильный вариант ответа:В каком году в Италии установился Фашистский режим?

A) 1922 г.

B) 1939 г.

C) 1914 г.

D) 1936 г.

ANSWER: A

Выберите правильный вариант ответа:В каком году была принята первая Конституция Советского Союза?

A) 1924 г.

B) 1922 г.

C) 1918 г.

D) 1936 г.

ANSWER: A

Выберите правильный вариант ответа:Какое положение из названных характеризует новую экономическую политику?

A) разрешение иностранных концессий

B) введение всеобщей трудовой повинности

C) отмена частной собственности на землю

D) установление продовольственной диктатуры

ANSWER: A

Выберите правильный вариант ответа:Что стало одной из причин свёртывания НЭПа?

A) несоответствие НЭПа идеологическим установкам большевиков

B) падение уровня жизни людей, по сравнению с периодом осуществления политики «военного коммунизма»

C) невозможность создания колхозов в условиях НЭПа

D) массовые крестьянские выступления с требованиями проведения сплошной коллективизации

ANSWER: A

Выберите правильный вариант ответа:К какому веку относится появление в славянских землях норманнов во главе с Рюриком?

A) IX век

B) XI век

C) X век

D) XII век

ANSWER: A

Выберите правильный вариант ответа:Крупнейшей стройкой первых пятилеток было … .

A) строительство Днепрогэса

B) строительство транссиба

C) освоение Донбасса

D) строительство Байконура

ANSWER: A

Выберите правильный вариант ответа:Благодаря советско-германскому договору от 1939 года в состав СССР вошла … .

A) Прибалтика

B) Украина

C) Болгария

D) Чехословакия

ANSWER: A

Выберите правильный вариант ответа:Главным вопросом Мюнхенской конференции 1938 года стал вопрос о … .

A) передаче Судетской области Германии

B) ненападении, между Чехословакией и Германией
C) объединении Австрии и Германии
D) заключении «Антикоминтерновского пакта»
ANSWER: A

Выберите правильный вариант ответа:В 1941 году немецкие войска были … .
A) разгромлены под Москвой
B) разгромлены под Смоленском
C) окружены в Сталинграде
D) разбиты в Ленинграде
ANSWER: A

Выберите правильный вариант ответа:В конце 40-х – начале 50-х преследовали «безродных космополитов» обвиняя людей в … .
A) преклонении перед Западом
B) коррупции
C) нелегальном пересечении границы
D) хищении государственного имущества
ANSWER: A

Выберите правильный вариант ответа:Что из нижеперечисленного связано с понятием «десталинизация»?
A) реабилитация политических заключённых
B) борьба с диссидентами
C) разрешение многопартийности
D) созыв съезда народных депутатов
ANSWER: A

Выберите правильный вариант ответа:Какое из приведенных событий произошло позже остальных?
A) ввод советских войск в Афганистан
B) Карибский кризис
C) ввод советских войск в Венгрию
D) создание НАТО
ANSWER: A

Выберите правильный вариант ответа:Кого в Советском Союза называли диссидентами?
A) борцов с существующим строем
B) злостных прогульщиков
C) агентов иностранной разведки
D) борцов с «космополитизмом»
ANSWER: A

Выберите правильный вариант ответа:Согласно решению XIX конференции КПСС высшим органом государственной власти в СССР становился … .
A) Съезд народных депутатов СССР
B) Совет Министров СССР
C) Государственная Дума СССР
D) Федеральное собрание
ANSWER: A

Укажите, что из перечисленного относится к реформам правительства Ельцина — Гайдара начала 1990-х гг.:
A) ваучерная приватизация
B) начало деятельности Съезда народных депутатов
C) реализация национальных проектов в социальной сфере и экономике
D) образование Государственного совета Российской Федерации
ANSWER: A

Выберите правильный вариант ответа:Ключевым принципом функционирования средневекового общества в Западной Европе был принцип … .

A) вассалитета
B) верховенства права
C) веротерпимости
D) демократического централизма
ANSWER: A

Выберите правильный вариант ответа:В соответствии с Конституцией Российской Федерации 1993 года высшим законодательным органом государственной власти стал двухпалатный парламент, получивший название … .

A) Федеральное собрание
B) Верховный Совет
C) Национальная ассамблея
D) Народное собрание
ANSWER: A

Выберите правильный вариант ответа:Когда впервые состоялся созыв Земского собора в России?

A) XVI век
B) XII век
C) XV век
D) XVII век
ANSWER: A

Выберите правильный вариант ответа:В европейской экономике XVI-XVII веков произошла … .

A) «революция цен»
B) промышленная революция
C) натурализация хозяйства
D) индустриализация
ANSWER: A

Выберите правильный вариант ответа:Какой из перечисленных городов был в XVII веке центром российской морской торговли со странами Западной Европы?

A) Архангельск
B) Рига
C) Кронштадт
D) Мурманск
ANSWER: A

Выберите правильный вариант ответа:Противником России, в ходе Северной войны была … .

A) Швеция
B) Польша
C) Пруссия
D) Дания
ANSWER: A

Выберите правильный вариант ответа:«Верховный тайный совет» играл определяющую роль в политической жизни России при … .

A) Петре II
B) Павле I
C) Екатерине II
D) Петре III
ANSWER: A

Выберите правильный вариант ответа:В число «просветителей», в европейской истории XVIII века, входил … .

A) Ж.-Ж. Руссо

B) Н. Макиавелли

C) Б. Спиноза

D) Ф. Аквинский

ANSWER: A

Алгоритм RSA основан на следующей математической задаче

A) дискретного логарифмирования

B) факторизации числа

C) нахождения простых чисел

ANSWER: B

Алгоритм Диффи-Хеллмана дает возможность

A) безопасно обменяться общим секретом при условии аутентификации сторон

B) безопасно обменяться общим секретом

C) зашифровать сообщение

D) подписать сообщение

ANSWER: A

Алгоритм Диффи-Хеллмана основан на следующей математической задаче

A) факторизации числа

B) нахождения простых чисел

C) дискретного логарифмирования

ANSWER: C

Аутентификация сторон в алгоритме Диффи-Хеллмана необходима, потому что

A) в противном случае атакующий может взломать дискретный логарифм

B) в противном случае атакующий может перехватить передаваемые открытые ключи и заменить их своим открытым ключом

C) в противном случае стороны не смогут вычислить общий секрет

ANSWER: B

Для создания цифровой подписи следует использовать

A) свой закрытый ключ

B) свой открытый ключ

C) закрытый ключ получателя

D) открытый ключ получателя

ANSWER: A

Другое название линейного поточного шифрования данных

A) перестановка

B) гаммирование

C) подстановка

D) имитовставка

ANSWER: B

Задачей дискретного логарифмирования является

A) нахождение степени, в которую следует возвести простое число для получения заданного целого числа

B) нахождение степени, в которую следует возвести целое число для получения заданного целого числа

C) разложение числа на простые сомножители

ANSWER: B

Ситуация, в которой при использовании различных ключей для шифрования одного и того же сообщения в результате получается один и тот же шифротекст

A) коллизия

B) избыточность

C) хеширование

D) атака повтора

ANSWER: A

Какой из алгоритмов реализует асимметричное шифрование и может использоваться для формирования цифровой подписи

A) 3DES

B) Blowfish

C) AES

D) RSA

ANSWER: D

Криптосистемы с последовательным выполнением преобразований над элементами открытого текста называются

A) блочными шифрами

B) поточными шифрами

C) двоичными аддитивными шифрами

D) криптосистемами с ключом однократного применения

ANSWER: B

Максимальная длина ключа в алгоритме Blowfish

A) 512 бит

B) 128 бит

C) 256 бит

D) 448 бит

ANSWER: D

Метод построения блочных шифров, используемый в алгоритме AES

A) SP-сеть

B) сеть Фейстеля

ANSWER: A

Название криптосистем, в которых ключ шифрования и ключ дешифрования совпадают

A) симметричные

B) асимметричные

C) простые

D) гибридные

ANSWER: A

Наука, изучающая математические методы нарушения конфиденциальности и целостности информации

A) криптоанализ

B) ктиптология

C) криптография

D) стегоанализ

ANSWER: A

Отличие самосинхронизирующихся поточных шифров от блочных

A) шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма

B) шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности

C) для шифрования и расшифровки используются разные ключи

D) каждый блок открытого текста шифруется независимо от остальных блоков

ANSWER: B

Отличие синхронных поточных шифров от блочных

A) шифрограмма есть результат наложения последовательности текста и последовательности гаммы, зависящей от входной последовательности

B) для шифрования и расшифровки используются разные ключи

C) каждый блок открытого текста шифруется независимо от остальных блоков

D) шифрограмма есть результат наложения последовательности текста и последовательности работающего генератора гамма

ANSWER: D

Порядок использования операций шифрования и расшифровки в алгоритме 3DES при создании зашифрованного сообщения

A) C = EK1[DK2[EK1[M]]], K1 ≠ K2 (E → D → E)

B) C = DK1[EK2[DK1[M]]], K1 ≠ K2 (D → E → D)

C) не имеет значения

ANSWER: C

Протокол Нидхема-Шредера применяется для

A) шифрования

B) аутентификации

C) выработки электронной подписи

ANSWER: B

Размер общего ключа алгоритма 3DES (все ключи разные)

A) 56 бит

B) 112 бит

C) 168 бит

D) 256 бит

ANSWER: C

Разрядность ключа алгоритма шифрования ГОСТ Р 34.12-2015

A) 128 бит

B) 192 бита

C) 256 бит

D) 320 бит

ANSWER: C

Разрядность шифруемых блоков данных в алгоритме RSA

A) больше разрядности ключа

B) равна разрядности ключа

C) меньше разрядности ключа

D) произвольная

ANSWER: C

Режим CBC используется для того, чтобы

A) одинаковые незашифрованные блоки преобразовывались в различные зашифрованные блоки

B) не было необходимости разбивать сообщение на целое число блоков достаточно большой длины

C) увеличить скорость шифрования

ANSWER: A

Режим шифрования, сохраняющий статистические особенности открытого текста

A) Cipher block chaining (CBC)

B) Cipher feed back (CFB)

C) Electronic code book (ECB)

ANSWER: C

Установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем

A) идентификация
B) авторизация
C) аутентификация
D) контроль целостности
ANSWER: C
Функция, для которой легко найти прямое отображение и очень сложно найти обратное
A) нелинейная
B) односторонняя
C) линейная
D) многозначная
ANSWER: B
Функция, предназначенная для сжатия строки произвольной длины до нескольких десятков или сотен бит
A) ЭЦП
B) логарифмическая функция
C) функция Эйлера
D) хеш-функция
ANSWER: D
Целостность – это
A) невозможность несанкционированного просмотра информации
B) невозможность несанкционированного доступа к информации
C) невозможность несанкционированного изменения информации
ANSWER: C
Шифр – это
A) состояние, выражающее процесс образования зашифрованных данных из открытых данных
B) ключевое запоминающее устройство
C) совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с использованием ключей
D) значение исходных открытых параметров алгоритма криптографического преобразования
ANSWER: C
Электронная подпись – это
A) имитовставка
B) информация, необходимая для шифрования и расшифровки сообщений
C) способ преобразования исходного секретного сообщения с целью его защиты
D) присоединяемый к сообщению блок данных, полученный с использованием криптографического преобразования
ANSWER: D
Алгоритм Рабина основан на алгоритме:
A) Алгоритм Рабина
B) Эль-Гамаля
C) RSA
D) AES
ANSWER: C
Алгоритм Рабина-Миллера является способом:
A) Проверки числа на простоту
B) Разложения числа на сомножители
C) Решения задачи дискретного логарифмирования
D) Вычисления функции Эйлера

ANSWER: A

Закрытым ключом в алгоритме RSA является:

A) Произвольно выбранное число, взаимно простое со значением функции Эйлера

B) Мультипликативно обратное число, вычисленное по алгоритму Евклида

ANSWER: A

Необходимым условием для использования функции в качестве односторонней является:

A) Теоретическая необратимость

B) Практическая необратимость

C) Практическая и теоретическая необратимость

D) Ни одно из перечисленных

ANSWER: B

Открытый ключ в схеме Эль-Гамаля получают при помощи:

A) Выбора произвольного целого числа, меньшего чем открытый параметр

B) Выбора числа, взаимно простого со значением функции Эйлера

C) Определением образующего элемента поля

D) Решением задачи дискретного логарифмирования

ANSWER: C

От схем асимметричного шифрования ЭЦП отличатся тем, что:

A) Требует доверенного посредника

B) Криптосистему формирует отправитель

C) Не может использоваться совместно с шифрованием

D) Не требует теоретической необратимости односторонних функций

ANSWER: B

К проблемам симметричных шифров не относятся:

A) Задача распространения ключей

B) Обеспечение подлинности

C) Низкая криптостойкость

D) Рост количества ключей при росте числа абонентов

ANSWER: C

Протоколы аутентификации являются:

A) Частным случаем интерактивных систем доказательства

B) Развитием схемы византийского соглашения

C) Модификацией схемы Шнорра

D) Групповыми криптопротоколами

ANSWER: A

Задача разложения большого целого числа на множители называется:

A) Дискретным логарифмированием

B) Нахождением вычетов по модулю

C) Факторизацией

D) Задачей Ферма

ANSWER: C

Теоретическую стойкость шифра не определяют:

A) То, что знание шифртекста не влечет перераспределение вероятностей на множестве шифруемых текстов

B) Априорное допущение об информированности противника о криптосистеме с точностью до ключевой информации

C) Стремление к нулю средней вероятности правильной дешифровки открытого текста с ростом длины сообщения

D) Возможность подбора эффективного метода взлома по принципу оптимального соотношения минимальной трудоемкости и максимальной вероятности верной дешифровки

ANSWER: D

К основным требованиям к хеш-функции не относятся:

A) Низкая вероятность совпадения дайджеста разных документов

B) Необратимость

C) Однозначность

D) Устойчивость к поиску коллизий

ANSWER: D

Что такое префиксный код?

A) Это код фиксированной длины

B) Это код, в котором никакое кодовое слово не совпадает с начальной частью какого-то другого кодового слова

C) Это код, в котором никакое кодовое слово не совпадает с завершением какого-то другого кодового слова

ANSWER: B

Выберите правильное значение расстояния Хэмминга для следующего двоичного кодового набора:0101100000010001101001001111011010100011100100100010100111001111101001110100

A) 12

B) 11

C) 10

D) 13

E) 14

ANSWER: A

В результате сложения со знаком двух двоичных 11-разрядных чисел 11101101000111110101011имели место следующие переносы относительно старшего разряда:

A) Входящий и исходящий вместе

B) Только входящий

C) Только исходящий

D) Не было переносов вообще

E) Больше двух переносов

ANSWER: A

Как называется характеристика радиотехнической системы, представляющей собой ее отклик на входной бесконечно короткий сигнал единичной площади:

A) Частотный коэффициент передачи

B) Спектр

C) Импульсная характеристика

D) Переходная характеристика

ANSWER: C

Сколько точек содержит сигнальное созвездие QPSK-сигнала (сигнал с квадратурной фазовой манипуляцией)?

A) 2

B) 4

C) 6

D) 8

ANSWER: B

Фильтр, амплитудно-частотная характеристика (АЧХ) которого повторяет форму амплитудного спектра сигнала, а фазочастотная характеристика (ФЧХ)

симметрична фазовому спектру с учетом задержки на время длительности сигнала и максимизирующий отношение сигнал/шум, называется:

A) фильтром низких частот

B) фильтром высоких частот

C) согласованным фильтром

D) режекторным фильтром

ANSWER: C

Вероятность ошибки связанная с вынесением решением в пользу наличия в принятой реализации полезного сигнала при условии его отсутствия называется:

A) вероятностью пропуска

B) вероятностью ложной тревоги

C) априорной вероятностью

D) полной вероятностью ошибки

ANSWER: B

Вероятность выхода из строя устройства, состоящего из трех последовательно соединенных функциональных блоков, при условии что вероятность безотказной работы каждого блока в течение определенного времени T равна p1, p2 и p3 соответственно:

A) 1-p1*p2*p3

B) p1* p2*p3

C) p1*p3-p2

D) p1-p2*p3

ANSWER: A

Сигнал на выходе линейной стационарной цепи связан с сигналом на входе через:

A) Интеграл Дюамеля

B) Интеграл Пуассона

C) Интеграл Лаплапса

D) Интеграл Фурье

ANSWER: A

Какое из нижеперечисленных утверждений является неверным:

A) у периодических сигналов линейчатые спектры

B) у непериодических сигналов непрерывные спектры

C) на выходе линейной стационарной системы модуль спектральной плотности выходного сигнала представляет собой произведение модуля спектральной плотности входного и модуля амплитудной характеристики системы

D) на выходе линейной стационарной системы модуль спектральной плотности выходного сигнала представляет собой произведение модуля спектральной плотности входного и квадрата модуля амплитудной характеристики системы

ANSWER: C

Представление объекта диагностики, при котором элементы представляются в виде совокупности вершин, а связи между ними в виде направленных дуг, соответствующих направлениям распространения энергии и информации называется:

A) ориентированным графом информационно-энергетических связей

B) структурной схемой

C) принципиальной схемой

D) ненаправленным графом

ANSWER: A

Прибор, предназначенный для исследования амплитудных и временных параметров электрического сигнала, подаваемого на его вход и позволяющий

в процессе диагностики наглядно отображать зависимости на экране называется:

A) вольтметром
B) амперметром
C) частотомером
D) осциллографом
ANSWER: D

Способ поиска неисправностей, при котором отказ определяется на основании анализа известных признаков, однозначно характеризующих данный отказ

A) способ характерного признака
B) способ промежуточных измерений
C) способ контрольных переключений и поверок
D) способ сравнения
ANSWER: A

Устройство для снижения амплитуды до нужного уровня с целью измерения, а также для защиты измерительного прибора от чрезмерных уровней сигнала, которые могут повредить его это:

A) аттенюатор
B) делитель частоты
C) фильтр
D) осциллограф
ANSWER: A

Как называется эффект искажения сигнала во временной области при аналого-цифровом преобразовании, вызванный наложением высокочастотных составляющих на низкочастотные, вследствие недостаточной частоты дискретизации?

A) Алиасинг
B) Перемодуляция
C) Замирания
D) Передискретизация
ANSWER: A

Многолучевость распространения радиоволн в точке приема вызывает эффект

A) замирания
B) модуляции
C) усиления
D) фильтрации
ANSWER: A

Какой, в соответствии с теоремой Котельникова, должна быть минимально допустимая частота дискретизации аналогового сигнала с ограниченным спектром, верхняя частота которого f=20 кГц.

A) 80 кГц
B) 10 кГц
C) 40 кГц
D) 40 Гц
ANSWER: C

Вид искажения в радиотехнической системе при которой форма огибающей модулированного сигнала на выходе модулятора перестает повторять форму передаваемого сообщения называется:

A) демодуляцией
B) перемодуляцией
C) дисперсией
D) передискретизацией

ANSWER: B

Суть комбинационного метода проверки неисправностей состоит в:

A) проверке полной группы параметров, обеспечивающих однозначное выявление неработоспособного элемента

B) в последовательном разбиении на группы (содержащие неисправный элемент) и осуществлении серии проверок до определения неисправного элемента

C) последовательной проверке всех элементов по одному в определенной последовательности

ANSWER: A

Что произойдет с шириной спектра сигнала при увеличении его длительности в 2 раза?

A) увеличится в 4 раза

B) не измениться

C) увеличится в 2 раза

D) уменьшится в 2 раза

ANSWER: D

Фильтр низких частот (ФНЧ) предназначен для:

A) пропускания низких частот в спектре и обрезания высоких

B) пропускания высоких частот в спектре и обрезания низких

C) пропускании сигнала без изменений

D) пропускании спектральных составляющих сигнала в некоторой полосе частот

ANSWER: A

Чем отличается амплитудно-модулированный сигнал (АМ-сигнал) с балансной модуляцией от обычного АМ-сигнала:

A) в спектре отсутствуют составляющие справа от несущего колебания

B) в спектре отсутствуют составляющие на несущей частоте

C) в спектре отсутствуют составляющие слева от несущего колебания

D) спектр сигнала находится в области низких частот

ANSWER: B

Как называется процесс переноса спектра сигнала из области низких частот в область высоких частот при котором один или несколько параметров несущего колебания изменяются по закону передаваемого сообщения:

A) модуляция

B) демодуляция

C) кодирование

D) декодирование

ANSWER: A

Вариант тестирование ПО, предполагающий наличие доступа к любым ресурсам, в первую очередь к исходным кодам, а также техническому заданию и всевозможной документации

A) тестирование по принципу «белого ящика»

B) тестирование по принципу «черного ящика»

C) тестирование по принципу «серого ящика»

ANSWER: A

Вариант тестирования ПО, для которого необходима лишь возможность взаимодействия с ПО, но не требуется подробная информация о внутреннем устройстве программы

A) тестирование по принципу «белого ящика»

B) тестирование по принципу «серого ящика»

C) тестирование по принципу «черного ящика»

ANSWER: C

Вариант тестирования ПО, при котором в распоряжении специалиста находится исполняемый файл приложения и, возможно, некая базовая документация

A) тестирование по принципу «белого ящика»

B) тестирование по принципу «черного ящика»

C) тестирование по принципу «серого ящика»

ANSWER: C

Верно ли утверждение: "Во время трансляции исходного кода в процессорные инструкции, компилятор может вносить в структуру программы значительные изменения, поэтому фрагменты анализируемого исходного кода могут не в полной мере соответствовать тому, как выполняется программа"

A) да

B) нет

ANSWER: A

Если отрицательные значения передаются стандартным функциям копирования или выделения памяти в качестве размера буферов, то

A) они неявно преобразуются в большие беззнаковые значения, что может привести к переполнению буфера

B) они неявно преобразуются в беззнаковые значения путем отбрасывания минуса (модуль числа), что может привести к неопределенному поведению программы

C) фиксируются ошибки на этапе компиляции программы

ANSWER: A

Метод фаззинга, не предполагающий наличия информации о синтаксической структуре входных данных, при котором формируются массивы псевдослучайных данных и передаются исследуемой программе

A) полностью случайное тестирование

B) мутирующее тестирование

C) порождающее тестирование

ANSWER: A

Метод фаззинга, предполагающий формирование тестовых наборов на основе предварительного изучения спецификаций протоколов или форматов файлов, создания грамматик с указанием в них переменных и статических данных, а также динамически вычисляемых величин

A) полностью случайное тестирование

B) мутирующее тестирование

C) порождающее тестирование

ANSWER: C

Метод фаззинга, формирующий тестовые наборы данных на основе коллекции имеющихся (корректно сформированных входных данных), путем искажения последних (искажаются случайные байты или строки)

A) полностью случайное тестирование

B) мутирующее тестирование

C) порождающее тестирование

ANSWER: B

Механизм ASLR используется для

A) быстрого отображения файлов в память

B) увеличения пространства данных программы на заданное число байт

C) рандомизации расположения сегментов в адресном пространстве процесса

ANSWER: C

Ошибки в программе, при которых компиляция завершается успешно, при пробных запусках программа ведет себя нормально, однако при анализе

результата выясняется, что он неверный. Для их устранения необходимо «вручную» анализировать алгоритм

A) синтаксические

B) времени выполнения

C) алгоритмические

D) препроцессорные

ANSWER: C

Сегмент BSS содержит

A) глобальные и статические переменные, которые не были явным образом инициализированы в исходном коде, и которые будут при запуске программы инициализированы нулями

B) глобальные переменные, которые инициализированы программистом

C) локальные переменные и аргументы

D) динамически размещаемые данные

ANSWER: A

Сегмент Heap содержит

A) глобальные и статические переменные, которые не были явным образом инициализированы в исходном коде, и которые будут при запуске программы инициализированы нулями

B) глобальные переменные, которые инициализированы программистом

C) локальные переменные и аргументы

D) динамически размещаемые данные

ANSWER: D

Фаззеры, предназначенные для выявления уязвимостей типа SQL-инъекций или межсайтового скриптинга

A) фаззеры сетевых протоколов

B) фаззеры веб-приложений

C) фаззеры файловых форматов

D) фаззеры командной строки

ANSWER: B

В чем заключается камуфлирование защищаемого программного обеспечения?

A) Камуфлированное защищаемое программное обеспечение не может быть использовано незарегистрированными пользователями

B) Камуфлированное защищаемое программное обеспечение не может быть найдено незарегистрированными пользователями

C) Камуфлированное защищаемое программное обеспечение не соответствует требованиям системы

D) Камуфлированное защищаемое программное обеспечение может быть использовано незарегистрированными пользователями

E) Камуфлированное защищаемое программное обеспечение содержит встроенную последовательность ЦВЗ

ANSWER: A

Каким образом формируются маски, накладываемые на блоки пикселей в алгоритме Bruyndonckx

A) случайный порядок

B) зигзагом, начиная с левого верхнего элемента

C) блоками заданной размерности (2*2)

D) зигзагом, начиная с правого верхнего элемента

E) последовательно (слева направо)

ANSWER: A

В чем заключается основная идея атаки хи-квадрат?

A) высчитывании вероятности встраивания на основе того, как близко располагаются значения частот четных и нечетных коэффициентов DCT

B) модификации НЗБ DCT

C) оценивании статистических характеристик контейнера

D) высчитывании вероятности восстановления встроенного сообщения

E) высчитывании разности между вероятностями встраивания на основе того, как близко располагаются значения частот четных и нечетных коэффициентов DCT

ANSWER: A

Стеганография это__

A) наука о скрытой передаче информации, путем сохранения в тайне самого факта передачи

B) наука о скрытой передаче информации, путем сохранения в тайне самой информации

C) наука о скрытой передаче информации, путем сохранения в тайне самого факта передачи и непосредственно передаваемой информации

D) наука о видимой передаче информации, путем сохранения в тайне самой информации

E) наука о скрытой передаче информации, путем сохранения в тайне исходного контейнера

ANSWER: A

По способу организации контейнера в методах компьютерной стеганографии различают

A) потоковые, фиксированные

B) систематические, несистематические

C) суррогатные, селективные, конструирующие

ANSWER: B

По способу выбора контейнера в методах компьютерной стеганографии различают

A) потоковые, фиксированные

B) систематические, несистематические

C) суррогатные, селективные, конструирующие

ANSWER: C

ЦВЗ могут быть:

A) робастные, хрупкие и полухрупкие

B) робастные, полухрупкие

C) текстовые, графические

D) суррогатные, селективные и конструирующие

E) робастные, хрупкие, полухрупкие, селективные, конструирующие

ANSWER: A

По используемому принципу скрытия методы компьютерной стеганографии делятся на

A) методы непосредственной замены и спектральные методы

B) пространственные методы и дискретные методы

C) систематические и несистематические

D) спектральные методы и дискретные методы

E) методы непосредственной замены, спектральные методы, дискретные методы

ANSWER: A

По способу доступа к информации в методах компьютерной стеганографии различают

A) потоковые, фиксированные

B) систематические, несистематические

C) суррогатные, селективные, конструирующие

ANSWER: A

Выберите правильное

A) свойства заполненного контейнера и восстанавливаемого сообщения должны искажаться минимально

B) свойства исходного контейнера и сообщения должны изменяться минимально

C) свойства заполненного контейнера и исходного сообщения должны искажаться минимально

D) свойства заполненного контейнера и восстанавливаемого сообщения должны искажаться максимально

E) свойства контейнера и сообщения не должны искажаться

ANSWER: A

В схеме встраивания и извлечения ЦВЗ для извлечения ЦВЗ из маркированного контейнера используется

A) декодер

B) детектор

C) прекодер

D) стегокодер

ANSWER: A

В схеме встраивания и извлечения ЦВЗ для определения наличия встроенного ЦВЗ в контейнере используется

A) декодер

B) детектор

C) прекодер

D) стегокодер

ANSWER: B

В схеме встраивания и извлечения ЦВЗ для реализации встраивания кодированного ЦВЗ в контейнер с учетом свойств контейнера и самого ЦВЗ используется

A) декодер

B) детектор

C) прекодер

D) стегокодер

ANSWER: D

Базовые стеганографические операторы, описывающие процедуры встраивания и извлечения данных из стегоконтейнеров, могут быть записаны в виде

A) I'=F(I,M,K), M'=F-1(I',K)

B) I'=F(I,M,K), M'=F-1(I')

C) I'=F(M,K), M'=F-1(I',K)

D) I'=F(K), M'=F-1(K)

E) I'=F(I,K), M'=F-1(I',K)

ANSWER: A

В схеме встраивания и извлечения ЦВЗ для реализации преобразования водяного знака к виду, пригодному для встраивания в контейнер используется

A) декодер

B) детектор

C) прекодер

D) стегокодер

ANSWER: C

В какому направлению стеганографии относятся следующие примерыиспользование стеганографических файловых систем, скрытие данных в неиспользуемых областях форматов файлов, подмена символов в названиях файлов, текстовая стеганография и т.д.

A) Компьютерная стеганография

B) Цифровая стеганография

ANSWER: A

Какие ЦВЗ характеризуются высокой устойчивостью к различным трансформациям заполненного контейнера включая компрессию с потерями, фильтрацию, яркостную коррекцию, масштабирование и т.д.

A) робастные

B) хрупкие

C) полухрупкие

ANSWER: A

Какие ЦВЗ разрушаются при незначительной модификации заполненного контейнера

A) робастные

B) хрупкие

C) полухрупкие

ANSWER: B

Какие ЦВЗ устойчивы по отношению к одному типу воздействий и неустойчивы по отношению к другим

A) робастные

B) хрупкие

C) полухрупкие

ANSWER: C

При реализации стеганографического встраивания в какой области контейнеров-изображений скрываемые данные внедряются в элементы преобразованного с использованием одного из известных спектральных методов растрового представления.

A) пространственной

B) частотной

ANSWER: B

Стегоалгоритмы данного класса предназначены для встраивания ЦВЗ в аудио- и графические контейнеры путем линейной их модификации

A) аддитивные

B) вероятностные

C) пространственные

D) частотные

ANSWER: A

Для чего реализуется камуфлирование защищаемого программного обеспечения

A) чтобы оно не могло быть использовано незарегистрированными пользователями

B) чтобы оно могло быть использовано зарегистрированными пользователями

C) чтобы оно не могло быть использовано всеми пользователями

ANSWER: A

В НАСТОЯЩЕЕ ВРЕМЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КРИПТОЗАЩИТЫ ИНФОРМАЦИИ ДЕЙСТВУЮТ СЛЕДУЮЩИЕ НОРМАТИВНО-МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ФСБ РОССИИ:

A) все вышеперечисленные;

B) Приказ ФСБ от 10 июля 2014 года N 378 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";

C) Приказ ФСБ России от 9 февраля 2005 года N 66 "Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)";

D) "Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну", утвержденная приказом ФАПСИ от 13 июня 2001 года N 152;

E) "Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности", утвержденные руководством 8 Центра ФСБ России (N 149/7/2/6-432 от 31.03.2015);

ANSWER: A

ЧЕМ УДОСТОВЕРЯЕТСЯ СООТВЕТСТВИЕ СРЕДСТВ КРИПТОЗАЩИТЫ ИНФОРМАЦИИ, ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ?

A) сертификатом соответствия;

B) аттестатом соответствия;

C) лицензией;

D) аттестатом аккредитации;

ANSWER: A

СКОЛЬКО КЛАССОВ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ МОЖЕТ ПРИМЕНЯТЬСЯ ДЛЯ НЕЙТРАЛИЗАЦИИ АТАК, ОРГАНИЗУЕМЫХ С ЦЕЛЬЮ НАРУШЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ?

A) пять классов;

B) два класса;

C) три класса;

D) четыре класса;

ANSWER: A

ФОРМИРОВАНИЕ ТРЕБОВАНИЙ К ЗАЩИТЕ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ, ПРЕДПОЛАГАЕТ СЛЕДУЮЩИЕ ЭТАПЫ:

A) принятие решения о необходимости защиты информации; классификацию информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

B) анализ рисков нарушения информационной безопасности; разработку модели угроз безопасности информации; определение требований к системе защиты информации;

C) анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система; определение угроз безопасности информации; определение требований к системе защиты информации;

D) определение информации, подлежащей защите в информационной системе и ее значимости; классификации информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

ANSWER: A

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ И (ИЛИ) ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА СОЗДАНИЕ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДОЛЖНЫ БЫТЬ СОГЛАСОВАНЫ (В ПРЕДЕЛАХ ИХ ПОЛНОМОЧИЙ В ЧАСТИ,

КАСАЮЩЕЙСЯ ВЫПОЛНЕНИЯ УСТАНОВЛЕННЫХ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ) С:

A) ФСТЭК России; ФСБ России;

B) ФСТЭК России; ФСБ России; Минцифры России; Роскомнадзор;

C) ФСТЭК России; Роскомнадзор; Минцифры России;

D) ФСТЭК России; ФСБ России; Роскомнадзор;

E) ФСТЭК России; Минцифры России;

ANSWER: A

ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОПРЕДЕЛЯЮТСЯВ ЗАВИСИМОСТИ ОТ:

A) класса защищенности информационной системы и угроз безопасности информации, включенных в модель угроз безопасности информации;

B) банка данных угроз безопасности информации (bdu.fstec.ru), а также результатов анализа уязвимостей информационной системы;

C) модели угроз безопасности информации, а также результатов анализа уязвимостей информационной системы;

D) от значимости обрабатываемой в ней информации и масштаба информационной системы;

ANSWER: A

В КАКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ В ЦЕЛЯХ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДУСМОТРЕНО ОБЯЗАТЕЛЬНОЕ ПРИМЕНЕНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ?

A) в информационных системах персональных данных, если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации и осуществляется передача таких персональных данных по не защищенным каналам связи и/или осуществляется хранение персональных данных на носителях информации, несанкционированный доступ к которым со стороны нарушителя не может быть исключен с помощью некриптографических методов и способов;

B) в государственных информационных системах;

C) в информационных системах персональных данных;

D) в информационных системах общего пользования;

ANSWER: A

В КАКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ В ЦЕЛЯХ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДУСМОТРЕНО ОБЯЗАТЕЛЬНОЕ ПРИМЕНЕНИЕ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ?

A) в информационных системах общего пользования;

B) в государственных информационных системах;

C) в информационных системах персональных данных;

D) во всех перечисленных выше информационных системах;

ANSWER: A

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОСУЩЕСТВЛЯЕТСЯ В СООТВЕТСТВИИ С ТЕХНИЧЕСКИМ ЗАДАНИЕМ НА СОЗДАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ И (ИЛИ) ТЕХНИЧЕСКИМ ЗАДАНИЕМ (ЧАСТНЫМ ТЕХНИЧЕСКИМ ЗАДАНИЕМ) НА СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И ВКЛЮЧАЕТ СЛЕДУЮЩИЕ СТАДИИ:

A) классификацию информационной системы по требованиям защиты информации; определение угроз безопасности информации; определение требований к системе защиты информации;

B) разработку модели угроз; определение требований к системе защиты информации; определение видов и типов средств защиты информации, обеспечивающих реализацию технических мер защиты информации; разработку эксплуатационной документации;

C) разработку модели угроз; определение требований к системе защиты информации; определение необходимых средств защиты информации; разработку организационно-распорядительной и эксплуатационной документации;

D) проектирование системы защиты информации; разработку эксплуатационной документации;макетирование и тестирование системы защиты информации (при необходимости);

ANSWER: A

ЭКСПЛУАТАЦИОННАЯ ДОКУМЕНТАЦИЯ НА СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ РАЗРАБАТЫВАЕТСЯ С УЧЕТОМ ГОСТ 34.601, ГОСТ 34.201 И ГОСТ Р 51624 И ДОЛЖНА В ТОМ ЧИСЛЕ СОДЕРЖАТЬ:

A) описание структуры системы защиты информации информационной системы; описание состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств; описание правил эксплуатации системы защиты;

B) руководство пользователя; руководство оператора; руководство администратора; описание правил эксплуатации системы защиты информации информационной системы;

C) руководство администратора информационной системы; описание правил развертывания и эксплуатации системы защиты информации информационной системы;

D) порядок развертывания и настройки средств защиты информации;описание правил эксплуатации системы защиты; правила и требования по реализации установленных мер защиты информации;

ANSWER: A

ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОСУЩЕСТВЛЯЕТСЯ В СООТВЕТСТВИИ С ПРОЕКТНОЙ И ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИЕЙ НА СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ И В ТОМ ЧИСЛЕ ВКЛЮЧАЕТ:

A) установку и настройку средств защиты; разработку организационно-распорядительных документов по защите информации; внедрение организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;

B) настройку средств защиты; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; приемочные испытания; аттестацию информационной системы;

C) развертывание средств защиты; разработку организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;

D) установку и настройку средств защиты; разработку организационно-распорядительных документов по защите информации; внедрение организационных мер защиты информации; обучение пользователей; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; приемочные испытания;

ANSWER: A

РАЗРАБАТЫВАЕМЫЕ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДОЛЖНЫ ОПРЕДЕЛЯТЬ ПРАВИЛА И ПРОЦЕДУРЫ:

A) управления (администрирования) системой защиты информации; выявления инцидентов безопасности информации и реагирования на них; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе; защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации;

B) управления (администрирования) системой защиты информации; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе; защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации;

C) управления (администрирования) системой защиты информации; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

D) выявления инцидентов безопасности информации и реагирования на них; управления конфигурацией информационной системы и системы защиты информации; контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

ANSWER: A

ПРИ ВНЕДРЕНИИ ОРГАНИЗАЦИОННЫХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ ОСУЩЕСТВЛЯЮТСЯ:

A) реализация правил разграничения доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения; проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов; отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации;

B) реализация правил разграничения доступа, установка и настройка средств защиты; разработка организационно-распорядительных документов по защите информации; обучение пользователей; предварительные испытания системы защиты информации; опытная эксплуатация системы защиты информации;

C) развертывание средств защиты; разработка организационных мер защиты информации; предварительные испытания системы защиты информации; опытную эксплуатацию системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; приемочные испытания;

D) обучение пользователей; предварительные испытания системы защиты информации; опытная эксплуатация системы защиты информации; анализ уязвимостей и принятие мер защиты информации по их устранению; реализация правил разграничения доступа, и введение ограничений на действия пользователей; проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов; отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации;

ANSWER: A

ОЦЕНКА ЭФФЕКТИВНОСТИ РЕАЛИЗОВАННЫХ В РАМКАХ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРОВОДИТСЯ ОПЕРАТОРОМ

A) не реже одного раза в 3 года;

B) ежегодно;

C) при возникновении инцидента;

ANSWER: A

ДЕЯТЕЛЬНОСТЬ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ЛИЦЕНЗИРУЕТСЯ В СООТВЕТСТВИИ С ПОЛОЖЕНИЯМИ:

A) Федерального закона от 04 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;

B) Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

C) Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;

ANSWER: A

ДЛЯ ОБЕСПЕЧЕНИЯ КАКОГО УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ НЕОБХОДИМО В ТОМ ЧИСЛЕ СОЗДАНИЕ СТРУКТУРНОГО ПОДРАЗДЕЛЕНИЯ, ОТВЕТСТВЕННОГО ЗА ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ, ЛИБО ВОЗЛОЖЕНИЕ НА ОДНО ИЗ СТРУКТУРНЫХ ПОДРАЗДЕЛЕНИЙ ФУНКЦИЙ ПО ОБЕСПЕЧЕНИЮ ТАКОЙ БЕЗОПАСНОСТИ?

A) первого;

B) любого уровня защищенности;

C) третьего и выше;

D) второго и выше;

ANSWER: A

ПОЛОЖЕНИЕ О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО РАЗРАБОТКЕ, ПРОИЗВОДСТВУ, РАСПРОСТРАНЕНИЮ ШИФРОВАЛЬНЫХ (КРИПТОГРАФИЧЕСКИХ) СРЕДСТВ УСТАНАВЛИВАЕТ ЛИЦЕНЗИОННЫЕ ТРЕБОВАНИЯ К СООТВЕТСТВУЮЩЕЙ ДЕЯТЕЛЬНОСТИ СО СРЕДСТВАМИ, ПРЕДНАЗНАЧЕННЫМИ

A) для защиты информации конфиденциального характера;

B) для защиты информации, содержащей персональные данные;

C) для защиты информации, обладатель которой осуществляет техническое обслуживание шифровальных (криптографических) средств для обеспечения собственных нужд;

ANSWER: A

КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ ЯВЛЯЕТСЯ ЭЛЕКТРОННАЯ ПОДПИСЬ, КОТОРАЯ СООТВЕТСТВУЕТ СЛЕДУЮЩИМ ПРИЗНАКАМ:

A) всем вышеперечисленным;

B) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

C) позволяет определить лицо, подписавшее электронный документ;

D) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

E) создается с использованием средств электронной подписи

F) ключ проверки электронной подписи указан в квалифицированном сертификате;

G) для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным Федеральными законами;

ANSWER: A

Математическая D-схема описывается следующим набором данных:

A) множество позиций, множество переходов, входная функция, выходная функция, функция маркировки

B) алфавит входов, алфавит состояний, алфавит выходов, семейство матриц вероятностей переходов

C) алфавит входов, алфавит состояний, алфавит выходов, оператор переходов, оператор выходов

D) множество моментов времени, множество входных воздействий, множество состояний, множество выходных реакций, дифференциальное уравнение для состояний, оператор выходов

E) множество входного потока, множество состояний, множество потока обслуживания, множество выходного потока, множество внутренних параметров, алгоритм функционирования

ANSWER: D

Математическая F-схема описывается следующим набором данных:

A) множество позиций, множество переходов, входная функция, выходная функция, функция маркировки

B) алфавит входов, алфавит состояний, алфавит выходов, семейство матриц вероятностей переходов

C) алфавит входов, алфавит состояний, алфавит выходов, оператор переходов, оператор выходов

D) множество моментов времени, множество входных воздействий, множество состояний, дифференциальное уравнение для состояний, оператор выходов

E) множество входного потока, множество состояний, множество потока обслуживания, множество выходного потока, множество внутренних параметров, алгоритм функционирования

ANSWER: C

Математическая P-схема описывается следующим набором данных:

A) множество позиций, множество переходов, входная функция, выходная функция, функция маркировки

B) алфавит входов, алфавит состояний, алфавит выходов, семейство матриц вероятностей переходов

C) алфавит входов, алфавит состояний, алфавит выходов, оператор переходов, оператор выходов

D) множество моментов времени, множество входных воздействий, множество состояний, дифференциальное уравнение для состояний, оператор выходов

E) множество входного потока, множество состояний, множество потока обслуживания, множество выходного потока, множество внутренних параметров, алгоритм функционирования

ANSWER: B

Математическая Q-схема описывается следующим набором данных:

A) множество позиций, множество переходов, входная функция, выходная функция, функция маркировки

B) алфавит входов, алфавит состояний, алфавит выходов, семейство матриц вероятностей переходов

C) алфавит входов, алфавит состояний, алфавит выходов, оператор переходов, оператор выходов

D) множество моментов времени, множество входных воздействий, множество состояний, дифференциальное уравнение для состояний, оператор выходов

E) множество входного потока, множество состояний, множество потока обслуживания, множество выходного потока, множество внутренних параметров, алгоритм функционирования

ANSWER: E

Математическая N-схема описывается следующим набором данных:

A) множество позиций, множество переходов, входная функция, выходная функция, функция маркировки

B) алфавит входов, алфавит состояний, алфавит выходов, семейство матриц вероятностей переходов

C) алфавит входов, алфавит состояний, алфавит выходов, оператор переходов, оператор выходов

D) множество моментов времени, множество входных воздействий, множество состояний, дифференциальное уравнение для состояний, оператор выходов

E) множество входного потока, множество состояний, множество потока обслуживания, множество выходного потока, множество внутренних параметров, алгоритм функционирования

ANSWER: A

Основными способами задания модельного времени являются:

A) способ просмотра активностей, способ анализа списка событий, транзактный способ

B) способ просмотра активностей, способ анализа списка событий, способ на основе процессов

C) способ просмотра активностей, способ анализа списка событий, способ на основе процессов, способ на основе агрегатов

D) способ просмотра активностей, способ анализа списка событий, способ на основе процессов, способ на основе агрегатов, способ на основе транзактов

E) способ фиксированного интервала и способ особых состояния

ANSWER: E

Элементы модели системы массового обслуживания делятся на

A) активные (накопители), пассивные (источники), активно-пассивные (каналы обслуживания)

B) активные (каналы обслуживания), пассивные (источники), активно-пассивные (накопители)

C) активные (накопители), пассивные (каналы обслуживания), активно-пассивные (источники)

D) активные (источники), пассивные (каналы обслуживания), активно-пассивные (накопители)

E) активные (источники), пассивные (накопители), активно-пассивные (каналы обслуживания)

ANSWER: E

Эволюционная технологическая схема синтеза сложных систем включает этапы:

A) декомпозиции, композиции, генерации вариантов, анализа вариантов

B) генерации вариантов, моделирования и анализа эффективности вариантов, выбора вариантов

C) концептуального, функционального, информационного, конструктивного синтеза

D) концептуального, функционального, технического, конструктивного синтеза;

E) концептуального, функционального, технического, конструктивного синтеза и испытаний

ANSWER: E

При реализации моделирующего алгоритма СМО создаются следующие множества объектов:

A) массивы элементов типа К, И, Н, Т, R

B) массивы элементов типа К, И, Н,КО, ЗО

C) массивы элементов типа К, И, Н, ОЗ, ОК

D) массивы элементов типа К, И, R,ОК, ОЗ

E) массивы элементов типа К, И, Н, R

ANSWER: C

Алгоритм регламентации модельного времени предусматривает выполнение следующей последовательности действий

A) установка начального состояния системы, определение перечня обслуживаемых событий, квазипараллельная обработка событий, приращение времени, проверка условия выполнения приращения

B) определение способа задания модельного времени, определение перечня обслуживаемых событий, квазипараллельная обработка событий, приращение времени проверка условия окончания процесса моделирования

C) установка начального состояния системы, описание активностей, обработка активностей, приращение времени, проверка условия окончания процесса моделирования

D) установка начального состояния системы, определение перечня обслуживаемых событий, квазипараллельная обработка событий, приращение времени, проверка условия окончания процесса моделирования

E) установка начального события, определение перечня обслуживаемых событий, квазипараллельная обработка событий, приращение перечня событий, проверка условия окончания процесса моделирования

ANSWER: D

Выберите формулу для стандартного датчика равномерной случайной величины

A)

B)

C)

D)

E)

ANSWER: D

Выберите формулу для стандартного датчика гауссовской случайной величины

A)

B)

C)

D)

E)

ANSWER: B

Для СМО с отказами используют следующие показатели эффективности:

A) абсолютная пропускная способность; относительная пропускная способность; среднее число одновременно занятых каналов; среднее время пребывания заявки в системе; коэффициент использования каналов

B) абсолютная пропускная способность; относительная пропускная способность; среднее число одновременно занятых каналов; коэффициент использования каналов

C) относительная пропускная способность; среднее число одновременно занятых каналов; среднее время пребывания заявки в системе; коэффициент использования каналов; время пребывания заявки в очереди

D) вероятность не превышения времени ожидания заявки в очереди заданного предельного значения; среднее количество заявок в очереди и в системе в целом; среднее время пребывания заявки в очереди и в системе в целом

E) абсолютная пропускная способность; относительная пропускная способность; вероятность не превышения времени ожидания заявки в очереди заданного значения; среднее время пребывания заявки в очереди и в

системе в целом; среднее количество одновременно занятых каналов; коэффициент их использования

ANSWER: B

Для СМО с ожиданием используют следующие показатели эффективности:

A) вероятность не превышения времени ожидания заявки в очереди заданного значения; среднее количество заявок в очереди и в системе в целом; среднее время пребывания заявки в очереди и в системе в целом; среднее количество одновременно занятых каналов; коэффициент их использования

B) абсолютная пропускная способность; относительная пропускная способность; среднее время пребывания заявки в очереди и в системе в целом; среднее количество одновременно занятых каналов; коэффициент их использования

C) вероятность не превышения времени ожидания заявки в очереди заданного значения; среднее количество заявок в очереди и в системе в целом; среднее количество одновременно занятых каналов; коэффициент их использования

D) относительная пропускная способность; вероятность не превышения времени ожидания заявки в очереди заданного значения; среднее количество заявок в очереди и в системе в целом; среднее время пребывания заявки в очереди и в системе в целом; среднее количество одновременно занятых каналов; коэффициент их использования

E) среднее количество заявок в очереди и в системе в целом; среднее время пребывания заявки в очереди и в системе в целом; среднее количество одновременно занятых каналов; коэффициент их использования

ANSWER: A

При разработке имитационной модели реализуются следующие типы отношений подобия систем

A) абстрактная – физическая, физическая – абстрактная

B) физическая – абстрактная, абстрактная – физическая

C) абстрактная – абстрактная, физическая, – физическая

D) физическая – физическая, абстрактная – абстрактная

E) отношение эквивалентности

ANSWER: B

Выберите формулу для алгоритма генерации пуассоновсокго потока событий

A)

B)

C)

D)

E)

ANSWER: E

Выберите формулу для алгоритма генерации потока Эрланга общего вида

A)

B)

C)

D)

E)

ANSWER: A

Описание структуры системы массового обслуживания включает:

A) количество источников входных потоков заявок и их интенсивности; количество фаз обслуживания заявок; количество накопителей в каждой фазе;

емкости накопителей; количество каналов обслуживания в каждой фазе и интенсивности потоков обслуживания каналов; связи между элементами в виде оператора сопряжения ;дисциплины ожидания заявок в накопителях и их выбора на обслуживание в каналах; правила ухода заявок

B) количество источников входных потоков заявок; количество фаз обслуживания заявок; количество накопителей в каждой фазе; количество каналов обслуживания в каждой фазе; связи между элементами в виде оператора сопряжения

C) количество источников входных потоков заявок; количество фаз обслуживания заявок; количество накопителей в каждой фазе; емкости накопителей; количество каналов обслуживания в каждой фазе и интенсивности потоков обслуживания каналов; дисциплины ожидания заявок в накопителях и их выбора на обслуживание в каналах; правила ухода заявок

D) количество источников входных потоков заявок и их интенсивности; количество фаз обслуживания заявок; количество накопителей в каждой фазе; предельные размеры очереди накопителей; количество каналов обслуживания в каждой фазе и интенсивности потоков обслуживания каналов; дисциплины ожидания заявок в накопителях и их выбора на обслуживание в каналах; правила ухода заявок

E) количество источников входных потоков заявок; количество фаз обслуживания заявок; количество накопителей в каждой фазе; количество каналов обслуживания в каждой фазе; связи между элементами в виде оператора сопряжения; количество каналов обслуживания в каждой фазе и интенсивности потоков обслуживания каналов; дисциплины ожидания заявок в накопителях и их выбора на обслуживание в каналах; правила ухода заявок

ANSWER: B

Математическая D-схема используется для построения:

A) непрерывно-стохастических моделей

B) дискретно-детерминированных моделей

C) непрерывно-детерминированных моделей

D) дискретно-стохастических моделей

E) детерминированных моделей

ANSWER: C

Математическая F-схема используется для построения

A) непрерывно-стохастических моделей

B) дискретно-детерминированных моделей

C) непрерывно-детерминированных моделей

D) дискретно-стохастических моделей

E) комбинированных моделей

ANSWER: B

Математическая P-схема используется для построения:

A) непрерывно-стохастических моделей

B) дискретно-детерминированных моделей

C) непрерывно-детерминированных моделей

D) дискретно-стохастических моделей

E) комбинированно-гибридных моделей

ANSWER: D

Математическая N-схема используется для построения:

A) непрерывно-стохастических моделей

B) дискретно-детерминированных моделей

C) непрерывно-детерминированных моделей

D) сетевых моделей

E) моделей реактивных систем

ANSWER: D

Обязательно ли применение технических средств при проведении измерений?

A) не обязательно

B) не обязательно, но желательно

C) обязательно

ANSWER: C

Эффективная оценка – это

A) оценка, которая сходиться по вероятности к оцениваемому значению при $n \to \infty$

B) оценка, математическое ожидание которой должно быть равно оцениваемому значению

C) оценка, выборочное распределение которой должно иметь наименьшую дисперсию

ANSWER: C

Функция правдоподобия выборкиконечного объема из параметрического распределения генеральной совокупности по закону Лапласа имеет вид

A)

B)

C)

ANSWER: C

Можно ли при фиксированном количестве измерений повысить достоверность получаемого результата?

A) Нет

B) да, путем расширения доверительного интервала

ANSWER: B

Какая из форм записи интервальной оценки является стандартной?

A)

B)

C)

ANSWER: C

Относительная дисперсия погрешности мультипликативной функции равна

A) сумме дисперсий абсолютных погрешностей сомножителей

B) сумме дисперсий относительных погрешностей сомножителей

C) сумме дисперсий относительных погрешностей сомножителей с весами равными квадрату показателя степени соответствующего аргумента

ANSWER: C

Когда при определении дисперсии аддитивной функции складываются частные невзвешенные составляющие дисперсий слагаемых?

A) всегда

B) в отсутствие отрицательных членов в аддитивной функции

C) в условиях равенства единице модулей коэффициентов в слагаемых аддитивной функции

ANSWER: C

Какой из двух типов задач обработки результатов совместных измерений нескольких величин представляет собой задачу уравнивания?

A) уточнение (путем введения поправок) значений полученных результатов измерений нескольких величин при сохранении неизменным вида функциональной зависимости между ними

B) уточнения вида функциональной зависимости (значений параметров функциональной зависимости для известного класса функций) по известным значениям величин

ANSWER: A

Преобразование задачи совместных неравноточных измерений нескольких величин к равноточному виду осуществляется путем умножения каждого из N условного уравнения на коэффициент Wi , связанный с весом измерений _GI (I=1,N)_ ,следующей функциональной зависимостью:

A)

B)

C)

D)

ANSWER: C

Для зависимости выравнивающими функциями называют функции и следующего вида:

A)

B)

C)

ANSWER: B

Что такое "значение физической величины"?

A) количественное содержание свойства в каждом объекте

B) выражение размера в виде некоторого числа принятых для этой величины единиц измерения

C) число, выражающее отношение значения величины к соответствующей единице измерения

D) число, символически отражающее интенсивность некоторого свойства

ANSWER: B

Как соотносятся по величине три различные оценки в виде среднего геометрического , среднего арифметического и среднего квадратического ?

A)

B)

C)

D)

E) соотношения между различны в зависимости от результатов измерений

ANSWER: C

К какому типу критериев относится

A) к типу составных критериев

B) к типу комбинированных критериев

ANSWER: B

Определить тройку средних из множества , построенных по результатам трех измерений , для которых уравнение связи имеет вид

A)

B)

C)

D)

ANSWER: D

Какую связь устанавливает Теорема Букенгема между _M_ физическими величинами, для описания которых используется _H_ основных единиц, и числом _Q_ безразмерных комбинаций этих величин?

A)

B)

C)

D)

ANSWER: B

Необходимым и достаточным условием подобия двух объектов является

A) равенство определяющих критериев подобия

B) равенство определяющих критериев подобия и пропорциональность сходственных параметров, входящих в условия однозначности

ANSWER: B

Предусматривает ли диагностирование осуществление следующих операций:

A) определение технического состояния работоспособного объекта

B) определение технического состояния неработоспособного объекта

ANSWER: B

Кто имеет право осуществлять сертификационные испытания?

A) разработчик

B) заказчик

C) третья сторона – орган по сертификации

ANSWER: C

Что такое принцип измерения?

A) физическое явление или эффект, положенное в основу измерения

B) прием или совокупность приемов сравнения измеряемой величины с ее единицей

C) совокупность операций и правил, выполнение которых обеспечивает получение результатов с известной погрешностью

ANSWER: A

Что такое совокупные измерения?

A) проводимые одновременно измерения нескольких одноименных величин, при котором искомые значения величин определяют путем решения системы уравнений, получаемых при измерениях этих величин в различных сочетаниях

B) производимые одновременно измерения нескольких неодноименных величин для нахождения зависимости между ними

ANSWER: A

В чем заключается особенность метода замещения?

A) это метод, в котором измеряемую величину сравнивают с величиной, воспроизводимой мерой

B) это метод, в котором измеряемая величина и величина, воспроизводимая мерой, одновременно воздействуют на прибор сравнения, с помощью которого устанавливаются соотношения между этими величинами

C) это метод, в котором на измерительный прибор воздействует разность измеряемой величины и известной величины, воспроизводимой мерой

D) это метод, в котором измеряемую величину замещают известной величиной, воспроизводимой мерой

E) это метод, в котором разность между измеряемой величиной и величиной, воспроизводимой мерой, измеряют, используя совпадения отметок шкал или периодических сигналов

ANSWER: D

Соотношение v=1+3,322 lg$n$ для определения количества интервалов (v) для подсчета частости в вариационном ряду из n результатов измерений называют:

A) формулой Скотта

B) формулой Фридмана-Диакониса

C) формулой Стерджесса

ANSWER: C

При каких условиях дифференциальный эмпирический закон распределения неограниченно приближается к теоретическому?

A) всегда

B) никогда

C) при неограниченном увеличении объема выборки

D) при неограниченном уменьшении ширины интервала разбиения вариационного ряда

E) при одновременном неограниченном увеличении объема выборки и уменьшении ширины интервала разбиения вариационного ряда

ANSWER: E

ВОЗМОЖНО ЛИ ИСПОЛЬЗОВАНИЕ ОДНОВРЕМЕННО ДВУХ АГРЕГИРУЮЩИХ ФУНКЦИЙ: select min(price), max(price) from Orders

A) Да, но данный запрос составлен неверно, надо так: select * from Orders where price IN (min, max)

B) Да, в результате мы получим минимальную и максимальную стоимости

C) Да, в результате мы получим стоимости, отсортированные от минимальной к максимальной

D) Нет, две функции использовать одновременно нельзя

ANSWER: C

КАК СДЕЛАТЬ НЕСКОЛЬКО ЗАПИСЕЙ В ТАБЛИЦУ ЗА ОДИН ЗАПРОС?

A) Как сделать несколько записей в таблицу за один запрос?

B) Использовать подзапрос

C) Перечислить через запятую все наборы значений после VALUES

D) Никак

ANSWER: C

КАКИЕ ДАННЫЕ МЫ ПОЛУЧИМ ИЗ ЭТОГО ЗАПРОСА? select id, date, customer_name from Orders

A) Неотсортированные номера и даты всех заказов с именами заказчиков

B) Никакие, запрос составлен неверно

C) Номера и даты всех заказов с именами заказчиков, отсортированные по первой колонке

D) Номера и даты всех заказов с именами заказчиков, отсортированные по всем колонкам, содержащим слово Order

ANSWER: A

КАКИЕ ПОЛЯ ИЗ ТАБЛИЦЫ ОБЯЗАТЕЛЬНО ПЕРЕЧИСЛЯТЬ В INSERT ДЛЯ ВСТАВКИ ДАННЫХ?

A) Конечно все

B) Только те, у которых нет DEFAULT значения

C) Те, у которых нет DEFAULT значения и которые не имеют атрибут auto_increment

D) Все поля имеют негласное DEFAULT значения, обязательных полей в SQL нет

ANSWER: C

КАКОГО ИЗ ПЕРЕЧИСЛЕННЫХ НИЖЕ ВИДОВ JOIN НА САМОМ ДЕЛЕ НЕ СУЩЕСТВУЕТ:

A) LEFT JOIN - который выведет все записи первой таблицы, а для ненайденных пар из правой таблицы проставит значение NULL

B) RIGHT JOIN - который выведет все записи второй таблицы, а на место недостающей информации из первой таблицы проставит NULL

C) INNER JOIN - который показывает только те записи, для которых нашлись пары

D) TRUE JOIN - который выведет все верные значения

ANSWER: D

КАКОГО СТРОКОВОГО ТИПА ДАННЫХ НЕТ В SQL:

A) VARCHAR

B) STRING
C) CHAR
D) TEXT
ANSWER: B
КАКОЕ ОСНОВНОЕ ОТЛИЧИЕ ТРИГГЕРА ОТ ХРАНИМОЙ ПРОЦЕДУРЫ
A) Триггер хранится вне базы данных
B) Триггер вызывается без участия пользователя, при модификации данных
C) Триггер не позволяет производить модификацию данных
D) Ни одно из вышеперечисленного
ANSWER: B
КАКОЙ КОМАНДОЙ МОЖНО СОЗДАТЬ НОВУЮ ТАБЛИЦУ?
A) CREATE TABLE
B) MAKE TABLE
C) SET TABLE
D) Создавать таблицы можно только через интерфейс СУБД, специальной SQL команды для этого нет
ANSWER: A
КАКОЙ ОПЕРАТОР ПОЗВОЛЯЕТ ЗАДАТЬ ПОРЯДОК СОРТИРОВКИ В ВЫХОДНОМ НАБОРЕ ДАННЫХ
A) GROUP BY
B) HAVING
C) ORDER BY
D) ORDER BY
ANSWER: C
КАКОЙ ОПЕРАТОР ПОЗВОЛЯЕТ НАКЛАДЫВАТЬ УСЛОВИЯ НА РЕЗУЛЬТАТЫ АГРЕГАТНЫХ ФУНКЦИЙ
A) HAVING
B) WHERE
C) GROUP BY
D) UNION
ANSWER: A
МОЖНО ЛИ ПОМЕНЯТЬ ТИП ДАННЫХ ПОЛЯ В УЖЕ СУЩЕСТВУЮЩЕЙ ТАБЛИЦЕ
A) Да, при помощи команды ALTER
B) Да, достаточно сделать INSERT с новым типом данных
C) Нет, только пересоздать таблицу
D) Тип бывает только у таблицы, а не у поля таблицы
ANSWER: A
ВЫБЕРИТЕ КОРРЕКТНО СОСТАВЛЕННЫЙ ЗАПРОС С ФУНКЦИЕЙ GROUP BY:
A) select count(*) from Orders GROUP seller_id
B) select seller_id, count(*) from Orders GROUP seller_id
C) select seller_id, count(*) from Orders GROUP BY seller_id
D) select count(*) from Orders GROUP ON seller_id
ANSWER: C
ЕСЛИ ЗНАЧЕНИЯ В ТАБЛИЦЕ ЯВЛЯЮТСЯ АТОМАРНЫМИ ДЛЯ КАЖДОГО АТРИБУТА ТАБЛИЦЫ, Т.Е. ТАКИМИ ЗНАЧЕНИЯМИ, КОТОРЫЕ НЕ ЯВЛЯЮТСЯ МНОЖЕСТВОМ ЗНАЧЕНИЙ ИЛИ ПОВТОРЯЮЩЕЙСЯ ГРУППОЙ, ТО ТАБЛИЦА НАХОДИТСЯ В…
A) 1 нормальной форме
B) 2 нормальной форме
C) 3 нормальной форме
D) 4 нормальной форме

ANSWER: A

ОБЪЕКТ БАЗЫ ДАНЫ, СОЗДАВАЕМЫЙ С ЦЕЛЬЮ ПОВЫШЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ ОПЕРАЦИИ ПОИСКА, НАЗЫВАЕТСЯ

A) Триггер

B) Хранимая процедура

C) Индекс

D) Домен

ANSWER: C

ОПЕРАЦИЯ С БАЗОЙ ДАННЫХ, КОТОРАЯ ПЕРЕВОДИТ ЕЕ ИЗ ОДНОГО ЦЕЛОСТНОГО СОСТОЯНИЯ В ДРУГОЕ, НАЗЫВАЕТСЯ…

A) Нормализация

B) Абстракция

C) Верификация

D) Транзакция

ANSWER: D

ПОРЯДОК ВЫПОЛНЕНИЯ ОПЕРАТОРОВ AND И OR СЛЕДУЮЩИЙ:

A) Сначала выполняется AND, а затем OR

B) Сначала выполняется OR, а затем AND

C) Порядок выполнения операторов AND и OR зависит от того, какой операторов стоит первым

D) Операторы AND и OR выполняются одновременно

ANSWER: A

ЧТО ДЕЛАЕТ СПЕЦСИМВОЛ '_' В ПАРЕ С ОПЕРАТОРОМ LIKE: select * from Orders where customer_name like 'mik_';

A) Найдет все имена, которые начинаются на mik и состоят из 4 символов

B) Найдет все имена, которые начинаются на mik, вне зависимости от того, из какого количества символов они состоят

C) Найдет данные, где имя равно mik

D) Запрос составлен неверно, в паре с оператором like не используются спецсимволы

ANSWER: A

ЧТО ИЗ НИЖЕПЕРЕЧИСЛЕННОГО НЕ ЯВЛЯЕТСЯ АГРЕГАТНОЙ ФУНКЦИЕЙ

A) SUM

B) COUNT

C) DIFF

D) AVG

ANSWER: C

ЧТО НЕ ТАК С ЭТИМ ЗАПРОСОМ select id, date from Orders where seller_id = NULL

A) Все верно, запрос покажет все заказы, продавцы которых не проставлены

B) NULL нужно взять в кавычки

C) Сравнение с NULL можно проводить только с оператором IS

D) Сравнение с NULL можно проводить только с оператором ON

ANSWER: C

ЧТО ПОКАЖЕТ СЛЕДУЮЩИЙ ЗАПРОС: select * from Orders where date between '2019-01-01' and '2019-12-31'

A) Все данные по заказам, совершенным за 2019 год, за исключением 01 января 2019 года

B) Все данные по заказам, совершенным за 2019 год, за исключением 31 декабря 2019 года

C) Все данные по заказам, совершенным за 2019 год

D) Ничего, запрос составлен неверно
ANSWER: C
ЧТО ПОКАЖЕТ СЛЕДУЮЩИЙ ЗАПРОС: select id from Orders where year (date) > 2018
A) Номера заказов, сделанных до 2018 года
B) Номера заказов, сделанных в 2018 году
C) Уникальные номера заказов
D) Номера заказов, сделанных после 2018 года
ANSWER: D
ЧТО ТАКОЕ JOIN:
A) Операция объединения
B) Операция группировки
C) Операция суммирования
D) Операция создания
ANSWER: A
ВЫБЕРИТЕ ПРАВИЛЬНЫЙ ПРИМЕР ЗАПРОСА С ИСПОЛЬЗОВАНИЕМ UNION:
A)
select id, city from Orders order by id union select id, city from Sellers order by city;
B)
select id, city, seller_id from Orders and select city, id from Sellers order by id;
C) select id, city from Orders union select id, city from Sellers order by id;
D) Все запросы верные
ANSWER: C
ЧТО ТАКОЕ АГРЕГАТНЫЕ ФУНКЦИИ:
A) Функции, которые фильтруют значения
B) Функции, которые сортируют значения
C) Функции, которые работают с набором данных, превращая их в одно итоговое значение
D) Функции, которые суммируют все значения
ANSWER: C
ЧТО ТАКОЕ РЕЛЯЦИОННЫЕ БАЗЫ ДАННЫХ:
A) База данных, в которой информация хранится в виде двумерных таблиц, связанных между собой
B) База данных, в которой одна ни с чем не связанная таблица
C) Любая база данных - реляционная
D) Совокупность данных, не связанных между собой
ANSWER: A
ВЫБЕРИТЕ ПРАВИЛЬНЫЙ ПРИМЕР ИСПОЛЬЗОВАНИЯ ФУНКЦИИ ОКРУГЛЕНИЯ ROUND
A) select id, price * discount AS total price from Orders ROUND (2);
B) select id, price * discount ROUND (2) AS total price from Orders;
C) select id, ROUND (price * discount, 2) AS total price from Orders;
D) Нет правильного примера
ANSWER: C
ВЫБЕРИТЕ ПРИМЕР ПРАВИЛЬНО СОСТАВЛЕННОГО ЗАПРОСА С ИСПОЛЬЗОВАНИЕМ АГРЕГИРУЮЩЕЙ ФУНКЦИИ SUM:
A) select sum(price) from Orders
B) select sum(price), customer_name from Orders
C) select * from Orders where price=sum()
D) select sum() from Orders group by price desc
ANSWER: A

ЕСТЬ ЛИ ОШИБКА В ЗАПРОСЕ:select id, date, customer_name from Orders where customer_name = Mike

A) Запрос составлен правильно
B) Mike необходимо записать в кавычках 'Mike'
C) Нужно убрать лишние поля из запроса
D) Нужно убрать лишние поля из запроса
ANSWER: B

ЗАЧЕМ СУЩЕСТВУЕТ КОМАНДА UPDATE, ЕСЛИ МОЖНО СНАЧАЛА УДАЛИТЬ ЗАПИСЬ, А ПОТОМ ДОБАВИТЬ НОВУЮ, ИСПРАВЛЕННУЮ

A) Именно так и делаю, UPDATE не использую
B) Так меньше нагрузки на базу, ведь команда одна, а не две
C) Потому что в записи могут быть автоматически проставляемые поля, такие как auto_increment или timestamp, которые собьются при внесении записи заново
D) Как раз удалять записи в SQL нельзя, вместо этого используется UPDATE с NULL-значениями для всех полей
ANSWER: C

КАК ВЫГЛЯДИТ ЗАПРОС, ДЛЯ ВЫВОДА ВСЕХ ЗНАЧЕНИЙ ИЗ ТАБЛИЦЫ ORDERS:

A) select * from Orders
B) select % from Orders
C) select ALL from Orders
D) select *.Orders from Orders
ANSWER: A

КАК ПОЛУЧИТЬ ЗНАЧЕНИЕ ТЕКУЩЕГО ГОДА В SQL?

A) select GetDate()
B) select year()
C) select year from Date
D) select year(GateDate())
ANSWER: D

Входят ли ограничения целостности в определение реляционной модели данных?

A) да
B) нет
ANSWER: A

Что понимается под ссылочной целостностью?

A) ограничения на допустимые значения внешнего ключа
B) ограничения на допустимые значения первичного ключа
C) ограничения на допустимые значения альтернативного ключа
ANSWER: A

Может ли внешний ключ являться потенциальным ключом?

A) нет
B) да
ANSWER: B

Какое понятие шире?

A) потенциальные ключи
B) первичные ключи
ANSWER: A

Сколько операций нарушают ссылочную целостность?

A) 3
B) 5
C) 4
D) 6

ANSWER: C

Сколько основных вариантов действий для обеспечения целостности данных

A) 3

B) 5

C) 2

ANSWER: C

Какой модели в структурном подходе к созданию БД соответствует объектно-ориентированная модель поведения (диаграмма прецедентов)?

A) функциональная модель

B) информационная модель

C) событийная модель

ANSWER: A

Могут ли атрибуты первичного ключа принимать значение NULL?

A) да

B) нет

ANSWER: B

При установлении неидентифицирующей связи между сущностями в модели IDEF1X

A) обе сущности независимые

B) одна сущность независимая, другая зависимая

ANSWER: A

Какие операции не нарушают ссылочной целостности?

A) вставка кортежа в родительское отношение

B) вставка кортежа в дочернее отношение

C) удаление кортежа в родительском отношении

D) удаление кортежа в дочернем отношении

ANSWER: D

Какие операции разрешаются при обновлении кортежа в родительском отношении?

A) ограничить

B) каскадировать

C) установить в NULL

D) установить по умолчанию

ANSWER: D

Сколькими свойствами обладает защищенная система с БД?

A) 4

B) 3

C) 5

ANSWER: B

На сколько типов делятся иерархии категорий в модели IDEF1X?

A) 3

B) 5

C) 2

ANSWER: C

Сколько основных функций реализуется в средствах поддержки доступности современных СУБД?

A) 2

B) 5

C) 3

ANSWER: C

Какая операция не используется при вставке кортежа в дочернее отношение?

A) ограничить

B) каскадировать
C) установить в NULL
D) установить по умолчанию
ANSWER: B

Операторы языка SQL GRANT и REVOKE предназначены для организации
A) дискреционной защиты
B) мандатной защиты
C) ролевой защиты
ANSWER: A

Каким ключевым словом задается ограничение таблицы в синтаксисе языка SQL?
A) CHECK
B) UNIQUE
C) CONSTRAINT
ANSWER: C

Уровень безопасности пользователя равен уровню безопасности таблицы БД. Какие операции пользователь может осуществлять над таблицей?
A) чтения
B) записи
ANSWER: B

Сколько фаз включает этап проектирования безопасных баз данных?
A) 5
B) 3
C) 2
ANSWER: B

Какая из моделей баз данных не зависит от любых физических аспектов реализации?
A) логическая
B) концептуальная
C) физическая
ANSWER: B

На сколько групп разделяют ограничения целостности БД?
A) 3
B) 5
C) 4
ANSWER: C

Какими свойствами обладает потенциальный ключ отношения БД?
A) уникальность
B) неизбыточность
C) потенциальная непротиворечивость
ANSWER: B

Сколько этапов в процессе создания защищенных систем с базами данных?
A) 3
B) 5
C) 4
ANSWER: C

Какой модели в объектно-ориентированном подходе к созданию БД соответствует структурная информационная модель «сущность-связь»?
A) модель поведения (диаграмма прецедентов)
B) модель состояний (диаграмма классов)
C) модель изменения состояний (диаграмма состояний)

ANSWER: B

К какому подходу проектирования БД относится нормализация?

A) нисходящему

B) восходящему

ANSWER: B

Сколько классов защищенности АС от НСД к информации устанавливают Руководящие документы (РД) Гостехкомиссии (ГТК) России?

A) 7

B) 9

C) 6

ANSWER: B

Требуется ли наличие администратора безопасности в классе 2Б?

A) да

B) нет

C) такого требования не предусмотрено

ANSWER: C

Какого класса СВТ должны использоваться для класса защищенности АС 1А

A) не ниже 3

B) не ниже 2

C) не ниже 4

ANSWER: B

Сколько классов защищенности СВТ от НСД к информации содержит первая группа?

A) 5

B) 3

C) 1

D) 2

ANSWER: C

Сколько классов защищенности СВТ от НСД к информации устанавливают руководящие документы ГТК (ФСТЭК) России:

A) 5

B) 10

C) 12

D) 7

ANSWER: D

Какой показатель защищенности СВТ используется для оценки только одного класса защищенности СВТ от НСД?

A) тестирование

B) гарантии проектирования

C) гарантии архитектуры

D) целостность

ANSWER: C

Чем характеризуется вторая группа классов защищенности СВТ от НСД к информации

A) мандатной защитой

B) дискреционной защитой

ANSWER: B

Сколько классов защищенности СВТ от НСД характеризуется верификационной защитой?

A) 4

B) 3

C) 1

D) 2

ANSWER: C

Какого класса защищенности СВТ от НСД должны использоваться при разработке АС по требованиям класса защищенности АС от НСД 1В?

A) не ниже 4

B) не ниже 3

C) не ниже 2

ANSWER: A

Сколько классов защищенности межсетевых экранов (МЭ) устанавливают руководящие документы Гостехкомиссии (ФСТЭК) России?

A) 4

B) 5

C) 7

ANSWER: B

Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 1Д с внешней средой?

A) 2

B) 4

C) 5

ANSWER: C

Сколько классов защищенности в соответствии с РД ГТК России включает первая группа?

A) 3

B) 6

C) 5

ANSWER: C

Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 1Б с внешней средой?

A) 2

B) 4

C) 3

ANSWER: A

Должен ли понижаться класс защищенности АС, полученной из исходной путем добавления в нее МЭ?

A) нет

B) да

C) РД не определено

ANSWER: A

Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 3Б с внешней средой?

A) не ниже 2

B) не ниже 3

C) не ниже 5

ANSWER: C

Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 3А с внешней средой при обработке информации с грифом “секретно”?

A) не ниже 2

B) не ниже 3

C) не ниже 5

ANSWER: B

Какой класс защищенности МЭ применяется для безопасного взаимодействия АС класса 2А с внешней средой при обработке информации с грифом “особой важности”?

A) не ниже 2

B) не ниже 1
C) не ниже 4
ANSWER: B

Сколько показателей защищенности используется для оценки классов защищенности МЭ?
A) 7
B) 12
C) 9
D) 10
ANSWER: B

Сколько показателей защищенности используется для оценки 5 класса защищенности МЭ?
A) 7
B) 12
C) 9
D) 10
ANSWER: C

Сколько показателей защищенности используется для оценки 4 класса защищенности МЭ?
A) 7
B) 12
C) 9
D) 10
ANSWER: D

В соответствии с РД ГТК России в классах защищенности какой группы пользователи имеют доступ ко всей информации?
A) 1
B) 2
C) 3
ANSWER: C

К какой группе защищенности АС от НСД к информации следует отнести АС, в которой работает один пользователь?
A) 1
B) 2
C) 3
ANSWER: C

Сколько подсистем включает СЗИ НСД в соответствии с РД ГТК России?
A) 5
B) 3
C) 4
ANSWER: C

К какой подсистеме СЗИ НСД относится функция управления потоками информации?
A) криптографическая подсистема
B) подсистема регистрации и учета
C) подсистема обеспечения целостности
D) ни к какой
ANSWER: D

В каком классе защищенности АС от НСД в соответствии с РД ГТК России предъявляются требования к криптографической подсистеме?
A) 2А
B) 2Б
C) 3А
D) 1Д

ANSWER: A

В соответствии с РД ГТК России требования к какому классу защищенности АС от НСД сильнее?

A) 3A

B) 2Б

C) сравнивать нельзя

ANSWER: B

Начиная с какого класса защищенности АС от НСД в соответствии с РД ГТК России тестирование СЗИ НСД должно осуществляться не реже одного раза в квартал?

A) 2A

B) 1B

C) 3A

D) 1Б

ANSWER: D

В классы моделей представления знаний НЕ входят:

A) Продукционные модели

B) Семантические сети

C) Формальные логические модели

D) Формы

ANSWER: D

[ГА-1]Что представлено на рисунке?

A) Оператор мутации в генетических алгоритмах, реализующий инверсию

B) Варианты кодирования текстовых строк

C) Пример сравнения строк на схожесть

ANSWER: A

Что представлено на рисунке?

A) Операция скрещивания строк в генетических алгоритмах (одноточечный оператор кроссовера)

B) Операция кодирования информации

C) Правило булевой логики

ANSWER: A

Формальная модель представления знаний, представленная в виде графа и позволяющая описывать субъективное восприятие человеком или группой людей какого-либо сложного объекта, проблемы или функционирования системы, – это

A) Семантическая сеть

B) Гипертекст

C) Логические формулы

ANSWER: A

В теории нечетких множеств характеристическая функция называется:

A) Степенью принадлежности

B) Функцией принадлежности

C) Срезом

D) Ядром

ANSWER: B

Если число A разложить на два слагаемых u1 и u2, то какое наибольшее значение может принять произведение u1.u2?

A) 4A2

B) 2A

C) A2/4

D) A-1

ANSWER: C

Решить задачу _I_(_u_)=u12 - u1u2 + u22 - 2u1 + u2 → inf
A) 0
B) -1
C) -3
D) 2
ANSWER: B
Решить задачу 4u1 + 3u2 → _inf_ при ограничении u12+u22=1.
A) 45
B) -3
C) -5
D) 0
ANSWER: C
Решить задачу u12 + u22 → _inf _ при ограничении 3u1+4u2=1.
A) 0
B) 1/3
C) -78
D) 1/25
ANSWER: D
Решить задачу
A) -12
B) 36
C) -4
D) 0,8
ANSWER: C
К МЕТОДАМ АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТНОСЯТ
A) Метод экспериментов
B) Статический метод
C) Динамический метод
D) Все предложенные выше методы
ANSWER: D
ОВЕРЛЕЙНАЯ ПРОГРАММА ЭТО:
A) которая полностью размещается в оперативной памяти
B) которая размещает в оперативной памяти только фрагменты кода, которые выполняются в данный момент
C) которая не использует для запуска оперативную память
D) которая полностью размещается в файле подкачки
ANSWER: B
КОНСОЛЬНАЯ ПРОГРАММА ИМЕЕТ:
A) одну точку входа
B) две точки входа
C) три точки входа
D) не имеет точек входа, точку входа имеет только программа с графическим интерфейсом
ANSWER: A
СИСТЕМНЫЙ ОТЛАДЧИК ИСПОЛЬЗУЕТСЯ ДЛЯ:
A) анализа консольных программ
B) анализа кода, выполняющегося в режиме ядра
C) анализа кода графических программ
D) такого отладчика не существует
ANSWER: B
ЯДЕРНЫЙ ОТЛАДЧИК ИСПОЛЬЗУЕТСЯ ДЛЯ:
A) анализа консольных программ
B) анализа кода, выполняющегося в режиме ядра
C) анализа кода графических программ

D) такого отладчика не существует
ANSWER: D
ГРАФИЧЕСКИЙ ОТЛАДЧИК ИСПОЛЬЗУЕТСЯ ДЛЯ:
A) анализа консольных программ
B) анализа кода, выполняющегося в режиме ядра
C) анализа кода графических программ
D) такого отладчика не существует
ANSWER: D
МЕТОД ВКЛЮЧЕНИЯ СРЕДСТВ ЗАЩИТЫ ОТ АНАЛИЗА В ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:
A) встроенная защита
B) пристыковочная защита
C) встроенная и пристыковочная защиты
D) ничего из вышеперечисленного
ANSWER: C
ДИНАМИЧЕСКОЕ ИЗМЕНЕНИЕ КОДА ПРОГРАММЫ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО:
A) код программы, за исключением распаковщика, хранится в исполняемом файле в искаженном виде, а преобразуется к нормальному в оперативной памяти
B) код программы, за исключением распаковщика, хранится в исполняемом файле в нормальном виде, преобразуется к искаженному в оперативной памяти
C) код программы, за исключением распаковщика, хранится в исполняемом файле в нормальном виде, в оперативной памяти по коду каждый раз генерится разный ассемблерный код
D) код программы может храниться только в оперативной памяти
ANSWER: A
МЕТОД ИСКУССТВЕННОГО УСЛОЖНЕНИЯ ПРОГРАММЫ:
A) использует обычную команду call для передачи управления из одной функции в другую
B) не использует обычную команду call для передачи управления из одной функции в другую
C) генерирует пустые функции в которые передается управления с помощью команды call
D) генерирует пустые функции в которые передается управления с помощью команды отличной от call
ANSWER: B
ОБРАЩЕНИЕ К СИСТЕМНЫМ ФУНКЦИЯМ ИЗ ПРОГРАММЫ МОЖЕТ ПРОИСХОДИТЬ ПОСРЕДСТВОМ:
A) динамического импорта
B) статического импорта
C) мы не можем использовать системные функции , так как они инкапсулированы
D) динамический и статический импорт
ANSWER: D
ИСКУССТВЕННОЕ УСЛОЖНЕНИЕ АЛГОРИТМА ОБРАБОТКИ ДАННЫХ ЗАКЛЮЧАЕТСЯ В:
A) многократное копирование данных с места на место
B) создание большого количества копий одних и тех же данных
C) применение к данным сложных преобразований
D) все из вышеперечисленного
ANSWER: D
МЕТОД ЭКСПЕРИМЕНТОВ С «ЧЕРНЫМ ЯЩИКОМ»:

A) подразумевает решение задачи построения автомата, эквивалентного данному на основе анализа его входа и выхода

B) метод проб и ошибок, так как основной функционал не описан и является для нас «черным ящиком»

C) такого метода не существует

ANSWER: A

В БОЛЬШИНСТВЕ СЛУЧАЕВ ВЗАИМОДЕЙСТВИЕ ПРОГРАММНОЙ ЗАКЛАДКИ С АТАКУЕМОЙ КОМПЬЮТЕРНОЙ СИСТЕМОЙ ОПИСЫВАЕТСЯ С ПОМОЩЬЮ ФОРМАЛЬНОЙ МОДЕЛИ:

A) наблюдатель

B) перехват

C) искажение

D) все из вышеперечисленного

ANSWER: D

МОДЕЛЬ НАБЛЮДАТЕЛЬ ПРИМЕНЯЕТСЯ ДЛЯ:

A) внедрения других программных закладок

B) анализ сетевого трафика

C) такой модели не существуе

ANSWER: A

В РОЛИ ОБЪЕКТА В МОДЕЛИ ПЕРЕХВАТ ВЫСТУПАЕТ:

A) клавиатура, файловые системы, физические и логические устройства сети

B) оперативная память, центральный процессор

C) такой модели не существует

ANSWER: A

В МОДЕЛИ ИСКАЖЕНИЕ:

A) программная закладка встраивается в программное обеспечение, обслуживающее сетевые потоки определенного класса

B) программная закладка встраивается в программное обеспечение, обслуживающее информационные потоки определенного класса

C) такой модели не существует

ANSWER: B

ТИПИЧНЫЕ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ:

A) переполнение буферов

B) отсутствие необходимых проверок входных данных

C) другое

D) переполнение буферов и отсутствие необходимых проверок входных данных

ANSWER: D

ВИРУС:

A) программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, компьютерных сетей, осуществлять деструктивные действия

B) программа для уничтожения информации в компьютерной системе

C) программа для утечки информации в компьютерной системе

D) программа для искажения информации в компьютерной системе

ANSWER: A

АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ ОНЛАЙН-ВИРУСА ВКЛЮЧАЕТ В СЕБЯ:

A) сканирование ip-адреса жертвы

B) сканирование серийного номера сетевого устройства

C) сканирование ip-адреса жертвы только в протоколе ipv4, так как в ipv6 данная уязвимость была закрыта

ANSWER: A

СИГНАТУРНОЕ СКАНИРОВАНИЕ:

A) поиск в файлах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов

B) поиск в файловых системах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов

C) поиск в операционных системах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов

D) поиск в браузерах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов

ANSWER: A

ЕСЛИ ИЗВЕСТНА ДЛИНА ТЕЛЕ ВИРУСА И ЗНАЧЕНИЯ НЕКОТОРЫХ БАЙТОВ ТЕЛА ВИРУСА, ТО ПРИЗНАКАМИ ЗАРАЖЕНИЯ ФАЙЛА ЯВЛЯЮТСЯ:

A) наличие в первых байтах проверяемого файла команды перехода на адрес длина_файла — длина_тела_вируса

B) наличие в конце проверяемого файла определенных байт

C) все из вышеперечисленного

D) ничего из вышеперечисленного

ANSWER: C

ЭВРИСТИЧЕСКОЕ СКАНИРОВАНИЕ:

A) поиск сигнатур, типичных не для конкретных образцов компьютерных вирусов и(или) программных закладок, а для вредоносного программного обеспечения вообще

B) поиск сигнатур, не типичных не для конкретных образцов компьютерных вирусов и(или) программных закладок, а для вредоносного программного обеспечения вообще

C) поиск сигнатур, не типичных для конкретных образцов компьютерных вирусов

D) поиск сигнатур, не типичных для конкретных образцов к программных закладок

ANSWER: A

ПРИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ АЛГОРИТМОВ ДИЗАССЕМБЛИРОВАНИЯ ВОЗНИКАЮТ СЛЕДУЮЩИЕ ПРОБЛЕМЫ:

A) проблема восстановления символических имен

B) проблема различения программ и данных

C) проблема определения границы машинной команды

D) все описанные проблемы

ANSWER: D

КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОСУЩЕСТВЛЯЕТСЯ ЗА СЧЕТ:

A) хранения длины файла

B) хранения контрольной суммы

C) хранения длины файла и контрольной суммы

D) закрытия исходного кода файла криптографическими протоколами

ANSWER: C

ДИНАМИЧЕСКИЙ МЕТОД АНАЛИЗА ПРОГРАММНЫХ РЕАЛИЗАЦИЙ:

A) основан на использовании программных отладочных средств

B) использует оперативную память как динамическую систему для анализа

C) использует в качестве анализа BIOS

D) ничего из вышеперечисленного не верно

ANSWER: A

ОТЛАДЧИК ЭТО:

A) программа, которая загружает в память другую программу и предоставляет пользователю возможность наблюдать за ходом выполнения этой программы

B) программа, которая предоставляет пользователю возможность наблюдать за ходом выполнения запущенных процессов в операционной системе, но сама ничего не загружает

C) программа для загрузки других программ в память

ANSWER: A

ФЛАГ ТРАССИРОВКИ:

A) когда равен 1, процессор после выполнения каждой машинной команды вызывает прерывание 5

B) когда равен 1, процессор после выполнения каждой машинной команды вызывает прерывание 48

C) когда равен 1, процессор после выполнения каждой машинной команды вызывает прерывание 1

D) такого флага не существует

ANSWER: C

В АНАЛИЗ ПРОГРАММЫ МЕТОДИЧЕСКИМ МЕТОДОМ ВКЛЮЧАЕТСЯ:

A) поиск подходов к интересующим функциям программы

B) поиск интересующих функций программы

C) анализ интересующих функций программы

D) все из вышеперечисленного

ANSWER: D

В МЕТОДЕ МАЯКОВ, МАЯКИ ЭТО:

A) точки входа в программу для анализа

B) точки выхода из программы

C) точки программы, в которых программа выполняет действия, легко понимаемые без знания контекста, в котором эти действия выполняются

D) точки программы, в которых программа выполняет действия, не понимаемые без знания контекста, в котором эти действия выполняются

ANSWER: C

МЕТОД STEP-TRACE МОЖЕТ БЫТЬ ИСПОЛЬЗОВАН ДЛЯ ПОИСКА В ПРОГРАММЕ ФУНКЦИИ X, ДЛЯ КОТОРОЙ ВЫПОЛНЯЕТСЯ УСЛОВИЕ:

A) реализует интересующие аналитика алгоритмы

B) легко обнаруживается по внешним проявлениям программы

C) может быть запущена в режиме Step (пошагово)

D) реализует интересующие аналитика алгоритмы и легко обнаруживается по внешним проявлениям программы

ANSWER: D

ЧТО ОЗНАЧАЕТ ШЕСТЬ КОРОТКИХ СИГНАЛОВ?

A) Ошибок не обнаружено, ПК исправен

B) Проблемы с блоком питания

C) Неисправность оперативной памяти

D) Неисправность контроллера клавиатуры

ANSWER: D

КАТАЛОГ /ETC СОДЕРЖИТ

A) Загрузочные файлы

B) Файлы пользователей

C) Конфигурационные файлы

D) Файлы устройств

E) Исполняемые файлы

F) Каталоги для монтирования временных файловых систем

ANSWER: C

КАТАЛОГ /MNT СОДЕРЖИТ

A) Загрузочные файлы

B) Файлы пользователей

C) Конфигурационные файлы

D) Файлы устройств
E) Исполняемые файлы
F) Каталоги для монтирования временных файловых систем
ANSWER: F
КАТАЛОГ /BIN СОДЕРЖИТ
A) Загрузочные файлы
B) Файлы пользователей
C) Конфигурационные файлы
D) Файлы устройств
E) Исполняемые файлы
ANSWER: E
КАТАЛОГ /SBIN СОДЕРЖИТ
A) Конфигурационные файлы
B) Файлы пользователей
C) Системные исполняемые файлы
D) Файлы устройств
E) Загрузочные файлы
F) Каталоги для монтирования временных файловых систем
ANSWER: C
ФАЙЛ /ETC/LILO.CONF СОДЕРЖИТ
A) Параметры настройки видеосистемы
B) Параметры начальной загрузки
C) Меню начальной загрузки
D) Путь к ядру операционной системы
ANSWER: B
ЧТОБЫ ИЗМЕНИТЬ РАЗМЕР ФАЙЛА ПОДКАЧКИ В WINDOWS, НЕОБХОДИМО РЕДАКТИРОВАТЬ ПАРАМЕТРЫ:
A) Загрузка и восстановление
B) Быстродействие
C) Переменные среды
D) Профили пользователей
ANSWER: B
С ЧЕМ ОБЫЧНО СВЯЗАНО ВОЗНИКАЮЩЕЕ В ПРОЦЕССЕ ДЛИТЕЛЬНОЙ ЭКСПЛУАТАЦИИ УВЕЛИЧЕНИЕ ВРЕМЕНИ ОТВЕТА ОС WINDOWS:
A) С необходимостью очистки системного блока от пыли
B) С ростом размера системного реестра
C) С уменьшением объема свободного места на системном диске
ANSWER: B
КАК НАЗЫВАЕТСЯ ТЕХНОЛОГИЯ УПРАВЛЕНИЯ РАСПРЕДЕЛЕННЫМИ СИСТЕМАМИ ОТ CISCO SYSTEMS, COMPAQ COMPUTER, INTEL И MICROSOFT , ПОЗВОЛЯЮЩАЯ РЕШАТЬ ТАКИЕ ЗАДАЧИ КАК УПРАВЛЕНИЕ ОС WINDOWS, УПРАВЛЕНИЕ РЕСУРСАМИ И СЛУЖБАМИ СЕТИ, МОНИТОРИНГ СОСТОЯНИЯ СИСТЕМЫ В РЕАЛЬНОМ ВРЕМЕНИ:
A) CIM (Common Information Model)
B) WBEM (Web-Based Enterprise Management)
C) WMI (Windows Management Instrumentation)
ANSWER: C
НА ОСНОВЕ КАКОЙ ОПЕРАЦИОННОЙ СИСТЕМЫ БЫЛА РАЗРАБОТАНА СИСТЕМА ANDROID:
A) Linux
B) MiniX
C) Windows iOS
ANSWER: A

КАК НАЗЫВАЕТСЯ РЕЖИМ ИСПОЛЬЗОВАНИЯ ANDROID-СИСТЕМЫ С МАКСИМАЛЬНЫМИ ПРАВАМИ (АНАЛОГ АДМИНИСТРАТОРА WINDOWS):

A) Суперпользователь

B) Root-Home пользователь Android

C) user

D) Up-User

ANSWER: A

ЧТО НЕ ЯВЛЯЕТСЯ ХАРАКТЕРНОЙ ЧЕРТОЙ RISC-АРХИТЕКТУРЫ:

A) Использование компиляторов, оптимизирующих работу конвейера машинных команд

B) В состав процессора включают расширенный набор регистров

C) Серьезное внимание должно быть уделено командам условного перехода

D) В процессорах можно использовать сокращенный набор команд

ANSWER: C

КАКАЯ АРХИТЕКТУРА ОС ИМЕЕТ ТАКОЙ НЕДОСТАТОК, КАК СНИЖЕНИЕ ЭФФЕКТИВНОСТИ РАБОТЫ ПО СРАВНЕНИЮ С РЕАЛЬНЫМ КОМПЬЮТЕРОМ, И, КАК ПРАВИЛО, ОНИ ОЧЕНЬ ГРОМОЗДКИ

A) Монолитное ядро

B) Многоуровневая ОС

C) Смешанная ОС

D) Виртуальная машина

ANSWER: D

КАКОЙ ИЗ ВНЕШНИХ ИНТЕРФЕЙСОВ ОБЛАДАЕТ ПЕРВОНАЧАЛЬНОЙ СКОРОСТЬЮ 850 МБИТ/С:

A) Параллельный порт (LPT)

B) Fire Wire

C) Последовательный порт (RS 323)

D) Fire Wire 800

E) USB 2.0

ANSWER: D

ОСНОВНЫМ ПРИЗНАКОМ КАКИХ СИСТЕМ ЯВЛЯЕТСЯ НАЛИЧИЕ ВЕКТОРНО-КОНВЕЙЕРНЫХ ПРОЦЕССОРОВ?

A) PVP-систем

B) NUMA-систем

C) SMP-систем

ANSWER: A

ПРЕИМУЩЕСТВА АРХИТЕКТУРЫ МИКРОЯДРА ОПЕРАЦИОННОЙ СИСТЕМЫ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО

A) Повышается скорость работы приложений

B) Эффективнее расходуются ресурсы системы

C) Ядро становится более надежное

ANSWER: C

АЛГОРИТМ ВЫБОРКИ ПО ТРЕБОВАНИЮ С КЛАСТЕРИЗАЦИЕЙ ПОЗВОЛЯЕТ

A) Загрузить требуемую в данный момент страницу и не загружать расположенные рядом с ней

B) Загрузить требуемую в данный момент страницу и расположенные рядом с ней

C) Загрузить требуемую в данный момент страницу

D) Упреждающе загружать страницу, которая потребуется в ближайшее время

E) Упреждающе загружать

ANSWER: B

КОМАНДА ОС UNIX: PS
A) Отображает содержимое текущего каталога
B) Позволяет завершить выполняющийся процесс
C) Отображает перечень запущенных процессов
D) Позволяет создать символическую связь
ANSWER: C
ВЕТВЬ РЕЕСТРА - HKEY_CLASSES_ROOT СОДЕРЖИТ
A) Информацию об аппаратных средствах компьютера
B) Ассоциации по типам файлов и данные по ярлыкам
C) Информацию об программном обеспечении
D) Информацию о пользователях
ANSWER: B
ВЕТВЬ РЕЕСТРА - HKEY_CURRENT_CONFIG СОДЕРЖИТ
A) Информацию о текущем аппаратном профиле
B) Информацию об программном обеспечении
C) Информацию о пользователях
D) Ассоциации по типам файлов и данные по ярлыкам
ANSWER: A
Возможности (capabilities) потоков в Linux позволяют
A) Разделить возможности суперпользователя на несколько отдельных возможностей, которые могут быть разрешены независимо на уровне потока
B) Ограничить использование потоком процессорного времени
C) Разрешить прямой доступ к объектам ядра
ANSWER: A
В MS Windows под термином олицетворение (impersonation) понимают
A) Возможность выполнения потока в контексте безопасности, отличном от контекста безопасности своего процесса
B) Возможность идентифицировать владельца потока
C) Возможность удаленного запуска потока с использованием механизма RPC
ANSWER: A
Контроль учетных записей (User Account Control, UAC) в MS Windows реализует
A) Механизм защиты от вредоносных программ
B) Ограничение срока действия учетной записи
C) Контроль уровеня доверия к учетной записи
ANSWER: A
При одновременном присутствии в списке контроля доступа разрешающей и запрещающей записи по одному и тому же виду доступа для одного и того же субъекта доступа в современных реализациях ОС MS Windows
A) Запрещающая запись имеет приоритет
B) Разрешающая запись имеет приоритет
C) Поведение системы не определено
ANSWER: A
В UNIX-подлобных системах Sticky-bit (атрибут T) установленный для каталога имеет следующее действие
A) Не оказывает никакого действия для каталогов в современных реализациях операционных систем
B) Для новых файлов группой-владельцем становится группа-владелец каталога
C) Пользователь может удалять из каталога только файлы, которыми он владеет
D) Файлы из каталога нельзя объявить исполняемыми

ANSWER: C

В UNIX-подобных системах при вычислении хэша пароля используется дополнительный открытый ключ (соль), применение которого обеспечивает

A) Генерацию разного хэша для одинаковых паролей

B) Увеличение числа вариантов пароля

ANSWER: A

В UNIX-подобных системах атрибут разрешение исполнения (x) применительно к каталогу разрешает

A) Получить список имен файлов из каталога

B) Создавать файлы в каталоге

C) Удалять файлы в каталоге

D) Переходить в каталог

ANSWER: D

Для проверки подлинности данных, полученных через открытый канал или хранимых в ненадежном хранилище, может быть использован алгоритм

A) HMAC – hash-based message authentication code

B) HOTP – HMAC-Based One-Time Password Algorithm

C) TOTP – Time-based One-Time Password Algorithm

ANSWER: A

Политика безопасности это

A) Набор правил, регламентирующих порядок хранения и обработки информации

B) Перечень требуемых программ технической защиты информации и их настроек

C) Список ограничений на действия пользователей

ANSWER: A

Встроенный программный межсетевой экран в Linux и MS Windows обеспечивает

A) Фильтрацию сетевого трафика в соответствии с заданными правилами для предотвращения возможности использования злоумышленником уязвимостей сетевых протоколов и программного обеспечения

B) Шифрование и контроль целостности пакетов в сетевом трафике для защиты от подмены данных

ANSWER: A

Оценочный уровень доверия 1 обеспечивает

A) Минимальный уровень доверия, который подтверждает только наличие в составе ОС некоторых средств защиты

B) Уровень доверия от невысокого до умеренного, достигаемый при отсутствии доступа к полной документации по разработке ОС, основанный на анализе структуры ОС с использованием полученной от разработчика ОС дополнительной информации.

C) Умеренный уровень доверия, основанный на всестороннем методическом исследовании функций безопасности и процесса разработки ОС

D) Уровень доверия от умеренного до высокого в отношении уже существующей ОС общего назначения, основанный на всестороннем методическом тестировании и проверке реализации функций безопасности ОС, на уверенности в правильном использовании типовых методов при проектирования ОС.

E) Высокий уровень доверия для разрабатываемой ОС, основанный на использовании полуформальных методов при проектировании и тестировании ОС.

F) Уверенность в безопасности ОС при работе в условиях высокого риска, где ценность защищаемых данных оправдывает дополнительные

затраты, основанную на использовании полуформальных методов при верификации и тестировании ОС

G) Уверенность в безопасности ОС при работе в условиях чрезвычайно высокого риска, где высокая ценность защищаемых данных оправдывает повышенные затраты, основанную на использовании формальных методов при верификации и тестировании ОС

ANSWER: A

Оценочный уровень доверия 4 (Наиболее высокий уровень доверия, достижимый при оценке существующих ОС общего назначения, так как боле высокий уровень доверия требует вмешательства в разработку ОС) обеспечивает

A) Некоторую уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией (в процессе реализации не были внесены неучтенные изменения)

B) Уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией

C) Высокую уверенность в том, что подсистема безопасности ОС реализована в соответствии с предъявляемыми требованиями

ANSWER: B

Переход от монолитной архитектуры ядра к модульному ядру

A) Упрощает добавление в ядро новых функций

B) Повышает защищенность операционной системы

C) Существенно снижает производительность

D) Существенно повышает производительность

ANSWER: A

Кэш системы трансляции адресов (TLB) позволяет

A) Сократить время, затрачиваемое на преобразование виртуального адреса в физический

B) Сэкономить место в памяти

C) Расширить объем виртуального адресного пространства

D) Защитить данные в памяти

ANSWER: A

Семафор это объект операционной системы, позволяющий

A) Реализовать ожидание процессами момента наступления запланированных событий

B) Исключить взаимную блокировку процессов

C) Обеспечить соблюдение приоритетов

D) Прервать выполнение процесса при ошибке

ANSWER: A

Критическая секция программного кода это

A) Участок кода программы, из которого выполняются действия с критическим ресурсом (ресурс, не допускающий одновременного использования несколькими процессами)

B) Участок кода программы, оказывающий критическое влияние на производительность

C) Участок кода программы, содержащий ошибку

ANSWER: A

Взаимная блокировка процессов это

A) Ситуация, когда два или более процессов заблокированы в ожидании действий друг от друга

B) Попытка одновременного доступа двух или более процессов к критическому ресурсу

C) Невозможность завершить процессы до запланированного срока (deadline) в операционной системе реального времени из-за недостатка производительности

ANSWER: A

Дисциплина планирования SJN реализует

A) Справедливую стратегию

B) Стратегию максимальной пропускной способности

C) Стратегию равного среднего времени ожидания

ANSWER: B

Дисциплина кругового планирования (RR) реализует

A) Справедливую стратегию

B) Стратегию максимальной пропускной способности

C) Стратегию равного среднего времени ожидания

ANSWER: A

Дисциплина планирования FIFO (FCFS) реализует

A) Справедливую стратегию

B) Стратегию максимальной пропускной способности

C) Стратегию равного среднего времени ожидания

ANSWER: C

Справедливая стратегия управления ставит целью управления

A) Предоставить всем потребителям равную долю ресурса

B) Обеспечить для всех потребителей равное среднее время ожидания ресурса

ANSWER: A

Любая дисциплина управления ресурсами, направленная на реализацию стратегии максимальной пропускной способности

A) Заведомо справедлива

B) Заведомо не справедлива

C) Может быть справедливой или не справедливой, в зависимости от дисциплины

ANSWER: C

Стратегия управления ресурсом

A) Определяет цель управления

B) Определяет права доступа к ресурсу

C) Описывает алгоритм управления

D) Определяет тип ресурса

ANSWER: A

Стратегия управления ресурсом является нереализуемой, если

A) Не существует алгоритма (дисциплины управления), которая в точности (строго) реализовала бы данную стратегию

B) Алгоритм (дисциплина управления) слишком сложен для практической реализации

C) Существует множество алгоритмов (дисциплин управления), которые реализуют данную стратегию

ANSWER: A

Дисциплина управления ресурсом (алгоритм управления) является справедливой, если

A) для любого процесса исключается бесконечно долгое ожидание доступа к ресурсу

B) все процессы получают примерно равную долю ресурса

ANSWER: A

Частью кодирования является

A) Сжатие

B) Шифрование

C) Исправление ошибок
D) Все являются
ANSWER: D
Что является мерой различия между кодовыми комбинациями?
A) Расстояние Хэмминга
B) Коэффициент сжатия
C) Энтропия
D) Все является
ANSWER: A
Какой формат архивации файлов позволяет также шифровать их содержимое?
A) Все перечисленные
B) .zip
C) .7z
D) .rar
ANSWER: A
Где используется ассиметричное шифрование?
A) Во всех перечисленных случаях
B) Цифровая подпись
C) SSL-сертификаты
D) TLS-сертификаты
ANSWER: A
Алгоритмом шифрования не является
A) Все являются
B) RSA
C) Код Цезаря
D) AES
ANSWER: A
Датчики случайных чисел могут быть реализованы при помощи
A) Всех перечисленных способов
B) Специальных таблиц
C) Путем замера показателей какого-либо физического процесса
D) При помощи программной реализации набора математических операций
E) Комбинации физического и программного способов
ANSWER: A
Кодирование не может отвечать за
A) Новизну информации
B) Целостность информации
C) Конфиденциальность информации
D) Эффективность использования канала связи при передаче информации
E) За все отвечает
ANSWER: A
В качестве базовой операции при шифровании может применяться
A) Все перечисленные
B) Гаммирование
C) Подстановка
D) Перестановка
ANSWER: A
Алгоритмом хеширования не является
A) RSA
B) SHA1
C) MD5

D) Все являются
ANSWER: A
Шифрование не может применяться
A) Может во всех перечисленных случаях
B) При передаче информации
C) При хранении информации
D) При обработке информации
ANSWER: A
Какой способ шифрования обладает свойством абсолютной секретности?
A) Код Вернама
B) Блочное шифрование
C) Асимметричное шифрование
D) Все перечисленные
ANSWER: A
Что является мерой количества информации?
A) Энтропия
B) Расстояние Хэмминга
C) Коэффициент сжатия
D) Ничего из перечисленного
ANSWER: A
Какой формат архивации файлов имеет режим сжатия с потерями?
A) Ни один из перечисленных
B) .zip
C) .7z
D) .rar
ANSWER: A
Частью общей схемы передачи информации не является
A) Источник
B) Приемник
C) Хранилище
D) Канал
E) Все является
ANSWER: C
Что является характеристикой алгоритма сжатия?
A) Коэффициент сжатия
B) Расстояние Хэмминга
C) Пропускная способность
D) Коэффициент сжатия и пропускная способность
ANSWER: A
Какой способ шифрования обладает свойством абсолютной секретности?
A) Такого способа шифрования не существует на практике
B) Код Цезаря
C) Блочное шифрование в режиме обратной связи по шифротексту
D) Код Вернама
ANSWER: D
Алгоритмом шифрования не является
A) Кодирование длин серий
B) Код Вернама
C) RSA
D) Все являются
ANSWER: A

Что является необязательным для достижения абсолютной секретности кода Вернама?

A) Использование ключа только один раз

B) Длина ключа должна быть не меньше длины передаваемого сообщения

C) Ключ должен быть подлинно случаен

D) Все обязательно

ANSWER: D

Что теоретически позволяет понять, что зашифрованное сообщение может быть расшифровано?

A) Энтропия зашифрованного сообщения меньше максимальной

B) Равномерное распределение значений элементов зашифрованного сообщения

C) Знание, что зашифрованное сообщение передано два раза

D) Все позволяет

ANSWER: A

Артефактом жизненного цикла ПО не является

A) Документация

B) Требования

C) Код

D) Все являются

ANSWER: D

Какой вид тестирования основывается только на сведениях о внешней структуре проверяемой системы

A) Тестирование белого ящика

B) Тестирование черного ящика

C) Тестирование серого ящика

D) Все перечисленные

ANSWER: B

К формальным методам верификации не относится

A) Проверка согласованности

B) Мониторинг

C) Проверка моделей

D) Все перечисленные

E) Дедуктивный анализ

ANSWER: B

Какая техника построения тестов основана на генерировании псевдослучайных данных с заданными распределениями?

A) Тестирование на основе классов эквивалентности

B) Вероятностное тестирование

C) Комбинаторное тестирование

D) Сценарное тестирование

ANSWER: B

Для какой модели жизненного цикла разработки ПО не применимы методы статической верификации?

A) Каскадная

B) Для всех применимы

C) Итеративная

D) Гибкая

ANSWER: B

К статическим методам верификации относится

A) Проверка согласованности

B) Ни один из перечисленных

C) Экспертиза

D) Проверка моделей
E) Дедуктивный анализ
ANSWER: B
Какой вид инструментирования при мониторинге основан на модификации бинарного кода ПО специализированным инструментом?
A) Ручное
B) На основе бинарной трансляции
C) Компиляторное
D) Времени выполнения
ANSWER: B
Какой вид тестирования относится к проверке работы ПО в целом в окружении с заданными характеристиками?
A) Модульное
B) Системное
C) Интеграционное
D) Компонентное
ANSWER: B
К пользовательскому тестированию не относится
A) Альфа-тестирование
B) Аттестационное тестирование
C) Бета-тестирование
D) Все относятся
ANSWER: B
Временной логикой не является
A) Модальная логика
B) Логика линейного времени (LTL)
C) Логика дерева вычислений (CTL)
D) Все являются
ANSWER: A
Какие критерии полноты тестирования основаны на проверке выполнения элементов требований к ПО?
A) Структурные
B) Функциональные
C) Критерии на основе гипотез об ошибках
D) Все основаны
ANSWER: B
К динамическим методам верификации не относится
A) Тестирование
B) Мониторинг
C) Проверка моделей
D) Все относятся
ANSWER: C
В рамках какого вида тестирования также может проводится и мониторинг
A) Модульное (компонентное)
B) Интеграционное
C) Системное
D) Все перечисленные
ANSWER: D
Примером статического анализа не является
A) Замеры показателей времени работы программы
B) Рекомендации и предупреждения среды разработки (IDE) о правильности написания кода
C) Места расположения недостижимого кода

D) Все являются
ANSWER: A
Соответствие стандартам является атрибутом качества
A) Функциональности
B) Надежности
C) Переностимости
D) Всех перечисленных
ANSWER: D
Какой вид тестирования основывается только на сведениях о внутренней структуре проверяемой системы
A) Тестирование белого ящика
B) Тестирование черного ящика
C) Тестирование серого ящика
D) Все перечисленные
ANSWER: A
Что такое префиксный код?
A) Это код фиксированной длины
B) Это код, в котором никакое кодовое слово не совпадает с начальной частью какого-то другого кодового слова
C) Это код, в котором никакое кодовое слово не совпадает с завершением какого-то другого кодового слова
ANSWER: B
Выберите правильное значение расстояния Хэмминга для следующего двоичного кодового набора:0101100000010001101001001111011010100011100100100010100111001111101001110100
A) 12
B) 11
C) 10
D) 13
E) 14
ANSWER: A
В результате сложения со знаком двух двоичных 11-разрядных чисел 11101101000111110101010имели место следующие переносы относительно старшего разряда:
A) Входящий и исходящий вместе
B) Только входящий
C) Только исходящий
D) Не было переносов вообще
E) Больше двух переносов
ANSWER: A
Каких типов процессоров (по виду набора команд) НЕ существует?
A) CISC
B) RISC
C) MISC
D) VLIW
E) MPLA
ANSWER: E
Что такое порог срабатывания?
A) напряжение, примерно равное 1,3...1,4 В
B) уровень выходного напряжения
C) уровень входного напряжения, выше которого сигнал воспринимается как единица, а ниже — как нуль
ANSWER: C

Что такое аналоговый сигнал?

A) это сигнал, который может принимать любые значения в определенных пределах

B) это сигнал, несущий в себе какую-то информацию

C) это сигнал, приходящий на электронную систему извне и искажающий полезный

ANSWER: A

Какие устройства называются аналоговыми?

A) устройства, работающие только с аналоговыми сигналами

B) устройства, аналогичные друг другу

C) устройства, преобразующие физические величины в напряжение или ток

ANSWER: A

Выберите утверждение, характеризующее связь температуры процессора и тротлинга:

A) Прямой взаимосвязи между температурой и тротлингом не существует

B) Чем выше температура, тем больше тротлинг

C) Чем ниже температура, тем меньше тротлинг

ANSWER: B

Выберите правильное утверждение, характеризующее функционал контроллера прерываний наиболее полно. Контроллер прерываний это…

A) микросхема или встроенный блок процессора, отвечающий за возможность последовательной обработки запросов на прерывание от разных устройств

B) особый вид часов реального времени, синхронизирующий обмен контроллеров данными

C) специальное устройство, перезагружающее СВТ при «зависании»

D) обработчик сигналов от устройств ввода/вывода

ANSWER: A

Какой функционал НЕ реализуется в математических сопроцессорах?

A) аппаратный функционал, реализующий взятие прямого и обратного преобразования Фурье

B) выполнение операций с плавающей точкой

C) перезагрузка СВТ при «зависании»

D) решение задач численными методами

ANSWER: C

Какими из перечисленных особенностей НЕ обладают процессоры архитектуры CISC:

A) нефиксированное значение длины команды

B) фиксированное значение длины команды

C) арифметические действия кодируются в одной команде

D) небольшое число регистров, каждый из которых выполняет строго определённую функцию

ANSWER: B

Какими из перечисленных особенностей НЕ обладают процессоры архитектуры CISC:

A) нефиксированное значение длины команды

B) фиксированное значение длины команды

C) арифметические действия кодируются в одной команде

D) небольшое число регистров, каждый из которых выполняет строго определённую функцию

ANSWER: B

Какой функционал реализуется в классических (не гибридных) видеопроцессорах (GPU)?

A) синхронизация генерации звука и процесса наложения текстур не модель

B) расчет реалистичной физики

C) рендер изображения и его вывод на интерактивное устройство отображения

D) выполнение арифметических операций с матрицами

ANSWER: C

Выберите пункт, нарушающий стандартную очередность операций BIOS:

A) выполнение тестирования оборудования компьютера

B) чтение настроек из энергонезависимого ПЗУ

C) обновление ядра операционной системы

D) применение настроек

E) поиск и загрузка в оперативную память кода загрузчика

F) передача управления загрузчику

ANSWER: C

Операция AND это:

A) операция логического умножения

B) операция отрицания

C) операция логического сложения

D) операция отрицания равнозначности

ANSWER: A

ОПЕРАЦИЯ ПО ОРГАНИЗАЦИИ ХРАНЕНИЯ ФАЙЛОВ, ПРИ КОТОРОЙ ПОЛЬЗОВАТЕЛЮ ПРЕДОСТАВЛЯЕТСЯ ВОЗМОЖНОСТЬ ОБЪЕДИНИТЬ ФС, НАХОДЯЩИЕСЯ НА РАЗНЫХ УСТРОЙСТВАХ, В ЕДИНУЮ ФС, ОПИСЫВАЕМУЮ ЕДИНЫМ ДЕРЕВОМ КАТАЛОГОВ, НАЗЫВАЕТСЯ

A) Монтирование,

B) Объединение

C) Слияние

ANSWER: A

ТЕХНИКА ТЕСТИРОВАНИЯ ПРОГРАММ СОСТОИТ В

A) Применении накопленного опыта тестирования

B) Обнаружении отдельных ошибок

C) Сокращении числа тестов и выявлении классов ошибок

ANSWER: C

СИЛЬНО СВЯЗАННЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ, КОТОРЫЕ ИСПОЛЬЗУЮТСЯ ДЛЯ УПРАВЛЕНИЯ МУЛЬТИПРОЦЕССОРНЫМИ И ГОМОГЕННЫМИ МУЛЬТИКОМПЬЮТЕРНЫМИ СИСТЕМАМИ ОБЫЧНО НАЗЫВАЮТСЯ

A) Распределенными ОС

B) Сетевыми ОС

C) Многозадачными ОС

ANSWER: A

ЧТО ИЗ ПЕРЕЧИСЛЕННОГО НЕ ОТНОСИТСЯ К МЕТОДАМ ИНТЕГРАЦИИ ПРИЛОЖЕНИЙ:

A) Обмен файлами, в которые помещаются общие данные;

B) Общая база данных, в которой сохраняется общая информация

C) Технологический стек, на котором реализовано приложение

D) Удалённый вызов процедур в рамках систем обмена сообщениями для выполнения действий или обмена данными

ANSWER: C

КЛАСС ТЕХНОЛОГИЙ, КОТОРЫЕ ПОЗВОЛЯЮТ КОМПЬЮТЕРНЫМ ПРОГРАММАМ ВЫЗЫВАТЬ ФУНКЦИИ ИЛИ ПРОЦЕДУРЫ В ДРУГОМ АДРЕСНОМ ПРОСТРАНСТВЕ НАЗЫВАЕТСЯ

A) Удаленный вызов процедур;
B) Процедуры для выполнения обмена;
C) Удаленные компоненты
ANSWER: A

ЧТО ИЗ ПЕРЕЧИСЛЕННОГО НЕ ОТНОСИТСЯ К ФУНКЦИЯМ СУБД

A) Непосредственное управление данными во внешней памяти
B) Управление буферами оперативной памяти
C) Управление транзакциями
D) Журнализация
E) Резервирование,
F) Поддержка языков базы данных
ANSWER: E

КЛИЕНТ-СЕРВЕРНАЯ СУБД РАСПОЛАГАЕТСЯ

A) На сервере вместе с БД
B) На сервере без БД
C) Частично на клиенте
D) Копируется на клиента с сервера
ANSWER: A

SADT-МОДЕЛИ И DFD ИСПОЛЬЗУЮТСЯ ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ "AS-IS" И МОДЕЛИ "TO-BE", ОТРАЖАЯ, ТАКИМ ОБРАЗОМ, СУЩЕСТВУЮЩУЮ И ПРЕДЛАГАЕМУЮ СТРУКТУРУ БИЗНЕС-ПРОЦЕССОВ ОРГАНИЗАЦИИ И ВЗАИМОДЕЙСТВИЕ МЕЖДУ НИМИ. НА КАКОЙ СТАДИИ РАЗРАБОТКИ ПО ЭТИ МОДЕЛИ СТРОЯТСЯ?

A) Формирования требований к ПО
B) Проектирования
C) Внедрения
D) Сопровождения
ANSWER: A

ДВА ОСНОВНЫХ ВИДА ПРИКЛАДНОГО ПО

A) Общего программирования и специальное
B) Общего назначения и специальное
C) Общего использования и специальное
ANSWER: B

КАКАЯ КОМАНДА ИЗМЕНИТ ВАШЕ МЕСТОПОЛОЖЕНИЕ, ПЕРЕМЕСТИВ ВАС В РЕГИСТРАЦИОННЫЙ КАТАЛОГ

A) ls
B) pwd
C) cd
ANSWER: B

ИСПОЛЬЗОВАНИЕ ОДНОГО ИМЕНИ ДЛЯ ЗАДАНИЯ ОБЩИХ ДЛЯ КЛАССА ДЕЙСТВИЙ, ЧТО ОЗНАЧАЕТ СПОСОБНОСТЬ ОБЪЕКТОВ ВЫБИРАТЬ ВНУТРЕННИЙ МЕТОД, ИСХОДЯ ИЗ ТИПА ДАННЫХ, ОПРЕДЕЛЯЕТ СВОЙСТВО ООП

A) Полиморфизм
B) Управление событиями
C) Инкапсуляция
D) Наследование
ANSWER: C

КАКАЯ АРХИТЕКТУРА ОС ИМЕЕТ ТАКОЕ ПРЕИМУЩЕСТВО, КАК ИСПОЛЬЗОВАНИЕ НА ОДНОЙ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ ПРОГРАММ, НАПИСАННЫХ ДЛЯ РАЗНЫХ ОПЕРАЦИОННЫХ СИСТЕМ

A) Монолитное ядро
B) Многоуровневая ОС
C) Смешанная ОС
D) Виртуальная машина
ANSWER: D
ПРОГРАММА «ЗАГЛУШКА» СЛУЖИТ ДЛЯ
A) Запуска программы на выполнение
B) Имитации запуска другой программы на выполнение
C) Проверки правильности работы программы
D) Имитации передачи параметров в другой модуль
ANSWER: B
ПРИ ВХОДЕ В СИСТЕМУ ЗАПУСКАЕТСЯ СПЕЦИАЛЬНАЯ ВЕРСИЯ ОБОЛОЧКИ, НАЗЫВАЕМАЯ
A) Интерактивной оболочкой
B) Интерпретированной оболочкой;
C) Индивидуальной оболочкой
ANSWER: B
КРИПТОГРАФИЧЕСКИЕ СРЕДСТВА – ЭТО…
A) Средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
B) Механизм, позволяющий получить новый класс на основе существующего
C) Специальные программы и системы защиты информации в информационных системах различного назначения
ANSWER: A
КОМПЛЕКС СПЛАНИРОВАННЫХ ДЕЙСТВИЙ, ПРЕДПРИНИМАЕМЫХ ДЛЯ РЕШЕНИЯ ПРОБЛЕМЫ ОПРЕДЕЛЕННОЙ ЦЕЛЕВОЙ ГРУППЫ, ОГРАНИЧЕННЫХ ПО ВРЕМЕНИ И РЕСУРСАМ, С КОНКРЕТНЫМИ РЕЗУЛЬТАТАМИ, НАЗЫВАЕТСЯ
A) План
B) Проект
C) Задание
ANSWER: B
СВОЙСТВО ОТКРЫТОСТИ ОЗНАЧАЕТ, ЧТО СИСТЕМА РЕАЛИЗУЕТ ОТКРЫТЫЕ СПЕЦИФИКАЦИИ, ДОСТАТОЧНЫЕ ДЛЯ ТОГО, ЧТОБЫ ОБЕСПЕЧИТЬ:
A) Возможность переноса разработанного прикладного программного обеспечения на широких диапазон систем с минимальными изменениями (мобильность приложений, переносимость)
B) Совместную работу (взаимодействие) с другими прикладными приложениями на локальных и удаленных платформах (интероперабельность, способность к взаимодействию)
C) Взаимодействие с пользователями в стиле, облегчающим последним переход от системы к системе (мобильность пользователей)
D) Все вышеперечисленное
ANSWER: D
В КАКИХ СЛУЧАЯХ НАИБОЛЕЕ ВЕРОЯТНО ПОЯВЛЕНИЕ УЯЗВИМОСТЕЙ?
A) При наличии пользовательского интерфейса
B) При несоблюдении принципов ООП
C) При вызове функции с переменным числом аргументов
D) На стыке взаимодействия приложения и операционной системы и/или приложения и базы данных
ANSWER: D

КАКАЯ ЧАСТЬ МЕТОДОЛОГИИ SECURE SOFTWARE DEVELOPMENT LIFECYCLE (SSDLC) НАХОДИТСЯ ЗА РАМКАМИ ПОДХОДА DEVSECOPS?

A) Разработка требований к безопасности приложения

B) Разработка исходного кода

C) Создание инсталляционного пакета

D) Развертывание в инфраструктуре

ANSWER: A

НА ЧТО НАПРАВЛЕН ОСНОВНОЙ ФОКУС ВНИМАНИЯ APPLICATION SECURITY?

A) Обнаружение уязвимостей в готовом продукте

B) Предотвращение появления уязвимостей

C) Исправление уязвимостей в готовом продукте

D) Классификация уязвимостей в приложениях

ANSWER: B

ВИД МУЛЬТИЗАДАЧНОСТИ, КОТОРЫЙ ХАРАКТЕРИЗУЕТСЯ ТЕМ, ЧТО РЕСУРСЫ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ РАСПРЕДЕЛЯЮТСЯ МЕЖДУ НЕСКОЛЬКИМИ ПРИЛОЖЕНИЯМИ, ПОЛУЧАЮЩИМИ ЦП В СООТВЕТСТВИИ СО СВОИМ ПРИОРИТЕТОМ

A) Переключательная

B) Невытесняющая

C) Вытесняющая

ANSWER: B

КАТАЛОГОВЫЕ ФАЙЛОВЫЕ СИСТЕМЫ ИМЕЮТ ИЕРАРХИЧЕСКУЮ СТРУКТУРУ. ЧТО ОБРАЗУЮТ КАТАЛОГИ, ЕСЛИ ФАЙЛУ РАЗРЕШЕНО ВХОДИТЬ ТОЛЬКО В ОДИН КАТАЛОГ?

A) Дерево

B) Сеть

C) Иерархическую структуру;

D) Каталог

ANSWER: A

ВЫБЕРИТЕ КОМПОНЕНТ ПО, КОТОРЫЙ ПОЗВОЛЯЕТ ЛИБО РАСШИРИТЬ ВОЗМОЖНОСТИ ПО УПРАВЛЕНИЮ ОС, ЛИБО ИЗМЕНИТЬ ВСТРОЕННЫЕ В СИСТЕМУ ВОЗМОЖНОСТИ

A) Интерфейсные оболочки;

B) Система управления файлами;

C) Инструментальные среды программирования

ANSWER: A

ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ ОПИСЫВАЮТ:

A) Особенности эксплуатации

B) Предоставляемые сервисы, поведение системы

C) Ограничения, накладываемые на систему

ANSWER: B

РАЗРАБОТКА СПЕЦИФИКАЦИЙ ПО ОСУЩЕСТВЛЯЕТСЯ ПО РЕЗУЛЬТАТАМ

A) Анализа требований

B) Кодирования

C) Проектирования

D) Тестирования

ANSWER: A

СПОСОБЫ ТЕСТИРОВАНИЯ:

A) Функциональное и структурное тестирование

B) Логическое и физическое тестирование

C) Синтаксический и семантический анализ

ANSWER: A

КАКОГО УРОВНЯ ТЕСТИРОВАНИЯ НЕ СУЩЕСТВУЕТ
A) α
B) β
C) Системное
D) Интеграционное
E) Модульное
F) Виртуальное
ANSWER: F
Кто является инициатором записи данных Cookie?
A) Веб-сервер
B) Клиентское приложение
C) Данные Cookie всегда сохраняются автоматически
D) Это может быть кто угодно
ANSWER: A
В какой части ответа сервера содержится запрашиваемый клиентом веб-ресурс?
A) В теле ответа сервера
B) В заголовке ответа сервера
C) В строке состояния ответа сервера
ANSWER: A
К какому классу языков относятся языки сценариев с точки зрения поддержки типизации переменных?
A) К типизированным языкам
B) К нетипизированным языкам
C) Это зависит от конкретного языка сценариев
ANSWER: B
Переход от монолитной архитектуры ядра к модульному ядру
A) Упрощает добавление в ядро новых функций
B) Повышает защищенность операционной системы
C) Существенно снижает производительность
D) Существенно повышает производительность
ANSWER: A
Кэш системы трансляции адресов (TLB) позволяет
A) Сократить время, затрачиваемое на преобразование виртуального адреса в физический
B) Сэкономить место в памяти
C) Расширить объем виртуального адресного пространства
D) Защитить данные в памяти
ANSWER: A
Семафор это объект операционной системы, позволяющий
A) Реализовать ожидание процессами момента наступления запланированных событий
B) Исключить взаимную блокировку процессов
C) Обеспечить соблюдение приоритетов
D) Прервать выполнение процесса при ошибке
ANSWER: A
Критическая секция программного кода это
A) Участок кода программы, из которого выполняются действия с критическим ресурсом (ресурс, не допускающий одновременного использования несколькими процессами)
B) Участок кода программы, оказывающий критическое влияние на производительность
C) Участок кода программы, содержащий ошибку
ANSWER: A

Взаимная блокировка процессов это

A) Ситуация, когда два или более процессов заблокированы в ожидании действий друг от друга

B) Попытка одновременного доступа двух или более процессов к критическому ресурсу

C) Невозможность завершить процессы до запланированного срока (deadline) в операционной системе реального времени из-за недостатка производительности

ANSWER: A

Дисциплина планирования SJN реализует

A) Справедливую стратегию

B) Стратегию максимальной пропускной способности

C) Стратегию равного среднего времени ожидания

ANSWER: B

Дисциплина кругового планирования (RR) реализует

A) Справедливую стратегию

B) Стратегию максимальной пропускной способности

C) Стратегию равного среднего времени ожидания

ANSWER: A

Дисциплина планирования FIFO (FCFS) реализует

A) Справедливую стратегию

B) Стратегию максимальной пропускной способности

C) Стратегию равного среднего времени ожидания

ANSWER: C

Справедливая стратегия управления ставит целью управления

A) Предоставить всем потребителям равную долю ресурса

B) Обеспечить для всех потребителей равное среднее время ожидания ресурса

ANSWER: A

Любая дисциплина управления ресурсами, направленная на реализацию стратегии максимальной пропускной способности

A) Заведомо справедлива

B) Заведомо не справедлива

C) Может быть справедливой или не справедливой, в зависимости от дисциплины

ANSWER: C

Стратегия управления ресурсом

A) Определяет цель управления

B) Определяет права доступа к ресурсу

C) Описывает алгоритм управления

D) Определяет тип ресурса

ANSWER: A

Стратегия управления ресурсом является нереализуемой, если

A) Не существует алгоритма (дисциплины управления), которая в точности (строго) реализовала бы данную стратегию

B) Алгоритм (дисциплина управления) слишком сложен для практической реализации

C) Существует множество алгоритмов (дисциплин управления), которые реализуют данную стратегию

ANSWER: A

Дисциплина управления ресурсом (алгоритм управления) является справедливой, если

A) для любого процесса исключается бесконечно долгое ожидание доступа к ресурсу

B) все процессы получают примерно равную долю ресурса
ANSWER: A
Как называется возможность скрыть детали реализации?
A) Инкапсуляция
B) Наследование
C) Полиморфизм
ANSWER: A
При наследовании:
A) Данные производному классу наследуются от базового класса
B) Методы производному классу наследуются от базового класса
C) Данные и методы производному классу наследуются от базового класса
ANSWER: C
Методы класса это:
A) правила, как работать с объектами класса
B) функции-члены класса, могут быть статическими или динамическими
C) динамические функции-члены класса
D) статические функции-члены класса
ANSWER: B
Можно ли в языке программирование c# не использовать блок get в реализации свойства?
A) можно
B) нельзя
C) можно, но с точки зрения корректности разработки — это неправильно
ANSWER: C
Как получить ссылку на текущий экземпляр класса внутри самого класса?
A) с помощью соответствующей переменной или параметра метода
B) с помощью ключевого слова super
C) с помощью ключевого слова this
D) с помощью ключевого слова value
E) с помощью ключевого слова base
ANSWER: C
Верно ли, что если метод использует открытые члены класса, то он должен быть открытым?
A) да
B) нет
ANSWER: B
верно ли написана реализация класса на языке программирования c#?class A{ public abstract void DoIt() { }}
A) да
B) нет
ANSWER: B
Возможно ли перекрытие абстрактных методов класса в производном классе?
A) да
B) нет
ANSWER: A
Обязательно ли перекрытие абстрактных методов класса в производном классе?
A) да
B) нет
ANSWER: B
Как удалить объект в программе, написанной на языке C#?

A) вызвать деструктор

B) с помощью оператора delete

C) удалять объект в программе не нужно, он будет удалён сборщиком мусора

D) присвоить переменной значение null

ANSWER: C

Возможно ли множественное наследование в языке программирования C#?

A) множественное наследование в языке C# не поддерживается

B) множественное наследование в языке C# возможно только для интерфейсов

ANSWER: B

Какие утверждения верны для массивов в языке Java?

A) Размер массива может быть изменен после его создания.

B) Индексация элементов в массиве начинается с 1.

C) Все элементы в конкретном массиве должны быть одного типа (или наследоваться от одного типа).

D) В одной программе могут использоваться массивы только для одного типа данных.

ANSWER: C

Почему для конкатенации множества строк в языке Java следует использовать StringBuilder (выберите верные утверждения)?

A) Конкатенация строк оператором «+» не предусмотрена.

B) При конкатенации строк с помощью оператором «+» результат всегда печатается в консоль (стандартный поток вывода – stdout).

C) Конкатенация строк оператором «+» приводит к созданию множества экземпляров строк и многократному копированию данных.

D) Строки не являются ссылочным типом данных.

ANSWER: C

Строгая типизация предполагает (выберите верные утверждения)?

A) Все используемые в функции переменные должны объявляться строго до остального кода функции.

B) При компиляции программы весь код (все операции) проверяется на совместимость или возможность преобразования типов, несовместимость считается ошибкой.

C) В программе нельзя определить несколько функций с одинаковым именем.

D) Язык программирования обязательно должен быть объектно-ориентированным.

ANSWER: B

Что возвращает функция, приведенная ниже:

A) последнее положительное значение в массиве

B) максимальное значение в массиве

C) минимальное значение после первого положительного значения в массиве

D) минимальное положительное значение в массиве

ANSWER: D

Как называется проверка соответствия продукта некоторого вида деятельности его спецификациям?

A) аудитом

B) валидацией

C) верификацией

ANSWER: C

Возможность начать разработку ПС с частично определенными требованиями допускает модель ЖЦ

A) Инкрементная
B) Эволюционная
C) Спиральная
D) Каскадная
ANSWER: B

Многоуровневая модель качества определена в международном стандарте

A) ISO/IEC 12207
B) ISO/IEC 9126
C) ISO/IEC 12119
D) ISO/IEC 25000
ANSWER: B

Процесс формализованного описания функциональных и нефункциональных требований называется

A) верификацией требований
B) аттестацией требований
C) спецификацией требований
D) трассировкой требований
ANSWER: C

Установленная и повторно используемая конструкция или архитектура, представляющая собой решение проблемы в рамках некоторого часто возникающего контекста

A) компонент
B) шаблон
C) сценарий
D) стандарт
ANSWER: B

Проверка соответствия продукта некоторого вида деятельности своему назначению и предполагаемым способа использования

A) ревизия
B) верификация
C) аудит
D) валидация
ANSWER: D

Схема Захмана применяется на этапе процесса разработки

A) конструирования
B) проектирования
C) анализа предметной области
D) тестирования
ANSWER: C

Диаграмма вариантов использования используется для представления

A) функциональных требований
B) требований эффективности
C) требований надежности
D) требований эргономичности
ANSWER: A

Модульное тестирование осуществляется в рамках процесса жизненного цикла

A) Комплексирование
B) Конструирование
C) Детальное проектирование
D) Квалификационное тестирование

ANSWER: B

Стратегии интеграционного тестирования

A) восходящая

B) структурная

C) нисходящая

D) функциональная

ANSWER: C

Определение процедур и методов по ослаблению отрицательных последствий рисковых событий

A) Идентификация рисков

B) Планирование управления рисками

C) Качественная оценка рисков

D) Разрешение рисков

E) Мониторинг и контроль рисков

ANSWER: D

Тестирование по методу «белого ящика» основано на использовании

A) классов эквивалентности данных

B) потоковых графов

C) анализа граничных значений

ANSWER: B

Входят ли ограничения целостности в определение реляционной модели данных?

A) да

B) нет

ANSWER: A

Что понимается под ссылочной целостностью?

A) ограничения на допустимые значения внешнего ключа

B) ограничения на допустимые значения первичного ключа

C) ограничения на допустимые значения альтернативного ключа

ANSWER: A

Может ли внешний ключ являться потенциальным ключом?

A) нет

B) да

ANSWER: B

Какое понятие шире?

A) потенциальные ключи

B) первичные ключи

ANSWER: A

Сколько операций нарушают ссылочную целостность?

A) 3

B) 5

C) 4

D) 6

ANSWER: C

Сколько основных вариантов действий для обеспечения целостности данных

A) 3

B) 5

C) 2

ANSWER: C

Какой модели в структурном подходе к созданию БД соответствует объектно-ориентированная модель поведения (диаграмма прецедентов)?

A) функциональная модель

B) информационная модель

C) событийная модель
ANSWER: A
Могут ли атрибуты первичного ключа принимать значение NULL?
A) да
B) нет
ANSWER: B
При установлении неидентифицирующей связи между сущностями в модели IDEF1X
A) обе сущности независимые
B) одна сущность независимая, другая зависимая
ANSWER: A
Какие операции не нарушают ссылочной целостности?
A) вставка кортежа в родительское отношение
B) вставка кортежа в дочернее отношение
C) удаление кортежа в родительском отношении
D) удаление кортежа в дочернем отношении
ANSWER: D
Какие операции разрешаются при обновлении кортежа в родительском отношении?
A) ограничить
B) каскадировать
C) установить в NULL
D) установить по умолчанию
ANSWER: D
Сколькими свойствами обладает защищенная система с БД?
A) 4
B) 3
C) 5
ANSWER: B
На сколько типов делятся иерархии категорий в модели IDEF1X?
A) 3
B) 5
C) 2
ANSWER: C
Сколько основных функций реализуется в средствах поддержки доступности современных СУБД?
A) 2
B) 5
C) 3
ANSWER: C
Какая операция не используется при вставке кортежа в дочернее отношение?
A) ограничить
B) каскадировать
C) установить в NULL
D) установить по умолчанию
ANSWER: B
Операторы языка SQL GRANT и REVOKE предназначены для организации
A) дискреционной защиты
B) мандатной защиты
C) ролевой защиты
ANSWER: A

Каким ключевым словом задается ограничение таблицы в синтаксисе языка SQL?

A) CHECK

B) UNIQUE

C) CONSTRAINT

ANSWER: C

Уровень безопасности пользователя равен уровню безопасности таблицы БД. Какие операции пользователь может осуществлять над таблицей?

A) чтения

B) записи

ANSWER: B

Сколько фаз включает этап проектирования безопасных баз данных?

A) 5

B) 3

C) 2

ANSWER: B

Какая из моделей баз данных не зависит от любых физических аспектов реализации?

A) логическая

B) концептуальная

C) физическая

ANSWER: B

На сколько групп разделяют ограничения целостности БД?

A) 3

B) 5

C) 4

ANSWER: C

Какими свойствами обладает потенциальный ключ отношения БД?

A) уникальность

B) неизбыточность

C) потенциальная непротиворечивость

ANSWER: B

Сколько этапов в процессе создания защищенных систем с базами данных?

A) 3

B) 5

C) 4

ANSWER: C

Какой модели в объектно-ориентированном подходе к созданию БД соответствует структурная информационная модель «сущность-связь»?

A) модель поведения (диаграмма прецедентов)

B) модель состояний (диаграмма классов)

C) модель изменения состояний (диаграмма состояний)

ANSWER: B

К какому подходу проектирования БД относится нормализация?

A) нисходящему

B) восходящему

ANSWER: B

Не заработал АПКШ в роли криптошлюза: в ПУ ЦУС статус "не включен", таблица arp после команды ping содержит MAC-адрес АПКШ. Возможные причины такого статуса?

A) неверная IP-конфигурация компьютера управления или АПКШ

B) несоответствие ключевой информации АПКШ и ПУ ЦУС

C) отсутствие правил, разрешающих прохождение пакетов для ping

D) неисправности физического подключения компьютера с ПУ ЦУС или АПКШ к сети

ANSWER: B

Как возникает пара ключей при создании сертификата в PKI ?

A) генерируется на стороне клиента

B) генерируется на стороне удостоверяющего центра

C) генерируется на стороне корневого удостоверяющего центра

D) генерируется на стороне CRL

E) генерируется на стороне AIA

ANSWER: A

В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие ключи должны быть переданы на АП?

A) ключи обмена коллективов, ключи защиты ключей обмена, ключи связи с ЦУС

B) ключи защиты ключей обмена, действующий персональный ключ, ключи подписи

C) ключи обмена коллективов, действующий персональный ключ, ключи подписи

D) ключи обмена коллективов, ключи защиты ключей обмена, действующий персональный ключ

E) ключи обмена коллективов, ключи защиты ключей обмена, ключи подписи

F) действующий персональный ключ, ключи подписи

ANSWER: A

В ходе конфигурирования VIPnet на рабочем месте администратора с помощьюЦУС выполнена адресная администрация сети и добавлен новый пользователь. Какие ключи должны быть переданы пользователю?

A) ключи обмена коллективов, ключи защиты ключей обмена, ключи связи с ЦУС

B) ключи защиты ключей обмена, действующий персональный ключ, ключи подписи

C) ключи обмена коллективов, действующий персональный ключ, ключи подписи

D) ключи обмена коллективов, ключи защиты ключей обмена, действующий персональный ключ

E) ключи обмена коллективов, ключи защиты ключей обмена, ключи подписи

F) действующий персональный ключ, ключи подписи

ANSWER: F

Какие уязвимости в PKI появляются при использовании KRA?

A) передача открытого ключа через сеть

B) передача закрытого ключа через сеть

C) передача ключевой пары через сеть

D) генерация ключевой пары не на стороне клиента

ANSWER: B

Какие уязвимости в PKI появляются при использовании KRA?

A) передача открытого ключа через сеть

B) хранение закрытого ключа не на стороне клиента

C) передача ключевой пары через сеть

D) генерация ключевой пары не на стороне клиента

E) хранение открытого ключа не на стороне клиента

ANSWER: B

Компоненты VPN (как системы удаленного доступа) обязательно доолжны включать:

A) NAS
B) DHCP
C) AAA
D) ADDS
E) Kerberos
ANSWER: A

Какие существуют методы восстановления закрытых ключей, например, в случае их повреждения?

A) импорт
B) экспорт
C) агент восстановления данных
D) шаблон сертификата
E) отзыв сертификата
ANSWER: A

Какие существуют методы восстановления закрытых ключей, например, в случае их повреждения?

A) kra
B) экспорт
C) агент восстановления данных
D) шаблон сертификата
E) отзыв сертификата
ANSWER: A

В ходе конфигурирования ViPNet администратору потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. В последовательности действий администратора ViPNet для введения этого АП (компьютер уже закуплен) обязательно будет следующий шаг:

A) работа с ЦУС
B) работа с УКЦ
C) Работа с Деловой Почтой
D) Установка Координатора
ANSWER: A

В ходе конфигурирования ViPNet администратору потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. В последовательности действий администратора ViPNet для введения этого АП (компьютер уже закуплен) обязательно будет следующий шаг:

A) формирование дистрибутива ключей
B) работа с УКЦ
C) Работа с Деловой Почтой
D) Установка Координатора
ANSWER: A

Что необходимо сделать в первую очередь, при потере секретного ключа от сертификата пользователя, используемого для проверки подлинности.

A) добавить серийный номер сертификата в CRL
B) добавить серийный номер сертификата в AIA
C) добавить отпечаток сертификата в CRL
D) восстановить из архива сохраненный предварительно ключ
E) обратиться к KRA для восстановления
ANSWER: A

Как проверить работу криптокоммутаторов, расположенных в филиалах?

A) ping на узел внутри одного сегмента, но находящегося в другом филиале

B) ping на узел внутри одного сегмента, находящегося в том же филиале

C) ping на узел в другом сегменте, находящийся в том же филиале

D) ping на узел в другом сегменте, находящийся в другом филиале

ANSWER: A

В ходе лабораторных вы создавали VPN-подключение PPTP и аналогичное по функционалу L3VPN решение от Кода Безопасности с применением АПКШ Континент. Как отличается скорости развертывания этих решений для создания защищенной сети с очень большим количеством рабочих мест (точек подключения к VPN)?.

A) развёртывание СД на АПКШ Континент медленнее

B) развёртывание СД наАПКШ Континент быстрее

ANSWER: A

В ходе лабораторных вы создавали VPN-подключение PPTP и аналогичное по функционалу L3VPN решение от Кода Безопасности с применением АПКШ Континент. Каким образом передаётся конфигурация клиента СД АПКШ Континент ?

A) через групповую политику

B) передаётся набор параметров: адрес, имя пользователя и т.д.

C) передается файл с параметрами конфигурации

ANSWER: C

В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие уровни/виды шифрования будут задействованы при посылки пользователем зашифрованного письма на этот АП?

A) на прикладном и сетевом уровнях

B) на прикладном уровне

C) на сетевом уровне

D) на транспортном уровне

E) на сетевом и транспортном уровнях

F) на прикладном и транспортном уровнях

G) на сетевом и канальном уровнях

H) на канальном уровне

ANSWER: A

Формируется новая защищенная сеть с использованием АПКШ Континент. Последовательность действий по включению в сеть ЦУС включает в себя.

A) выполнить инициализацию ЦУС на стороне АПКШ

B) выполнить инициализацию ЦУС на стороне ПУ ЦУС

C) передать ключевую информацию на носителе из ПУ ЦУС в АПКШ

ANSWER: A

Что такое удостоверяющий центр (CA – Certification Authority)?

A) сервер, который подписывает данные субъекта и его открытый ключ

B) сервер, который подписывает данные субъекта и его закрытый ключ

C) сервер, который подписывает открытый ключ субъекта

D) сервер, который подписывает закрытый ключ субъекта

E) сервер, который подписывает данные субъекта

ANSWER: A

Назовите типы удостоверяющего центра (CA – Certification Authority), с точки зрения функциональности и поддержки сетевых протоколов

A) Standalone, Enterprise

B) Root, Subordinate
C) Public
D) Private
ANSWER: A
Назовите типы удостоверяющего центра (CA – Certification Authority), с точки зрения PKI-иерархии
A) Standalone, Enterprise
B) Root, Subordinate
C) Public
D) Private
ANSWER: B
Кто является инициатором записи данных Cookie?
A) Веб-сервер
B) Клиентское приложение
C) Данные Cookie всегда сохраняются автоматически
D) Это может быть кто угодно
ANSWER: A
В какой части ответа сервера содержится запрашиваемый клиентом веб-ресурс?
A) В теле ответа сервера
B) В заголовке ответа сервера
C) В строке состояния ответа сервера
ANSWER: A
К какому классу языков относятся языки сценариев с точки зрения поддержки типизации переменных?
A) К типизированным языкам
B) К нетипизированным языкам
C) Это зависит от конкретного языка сценариев
ANSWER: B
Входят ли ограничения целостности в определение реляционной модели данных?
A) да
B) нет
ANSWER: A
Что понимается под ссылочной целостностью?
A) ограничения на допустимые значения внешнего ключа
B) ограничения на допустимые значения первичного ключа
C) ограничения на допустимые значения альтернативного ключа
ANSWER: A
Может ли внешний ключ являться потенциальным ключом?
A) нет
B) да
ANSWER: B
Какое понятие шире?
A) потенциальные ключи
B) первичные ключи
ANSWER: A
Сколько операций нарушают ссылочную целостность?
A) 3
B) 5
C) 4
D) 6
ANSWER: C

Сколько основных вариантов действий для обеспечения целостности данных

A) 3

B) 5

C) 2

ANSWER: C

Какой модели в структурном подходе к созданию БД соответствует объектно-ориентированная модель поведения (диаграмма прецедентов)?

A) функциональная модель

B) информационная модель

C) событийная модель

ANSWER: A

Могут ли атрибуты первичного ключа принимать значение NULL?

A) да

B) нет

ANSWER: B

При установлении неидентифицирующей связи между сущностями в модели IDEF1X

A) обе сущности независимые

B) одна сущность независимая, другая зависимая

ANSWER: A

Какие операции не нарушают ссылочной целостности?

A) вставка кортежа в родительское отношение

B) вставка кортежа в дочернее отношение

C) удаление кортежа в родительском отношении

D) удаление кортежа в дочернем отношении

ANSWER: D

Какие операции разрешаются при обновлении кортежа в родительском отношении?

A) ограничить

B) каскадировать

C) установить в NULL

D) установить по умолчанию

ANSWER: D

Сколькими свойствами обладает защищенная система с БД?

A) 4

B) 3

C) 5

ANSWER: B

На сколько типов делятся иерархии категорий в модели IDEF1X?

A) 3

B) 5

C) 2

ANSWER: C

Сколько основных функций реализуется в средствах поддержки доступности современных СУБД?

A) 2

B) 5

C) 3

ANSWER: C

Какая операция не используется при вставке кортежа в дочернее отношение?

A) ограничить

B) каскадировать

C) установить в NULL
D) установить по умолчанию
ANSWER: B
Операторы языка SQL GRANT и REVOKE предназначены для организации
A) дискреционной защиты
B) мандатной защиты
C) ролевой защиты
ANSWER: A
Каким ключевым словом задается ограничение таблицы в синтаксисе языка SQL?
A) CHECK
B) UNIQUE
C) CONSTRAINT
ANSWER: C
Уровень безопасности пользователя равен уровню безопасности таблицы БД. Какие операции пользователь может осуществлять над таблицей?
A) чтения
B) записи
ANSWER: B
Сколько фаз включает этап проектирования безопасных баз данных?
A) 5
B) 3
C) 2
ANSWER: B
Какая из моделей баз данных не зависит от любых физических аспектов реализации?
A) логическая
B) концептуальная
C) физическая
ANSWER: B
На сколько групп разделяют ограничения целостности БД?
A) 3
B) 5
C) 4
ANSWER: C
Какими свойствами обладает потенциальный ключ отношения БД?
A) уникальность
B) неизбыточность
C) потенциальная непротиворечивость
ANSWER: B
Сколько этапов в процессе создания защищенных систем с базами данных?
A) 3
B) 5
C) 4
ANSWER: C
Какой модели в объектно-ориентированном подходе к созданию БД соответствует структурная информационная модель «сущность-связь»?
A) модель поведения (диаграмма прецедентов)
B) модель состояний (диаграмма классов)
C) модель изменения состояний (диаграмма состояний)
ANSWER: B

К какому подходу проектирования БД относится нормализация?

A) нисходящему

B) восходящему

ANSWER: B

Не заработал АПКШ в роли криптошлюза: в ПУ ЦУС статус "не включен", таблица arp после команды ping содержит MAC-адрес АПКШ. Возможные причины такого статуса?

A) неверная IP-конфигурация компьютера управления или АПКШ

B) несоответствие ключевой информации АПКШ и ПУ ЦУС

C) отсутствие правил, разрешающих прохождение пакетов для ping

D) неисправности физического подключения компьютера с ПУ ЦУС или АПКШ к сети

ANSWER: B

Как возникает пара ключей при создании сертификата в PKI ?

A) генерируется на стороне клиента

B) генерируется на стороне удостоверяющего центра

C) генерируется на стороне корневого удостоверяющего центра

D) генерируется на стороне CRL

E) генерируется на стороне AIA

ANSWER: A

В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие ключи должны быть переданы на АП?

A) ключи обмена коллективов, ключи защиты ключей обмена, ключи связи с ЦУС

B) ключи защиты ключей обмена, действующий персональный ключ, ключи подписи

C) ключи обмена коллективов, действующий персональный ключ, ключи подписи

D) ключи обмена коллективов, ключи защиты ключей обмена, действующий персональный ключ

E) ключи обмена коллективов, ключи защиты ключей обмена, ключи подписи

F) действующий персональный ключ, ключи подписи

ANSWER: A

В ходе конфигурирования VIPnet на рабочем месте администратора с помощьюЦУС выполнена адресная администрация сети и добавлен новый пользователь. Какие ключи должны быть переданы пользователю?

A) ключи обмена коллективов, ключи защиты ключей обмена, ключи связи с ЦУС

B) ключи защиты ключей обмена, действующий персональный ключ, ключи подписи

C) ключи обмена коллективов, действующий персональный ключ, ключи подписи

D) ключи обмена коллективов, ключи защиты ключей обмена, действующий персональный ключ

E) ключи обмена коллективов, ключи защиты ключей обмена, ключи подписи

F) действующий персональный ключ, ключи подписи

ANSWER: F

Какие уязвимости в PKI появляются при использовании KRA?

A) передача открытого ключа через сеть

B) передача закрытого ключа через сеть

C) передача ключевой пары через сеть

D) генерация ключевой пары не на стороне клиента
ANSWER: B
Какие уязвимости в PKI появляются при использовании KRA?
A) передача открытого ключа через сеть
B) хранение закрытого ключа не на стороне клиента
C) передача ключевой пары через сеть
D) генерация ключевой пары не на стороне клиента
E) хранение открытого ключа не на стороне клиента
ANSWER: B
Компоненты VPN (как системы удаленного доступа) обязательно доолжны включать:
A) NAS
B) DHCP
C) AAA
D) ADDS
E) Kerberos
ANSWER: A
Какие существуют методы восстановления закрытых ключей, например, в случае их повреждения?
A) импорт
B) экспорт
C) агент восстановления данных
D) шаблон сертификата
E) отзыв сертификата
ANSWER: A
Какие существуют методы восстановления закрытых ключей, например, в случае их повреждения?
A) kra
B) экспорт
C) агент восстановления данных
D) шаблон сертификата
E) отзыв сертификата
ANSWER: A
В ходе конфигурирования ViPNet администратору потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. В последовательности действий администратора ViPNet для введения этого АП (компьютер уже закуплен) обязательно будет следующий шаг:
A) работа с ЦУС
B) работа с УКЦ
C) Работа с Деловой Почтой
D) Установка Координатора
ANSWER: A
В ходе конфигурирования ViPNet администратору потребовалось добавить еще один "Абонентский Пункт" для администрации нового района города. В последовательности действий администратора ViPNet для введения этого АП (компьютер уже закуплен) обязательно будет следующий шаг:
A) формирование дистрибутива ключей
B) работа с УКЦ
C) Работа с Деловой Почтой
D) Установка Координатора
ANSWER: A

Что необходимо сделать в первую очередь, при потере секретного ключа от сертификата пользователя, используемого для проверки подлинности.

A) добавить серийный номер сертификата в CRL

B) добавить серийный номер сертификата в AIA

C) добавить отпечаток сертификата в CRL

D) восстановить из архива сохраненный предварительно ключ

E) обратиться к KRA для восстановления

ANSWER: A

Как проверить работу криптокоммутаторов, расположенных в филиалах?

A) ping на узел внутри одного сегмента, но находящегося в другом филиале

B) ping на узел внутри одного сегмента, находящегося в том же филиале

C) ping на узел в другом сегменте, находящийся в том же филиале

D) ping на узел в другом сегменте, находящийся в другом филиале

ANSWER: A

В ходе лабораторных вы создавали VPN-подключение PPTP и аналогичное по функционалу L3VPN решение от Кода Безопасности с применением АПКШ Континент. Как отличается скорости развертывания этих решений для создания защищенной сети с очень большим количеством рабочих мест (точек подключения к VPN)?.

A) развёртывание СД на АПКШ Континент медленнее

B) развёртывание СД наАПКШ Континент быстрее

ANSWER: A

В ходе лабораторных вы создавали VPN-подключение PPTP и аналогичное по функционалу L3VPN решение от Кода Безопасности с применением АПКШ Континент. Каким образом передаётся конфигурация клиента СД АПКШ Континент ?

A) через групповую политику

B) передаётся набор параметров: адрес, имя пользователя и т.д.

C) передается файл с параметрами конфигурации

ANSWER: C

В ходе конфигурирования VIPnet на рабочем месте администратора с помощью ЦУС выполнена адресная администрация сети и добавлено новое рабочее место (АП). Какие уровни/виды шифрования будут задействованы при посылки пользователем зашифрованного письма на этот АП?

A) на прикладном и сетевом уровнях

B) на прикладном уровне

C) на сетевом уровне

D) на транспортном уровне

E) на сетевом и транспортном уровнях

F) на прикладном и транспортном уровнях

G) на сетевом и канальном уровнях

H) на канальном уровне

ANSWER: A

Формируется новая защищенная сеть с использованием АПКШ Континент. Последовательность действий по включению в сеть ЦУС включает в себя.

A) выполнить инициализацию ЦУС на стороне АПКШ

B) выполнить инициализацию ЦУС на стороне ПУ ЦУС

C) передать ключевую информацию на носителе из ПУ ЦУС в АПКШ

ANSWER: A

Что такое удостоверяющий центр (CA – Certification Authority)?

A) сервер, который подписывает данные субъекта и его открытый ключ
B) сервер, который подписывает данные субъекта и его закрытый ключ
C) сервер, который подписывает открытый ключ субъекта
D) сервер, который подписывает закрытый ключ субъекта
E) сервер, который подписывает данные субъекта
ANSWER: A
Назовите типы удостоверяющего центра (CA – Certification Authority), с точки зрения функциональности и поддержки сетевых протоколов
A) Standalone, Enterprise
B) Root, Subordinate
C) Public
D) Private
ANSWER: A
Назовите типы удостоверяющего центра (CA – Certification Authority), с точки зрения PKI-иерархии
A) Standalone, Enterprise
B) Root, Subordinate
C) Public
D) Private
ANSWER: B
6_x_ – 4 ≡ 0 (mod 8)
A) _x_ ≡ 2 (mod 8)
B) _x_ ≡ 6 (mod 8)
C) нет корней
D) _x_ ≡ 2 (mod 8), _x_ ≡ 6 (mod 8)
ANSWER: D
Наибольший общий делитель двух чисел a и b это
A) такое целое натуральное число, на которое делится данное число без остатка. Если у натурального числа больше двух делителей, его называют составным
B) такое число, которое может быть делителем каждого числа из указанного множества
C) наибольшее число, на которое a и b делятся без остатка
ANSWER: C
Наименьшее общее кратное двух целых чисел a и b это
A) наименьшее натуральное число, которое делится на a и b без остатка
B) наибольшее число, на которое a и b делятся без остатка
C) наибольшее натуральное число, которое делится на a и b без остатка
D) наименьшее число, на которое a и b делятся без остатка
ANSWER: A
НОД (28, 64)
A) 2
B) 7
C) 4
D) 1
ANSWER: C
НОД(4,16)
A) 16
B) 4
C) 8
D) 1
ANSWER: B
НОК(16, 8)
A) 16

B) 8
C) 1
ANSWER: A
Основная теорема арифметики
A) несколько связанных утверждений о решении линейной системы сравнений
B) всякое натуральное число можно разложить на простые множители, т. е. однозначно записать его в виде произведения степеней простых чисел
C) это тест простоты натурального числа _n_
ANSWER: B
Посчитать значение функции Эйлера для 15
A) 2
B) 4
C) 6
D) 8
ANSWER: D
Посчитать значение функции Эйлера для 7
A) 1
B) 2
C) 4
D) 6
ANSWER: D
Простое число
A) это натуральное число, единственными делителями которого являются только оно само и единица
B) это натуральное число, единственными делителем которого являются только оно само
C) это натуральное число, единственными делителем которого являются только еди
ANSWER: A
Результат факторизации числа 1024
A) 2 в 10 степени
B) 512 двоек, которые образуют сумму 1024
C) оба варианта верны
ANSWER: A
Результат факторизации числа 17
A) 10 + 7
B) 17
C) 1 + 1 + 3 + 5 + 7
ANSWER: B
Результат факторизации числа 26
A) 2 * (7 + 6)
B) 2 * 13
C) 1 * 26
D) 2 * (7 + 3 + 2)
ANSWER: B
Символ Якоби
A) теоретико-числовая функция двух аргументов. Является квадратичным характером в кольце вычетов
B) пределённое обобщение производной функции одной переменной на случай отображений из евклидова пространства в себя
C) вектор, своим направлением указывающий направление возрастания (а антиградиент - убывания) некоторой скалярной величины
ANSWER: A

Факторизация числа

A) называется его разложение в произведение простых множителей. Существование и единственность (с точностью до порядка следования множителей) такого разложения следует из основной теоремы арифметики

B) называется его разложение в сумму простых слагаемых. Существование и единственность (с точностью до порядка следования слагаемых) такого разложения следует из основной теоремы арифметики

C) называется его разложение в множество чисел, которое может быть как слагаемыми так и множителями числа, так как это следует из основной теоремы арифметики

ANSWER: A

Числом \(M_A \) матрицы \(A \) называется:

A) \(M_A = det(A) \)

B) \(M_A = ||A|| ||x|| \)

C) \(M_A = ||A^{-1}|| ||A|| \)

D) \(M_A = ||A^{-1}|| \)

ANSWER: C

Функция f(x) задана таблицей из шести значений. Необходимо построить таблицу четвертых производных этой функции. Укажите, с помощью какого интерполяционного многочлена могут быть получены формулы численного дифференцирования:

A) Интерполяционный многочлен Лагранжа 4 степени

B) Интерполяционный многочлен Ньютона 3 степени

C) Интерполяционный многочлен Лагранжа 2 степени

D) Интерполяционный многочлен Ньютона 6 степени

ANSWER: A

Система линейных алгебраических уравнений \(\widetilde{x} = B \widetilde{x} + f \) решается методом простых итераций. Найдено, что все собственные значения \(^ \lambda B \) матрицы \(B \) удовлетворяют условию \(^ \lambda B ^{\in(a;b)} \). Укажите, при каких \(a \) и \(b \) метод будет сходиться при любом начальном приближении

A) \(a = 2; b = 7 \)

B) \(a = -1; b = 3 \)

C) \(a = -1; b = 1 \)

D) \(a = 1; b = 4 \)

ANSWER: C

Выберите правильное утверждение: метод Якоби, примененный к системе линейных алгебраических уравнений \(Ax=f \), (\(A \) – невырожденная матрица) будет сходиться при любом начальном приближении, если

A) если хотя бы одно собственное значение матрицы A по модулю больше единицы

B) матрица A – матрица с диагональным преобладанием

C) если хотя бы одно собственное значение матрицы A по модулю меньше единицы

D) матрица A вещественная

ANSWER: B

Система линейных алгебраических уравнений \(\widetilde{x} = B \widetilde{x} + f \) решается методом простых итераций. Найдено, что все собственные значения \(^ \lambda B \) матрицы \(B \) удовлетворяют условию \(^ \lambda B ^{\in(a;b)} \). Укажите, при каких \(a \) и \(b \) метод будет расходиться при любом начальном приближении

A) \(a = 2; b = 5 \)

B) \(a = -1; b = 0,5 \)

C) \(a = -0,5; b = 1 \)

D) \(a = 0,5; b = 0,9 \)
ANSWER: A
Система линейных алгебраических уравнений \(Ax=b \) плохо обусловлена, если у матрицы \(A \) этой системы
A) число обусловленности много больше единицы
B) число обусловленности близко к единице
C) \(det A \approx 0 \)
D) \(det A \neq 0 \)
ANSWER: B
Функция f(x) задана таблицей из трех значений. Необходимо построить таблицу вторых производных этой функции. Укажите, с помощью какого интерполяционного многочлена могут быть получены формулы численного дифференцирования:
A) интерполяционный многочлен Лагранжа 3степени
B) интерполяционный многочлен Лагранжа 2 степени
C) интерполяционный многочлен Ньютона 3 степени
D) интерполяционный многочлен Лагранжа 1 степени
ANSWER: B
Решается система линейных алгебраических уравнений \(Ax=b \). В результате найдено приближенное решение \(\widetilde{x} \) (\(x^* \) - точное решение системы). Невязкой называется величина
A) \(R = x^* - \widetilde{x} \)
B) \(R=A\widetilde{x}-b \)
C) \(R = A\widetilde{x}-x^* \)
ANSWER: B
Функция f(x) задана таблицей из четырех значений. Необходимо построить таблицу третьих производных этой функции. Укажите, с помощью какого интерполяционного многочлена могут быть получены формулы численного дифференцирования:
A) интерполяционный многочлен Лагранжа 4 степени
B) интерполяционный многочлен Лагранжа 3 степени
C) интерполяционный многочлен Ньютона 2 степени
D) интерполяционный многочлен Ньютона 5 степени
ANSWER: B
Выберите правильное утверждение:
A) Области сходимости метода простой итерации (МПИ) и метода Зейделя всегда одинаковы
B) Если МПИ сходится, то метод Зейделя расходится
C) Если метод Зейделя сходится, то МПИ расходится
D) Области сходимости МПИ и метода Зейделя в общем случае различны
ANSWER: D
Выберите правильное утверждение: для таблично заданной функции можно построить единственный интерполяционный многочлен степени N, если
A) таблица содержит ровно N узлов интерполяции, которые расположены в порядке возрастания
B) таблица содержит ровно N+1 узел интерполяции, и среди узлов интерполяции нет совпадающих
C) таблица содержит ровно N+1 узел интерполяции, и среди узлов интерполяции есть совпадающие
D) таблица содержит ровно N узлов интерполяции, и среди узлов интерполяции нет совпадающих
ANSWER: B

Выберите правильное утверждение: для таблично заданной функции можно построить интерполяционный кубический сплайн ТОЛЬКО В ТОМ СЛУЧАЕ, если

A) таблица содержит четное число узлов интерполяции, и среди узлов интерполяции есть совпадающие

B) таблица содержит нечетное число узлов интерполяции, и среди узлов интерполяции нет совпадающих

C) таблица содержит не менее трех узлов интерполяции, которые расположены в порядке строгого возрастания

D) таблица содержит четное число узлов интерполяции, и среди узлов интерполяции нет совпадающих

ANSWER: C

Выберите правильное утверждение: погрешность интерполяции можно минимизировать, если

A) узлы интерполяции расположить в порядке возрастания

B) если в качестве узлов интерполяции взять нули исходной заданной таблично функции

C) если в качестве узлов интерполяции взять нули полинома Чебышева

D) узлы интерполяции расположить в порядке убывания

ANSWER: C

Выберите правильное утверждение: метод Гаусса-Зейделя, примененный к системе линейных алгебраических уравнений \(Ax=f \), (\(A \) – невырожденная матрица) будет сходиться при любом начальном приближении, если

A) хотя бы одно собственное значение матрицы A по модулю больше единицы

B) матрица (\A\) – матрица с диагональным преобладанием

C) если хотя бы одно собственное значение матрицы A по модулю меньше единицы

D) матрица (\A\) вещественная

ANSWER: B

Функция \(f(x)\) задана таблицей из пяти значений. Необходимо построить таблицу четвертых производных этой функции. Укажите, с помощью какого интерполяционного многочлена могут быть получены формулы численного дифференцирования

A) Интерполяционный многочлен Ньютона 4 степени

B) Интерполяционный многочлен Лагранжа 3 степени

C) Интерполяционный многочлен Лагранжа 2 степени

D) Интерполяционный многочлен Лагранжа 5 степени

ANSWER: A

Мощность какого множества модели ХРУ больше: субъектов или объектов ?

A) субъектов

B) объектов

ANSWER: B

Какая ролевая модель реализует статическое разделение обязанностей?

A) модель с иерархической организацией ролей

B) модель с ограничениями на одновременное использование ролей в одном сеансе

C) модель со взаимоисключающими ролями

ANSWER: C

Какими понятиями замещается понятие «субъект» в ролевой модели?

A) объект

B) пользователь

C) сущность
D) роль
ANSWER: B
Что означает правило управления доступом user в ролевой модели?
A) для каждого сеанса определяет пользователя, который осуществляет этот сеанс работы с системой
B) для каждого сеанса задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе
C) для каждого сеанса определяет набор ролей, которые могут быть одновременно доступны пользователю в этом сеансе
ANSWER: A
Какая ролевая модель реализует динамическое разделение обязанностей?
A) модель с иерархической организацией ролей
B) модель с ограничениями на одновременное использование ролей в одном сеансе
C) модель со взаимоисключающими ролями
ANSWER: B
К какому классу моделей безопасности относится модель Take-Grant?
A) дискреционные модели безопасности
B) мандатные модели безопасности
C) ролевые модели безопасности
ANSWER: A
К какому классу моделей безопасности относится модель типизированной матрицы доступа?
A) дискреционные модели безопасности
B) мандатные модели безопасности
C) ролевые модели безопасности
ANSWER: A
К какому классу моделей безопасности относится модель Белла-ЛаПадулы?
A) дискреционные модели безопасности
B) мандатные модели безопасности
C) ролевые модели безопасности
ANSWER: B
К какому классу моделей безопасности относится модель безопасности переходов?
A) дискреционные модели безопасности
B) мандатные модели безопасности
C) ролевые модели безопасности
ANSWER: B
Сколько примитивных (элементарных) операций используется в классической модели XPУ?
A) 4
B) 6
C) 5
D) 7
ANSWER: B
К какому классу операций относится операция Create классической модели XPУ?
A) монотонная
B) немонотонная
ANSWER: A

Сколько основных множеств использует ролевая модель для описания системы?

A) 5

B) 4

C) 3

D) 7

ANSWER: B

В каком случае задача проверки безопасности системы ХРУ является разрешимой?

A) система команд не содержит элементарных операций «удалить» и «уничтожить»

B) команды являются монооперационными

C) команды системы являются одноусловными и монотонными

ANSWER: C

Сколько функций уровня безопасности используется в модели безопасности переходов?

A) 3

B) 2

C) 1

ANSWER: B

Состояние в модели Белла-ЛаПадулы называется безопасным по чтению, если

A) уровень безопасности субъекта не ниже уровня безопасности объекта

B) уровень безопасности объекта не ниже уровня безопасности субъекта

ANSWER: A

Система ХРУ называется монооперационной, если

A) система команд не содержит элементарных операций «удалить» и «уничтожить»

B) каждая команда системы содержит одну элементарную операцию

C) команды системы являются одноусловными

ANSWER: B

Удовлетворяет ли функция перехода Z-системы ограничениям основной теоремы безопасности Белла-ЛаПадулы?

A) да

B) нет

ANSWER: A

Ячейка матрицы доступа модели ХРУ является

A) строкой

B) множеством

C) числом

ANSWER: B

Какое дополнительное отношение на множестве ролей вводится в ролевой модели с иерархической организацией ролей?

A) отношение строгого порядка

B) отношение эквивалентности

C) отношение толерантности

D) отношение нестрогого порядка

ANSWER: D

Какое количество базовых представлений включают в себя модели безопасности?

A) 4

B) 6

C) 7

D) 5

ANSWER: B

Существует ли алгоритм проверки безопасности произвольной системы ХРУ?

A) да

B) нет

ANSWER: B

Какое решающее правило при разработке алгоритма распознавании образов следует реализовать при задании функций правдоподобия классов и априорных вероятностей гипотез

A) решающее правило в соответствии с критерием минимума среднего риска

B) решающее правило в соответствии с критерием максимума апостериорной вероятности

C) решающее правило на основе деревьев решений

D) решающее правило в соответствии с критерием максимума функции правдоподобия соответствии с критерием максимума функции правдоподобия

ANSWER: B

Выберите общий сценарий решения задачи кластерного анализа и при неизвестном количестве классов

A) в цикле по неизвестному числу классов перебор всех возможных комбинаций кластеров с их объединением и разделением

B) реализация EM-алгоритма с перебором числа кластеров

C) выполнение кластеризаций с перебором числа кластеров и использование специальных критериев для определения числа кластеров

D) использование специальных критериев для определения числа кластеров

ANSWER: C

Что такое машинное обучение?

A) синоним понятия «искусственный интеллект»

B) совокупность методов построения алгоритмов, способных улучшать свое поведение в процессе накопления информации

C) формализация знаний экспертов и их перенос в компьютер в виде базы знаний (область экспертных систем)

D) выявление общих закономерностей по частным эмпирическим (экспериментальным) данным

ANSWER: B

Основное предположение при синтезе наивного байесовского классификатора состоит в следующем

A) признаки распознавания не коррелированны друг относительно друга

B) матрицы ковариаций признаков распознавания диагональны

C) признаки распознавания подчиняются распределению Бернулли

D) признаки распознавания статистически независимы

ANSWER: D

Какие алгоритмы используются при наличии неизвестных параметров функций правдоподобия?

A) на основе оценок с использованием окон Парзена

B) подстановочные алгоритмы

C) оптимальные алгоритмы по критерию максимального правдоподобия

D) оптимальные алгоритмы по критерию максимума апостериорной вероятности

ANSWER: B

Какие инъекции случайности используется при построении алгоритма «случайный лес»?

A) случайная подвыборка и случайный набор признаков при формировании каждого дерева решений в ансамбле

B) случайная подвыборка и случайное ветвление при формировании каждого дерева решений в ансамбле

C) случайная подвыборка, случайный набор признаков, случайный размер дерева при формировании каждого дерева решений в ансамбле

D) случайное количество деревьев, случайный набор признаков, случайный размер дерева при формировании ансамбля

ANSWER: A

Какие алгоритмы используются при наличии неизвестных функций правдоподобия?

A) на основе оценок с использованием окон Парзена

B) подстановочные алгоритмы

C) оптимальные алгоритмы по критерию максимального правдоподобия

D) оптимальные алгоритмы по критерию максимума апостериорной вероятности

ANSWER: A

Выберите известные Вам алгоритмы, относящиеся к классу композиционных

A) Случайный лес, алгоритм SVM

B) Случайный лес, алгоритм SVM, алгоритм K-соседей

C) Случайный лес, алгоритм AdaBoost

D) Случайный лес, алгоритм K-соседей, алгоритм K-средних

ANSWER: C

Какое решающее правило при разработке алгоритма классификации образов следует реализовать при задании функций правдоподобия классов, штрафных функций, априорных вероятностей гипотез?

A) решающее правило в соответствии с критерием минимума среднего риска

B) решающее правило в соответствии с критерием максимума апостериорной вероятности

C) решающее правило в соответствии с критерием максимума функции правдоподобия

D) наивный байесовский классификатор

ANSWER: A

Наиболее полный набор данных для синтеза оптимальных алгоритмов классификации из перечисленных исходных включает:

A) число классов, ядерные оценки плотности распределения классов

B) число классов, априорные вероятностей гипотез, функции правдоподобия классов, штрафные функции

C) число классов, априорные вероятностей гипотез, функции правдоподобия классов с подстановкой неизвестных параметров

ANSWER: B

Какие исходные данные входят в постановку задачи кластерного анализа в рамках детерминистского подхода?

A) размеченная обучающая смешанная выборка, число классов (кластеров), мера близости образов различных классов

B) неразмеченная обучающая смешанная выборка, число классов (кластеров), мера близости образов различных классов, способ сравнении классов

C) неразмеченная обучающая смешанная выборка, число классов (кластеров), мера близости образов различных классов

ANSWER: C

Постановка задачи регрессии в рамках детерминистского подхода предполагает

A) задание неразмеченной обучающей выборки, использование критерия наименьших квадратов, задание типа регрессии

B) задание размеченной обучающей выборки, использование критерия максимума апостериорной вероятности, решение системы линейных уравнений

C) задание размеченной обучающей выборки, использование критерия наименьших квадратов, выполнение нелинейного преобразования входных переменных, решение системы линейных уравнений

D) задание размеченной обучающей выборки, использование критерия наименьших квадратов, задание типа регрессии

ANSWER: D

Какие штрафные функции (функции потерь) используется при синтезе алгоритма классификации на основе критерия максимума апостериорной вероятности?

A) симметричные штрафные функций с фиксированной нулевой платой за правильное решение и не одинаковой платой за ошибки

B) симметричные штрафные функций с нулевой платой за правильное решение и одинаковой платой за ошибки

C) несимметричные штрафные функций с нулевой платой за правильное решение и одинаковой платой за ошибки

D) симметричные штрафные функций с фиксированной ненулевой платой за правильное решение и одинаковой платой за ошибки

ANSWER: B

Диапазон частот ПЭМИН:

A) 9 КГц – 10 ГГц

B) 20 Гц – 20 КГц

C) 300 Гц – 300 КГц

D) 2 ГГц – 20 ГГц

ANSWER: A

При индуктивном подключении телефонного закладочного устройства к телефонной линии общее сопротивление:

A) возрастет

B) уменьшится

C) останется без изменений

D) изменится в соответствии с гармоническим законом

ANSWER: C

Параметрический канал утечки информации образуется:

A) в результате высокочастотного облучения ОТСС

B) в результате изменения параметров среды распространения сигнала

C) в результате изменения параметров окружающей среды

D) в результате высокочастотного облучения ВТСС

ANSWER: A

Видимый диапазон длин волн:

A) 0,4 – 0,7 мкм

B) 0,4 – 1,2 мкм

C) 3 – 5 мкм

D) 8 – 14 мкм

ANSWER: A

Учетные записи локальных пользователей в системе Dallas Lock 8.0:

A) создаются в системе Dallas Lock только пользователями наделенными соответствующими полномочиями

B) создаются в операционной системе только пользователями, наделенными соответствующими полномочиями

C) создаются только администраторами безопасности системы Dallas Lock

D) создаются любым пользователем системы Dallas Lock

ANSWER: A

Межсетевой экран применяется для:

A) обнаружения сетевых атак или подозрительных намерений злоумышленника

B) разграничения доступа между двумя сетями с различными требованиями по обеспечению безопасности

C) контроля почтового трафика и Web-трафика

D) организации шифрованного сетевого соединения

ANSWER: B

Какой принцип управления межсетевым экраном предпочтительнее в компьютерной системе, обрабатывающей конфиденциальную информацию?

A) разрешено все, что не запрещено

B) запрещено все, что не разрешено

C) выборочной фильтрации трафика

D) контроля сетевых соединений

ANSWER: B

Защита информации в VPN (виртуальных частных сетях) обеспечивается с помощью:

A) межсетевых экранов и шифрования трафика

B) физической защиты информационных линий связи

C) инкапсуляции и декапсуляции сетевых пакетов

D) журналирования событий безопасности

ANSWER: C

Механизм замкнутой программной среды в системе Dallas Lock 8.0:

A) позволяет явно указать с какими программами пользователь может работать

B) позволят производить разграничение доступа пользователя к настройкам операционной системы

C) позволяет производить блокировку работы пользователя при НСД

D) позволяет осуществлять кодирование файлов и папок

ANSWER: A

Защита информации от непреднамеренного воздействия – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: A

Защита информации от НСД – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: B

Защита информации от НСВ – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с

нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: D

Защита информации от утечки – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: C

Способ защиты информации – это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) заранее намеченный результат защиты информации

C) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации

D) порядок и правила применения определенных принципов и средств защиты информации

ANSWER: D

Специальное исследование (объекта защиты информации) – это:

A) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ

B) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации

C) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации

D) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств

ANSWER: C

Специальная проверка – это:

A) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ

B) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации

C) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных правовых документов в области безопасности информации

D) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств

ANSWER: D

Контроль целостности в системе Secret Net предназначен для:

A) слежения за неизменностью контролируемых объектов

B) выявления НСД

C) выявления вредоносного программного обеспечения

D) выявления нештатного подключения внешних устройств

ANSWER: A

Идентификация – это:

A) проверка принадлежности субъекту доступа предъявленного им идентификатора

B) установление соответствия реального объекта представленной на него документации, названию во избежание подмены одного объекта другим

C) присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

D) совокупность мероприятий по установлению и подтверждению достоверности сведений о пользователях с использованием оригиналов документов и (или) надлежащим образом заверенных копий

ANSWER: C

Какие основные способы разграничения доступа применяются в компьютерных системах?

A) дискреционный и мандатный

B) по специальным спискам и многоуровневый

C) по группам пользователей и специальным разовым разрешениям

D) парольное разграничение доступа и иерархическое

ANSWER: A

Что такое аудит безопасности компьютерной системы?

A) инструмент политики безопасности, позволяющий контролировать процесс загрузки системных драйверов

B) инструмент политики безопасности, позволяющий отслеживать действия пользователей и системные события и регистрировать их в журнале

C) инструмент политики безопасности, позволяющий наблюдать динамические изменения технического состояния аппаратных компонентов компьютера (температура материнской платы, скорость вращения вентилятора на процессоре и т.д.)

D) инструмент политики безопасности, направленный на проверку реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности

ANSWER: B

Замысел защиты информации - это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) деятельность по обеспечению защиты информации не криптографическими методами от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию

C) совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация

D) реализация конституционных прав человека и гражданина на до-ступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность

ANSWER: A

Несанкционированный доступ (НСД) к информации – это:

A) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)

B) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств

C) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа

D) совокупность объекта разведки, средства разведки, среды распространения сигнала

ANSWER: A

Системы анализа уязвимостей позволяют:

A) выявить злоумышленника, работающего в компьютерной сети

B) выявить уязвимости проектируемой системы защиты информации

C) выявить уязвимости действующей системы защиты информации

D) выявить уязвимости по результатам журнала аудита безопасности

ANSWER: C

Акустические закладочные устройства – это:

A) специальные миниатюрные электронные устройства перехвата акустической (речевой) информации

B) специальные миниатюрные электронные устройства для перехвата информации в проводных линиях связи

C) специальные миниатюрные электронные устройства для съема видеоинформации

D) специальные миниатюрные электронные устройства для съема акустической информации, передаваемой по линиям связи

ANSWER: A

Радиозакладочными устройствами называют:

A) акустические закладки, передающие информацию по радиоканалу
B) акустические закладки, передающие информацию по проводным линиям связи
C) акустические закладки, передающие информацию по ИК-каналу
D) акустические закладки, передающие информацию по ВОЛС-линиям
ANSWER: A
Диапазон частот работы сканирующего приемника ar-8200:
A) 50 кГц…1500 МГц
B) 100 кГц… 1000 МГц
C) 1000МГц … 5200МГц
D) 500 кГц...2040 МГц
ANSWER: D
Цели защиты информации от технических средств разведки:
A) предотвращение утечки, хищения, утраты, искажения, подделки информации
B) предотвращение угроз безопасности личности, общества, государства
C) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации
D) все вышеперечисленные цели
ANSWER: D
Электрические каналы утечки информации образуются за счет:
A) наводок электромагнитных излучений технических средств передачи информации на соединительные линии вспомогательных технических средств связи и посторонние проводники, выходящие за пределы контролируемой зоны
B) просачивания информационных сигналов в цепи электропитания технических средств передачи информации
C) просачивания информационных сигналов в цепи заземления технических средств передачи информации
D) все ответы верны
ANSWER: D
К какому классу устройств относится устройство AR8200?
A) индикатор поля
B) сканирующий приемник
C) анализатор спектра
D) нет правильных ответов
ANSWER: B
Комплекс радиомониторинга и выявления каналов утечки информации «Навигатор» предназначен для решения следующих задач:
A) оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации
B) оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства, системы и их коммуникации
C) оценки защищенности вспомогательных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации
D) оценки защищенности конфиденциальной информации от утечки по виброакустическому каналу
ANSWER: B
Протокол маршрутизации OSPF относится к следующему классу алгоритмов:

A) алгоритмы состояния связей (LSA)
B) дистанционно-векторные алгоритмы (DVA)
C) алгоритмы централизованной маршрутизации
D) алгоритмы лавинной маршрутизации
E) алгоритмы фиксированной (статической) маршрутизации
ANSWER: A

Защита данных от искажений при передаче по радиоканалу путём внесения в них структурной избыточности происходит при:
A) кодировании источника данных
B) канальном кодировании
C) модуляции
D) криптографическом кодировании
E) форматировании источника данных
ANSWER: B

Прикладной процесс однозначно определяется в пределах сети и в пределах отдельного компьютера:
A) IP-адресом
B) сокетом
C) номером порта
D) UDP-дейтаграммой
E) TCP-сегментом
ANSWER: B

Каково назначение протокола ARP?
A) ручное назначение статических адресов
B) автоматическое назначение статических адресов
C) определения локального адреса используемого протокола физического уровня по IP-адресу
D) автоматическое распределение динамических адресов
E) мультиплексирование и демультиплексирование информационных потоков
ANSWER: C

Каков объём IP-адреса (в версии IPv4)?
A) 8 байт
B) 4 бита
C) 16 байт
D) 4 байта
E) 16 бит
ANSWER: C

Укажите протокольную единицу физического уровня в модели OSI/ISO:
A) пакет
B) кадр
C) бит
D) SPDU
E) TPDU
ANSWER: C

К какому типу каналов относится канал с аддитивным белым гауссовским шумом?
A) двоичный симметричный канал
B) канал с замираниями
C) многолучевой канал
D) дискретный канал без памяти
E) канал с дискретным входом и непрерывным выходом
ANSWER: E

Как называется характеристика радиотехнической системы, представляющей собой ее отклик на входной бесконечно короткий сигнал единичной площади:

A) Частотный коэффициент передачи

B) Спектр

C) Импульсная характеристика

D) Переходная характеристика

ANSWER: C

Сколько точек содержит сигнальное созвездие QPSK-сигнала (сигнал с квадратурной фазовой манипуляцией)?

A) 2

B) 4

C) 6

D) 8

ANSWER: B

Фильтр, амплитудно-частотная характеристика (АЧХ) которого повторяет форму амплитудного спектра сигнала, а фазочастотная характеристика (ФЧХ) симметрична фазовому спектру с учетом задержки на время длительности сигнала и максимизирующий отношение сигнал/шум, называется:

A) фильтром низких частот

B) фильтром высоких частот

C) согласованным фильтром

D) режекторным фильтром

ANSWER: C

Вероятность ошибки связанная с вынесением решением в пользу наличия в принятой реализации полезного сигнала при условии его отсутствия называется:

A) вероятностью пропуска

B) вероятностью ложной тревоги

C) априорной вероятностью

D) полной вероятностью ошибки

ANSWER: B

Вероятность выхода из строя устройства, состоящего из трех последовательно соединенных функциональных блоков, при условии что вероятность безотказной работы каждого блока в течение определенного времени T равна p1, p2 и p3 соответственно:

A) 1-p1*p2*p3

B) p1* p2*p3

C) p1*p3-p2

D) p1-p2*p3

ANSWER: A

Сигнал на выходе линейной стационарной цепи связан с сигналом на входе через:

A) Интеграл Дюамеля

B) Интеграл Пуассона

C) Интеграл Лаплапса

D) Интеграл Фурье

ANSWER: A

Какое из нижеперечисленных утверждений является неверным:

A) у периодических сигналов линейчатые спектры

B) у непериодических сигналов непрерывные спектры

C) на выходе линейной стационарной системы модуль спектральной плотности выходного сигнала представляет собой произведение модуля

спектральной плотности входного и модуля амплитудной характеристики системы

D) на выходе линейной стационарной системы модуль спектральной плотности выходного сигнала представляет собой произведение модуля спектральной плотности входного и квадрата модуля амплитудной характеристики системы

ANSWER: C

Представление объекта диагностики, при котором элементы представляются в виде совокупности вершин, а связи между ними в виде направленных дуг, соответствующих направлениям распространения энергии и информации называется:

A) ориентированным графом информационно-энергетических связей

B) структурной схемой

C) принципиальной схемой

D) ненаправленным графом

ANSWER: A

Прибор, предназначенный для исследования амплитудных и временных параметров электрического сигнала, подаваемого на его вход и позволяющий в процессе диагностики наглядно отображать зависимости на экране называется:

A) вольтметром

B) амперметром

C) частотомером

D) осциллографом

ANSWER: D

Способ поиска неисправностей, при котором отказ определяется на основании анализа известных признаков, однозначно характеризующих данный отказ

A) способ характерного признака

B) способ промежуточных измерений

C) способ контрольных переключений и поверок

D) способ сравнения

ANSWER: A

Устройство для снижения амплитуды до нужного уровня с целью измерения, а также для защиты измерительного прибора от чрезмерных уровней сигнала, которые могут повредить его это:

A) аттенюатор

B) делитель частоты

C) фильтр

D) осциллограф

ANSWER: A

Как называется эффект искажения сигнала во временной области при аналого-цифровом преобразовании, вызванный наложением высокочастотных составляющих на низкочастотные, вследствие недостаточной частоты дискретизации?

A) Алиасинг

B) Перемодуляция

C) Замирания

D) Передискретизация

ANSWER: A

Многолучевость распространения радиоволн в точке приема вызывает эффект

A) замирания

B) модуляции

C) усиления
D) фильтрации
ANSWER: A
Какой, в соответствии с теоремой Котельникова, должна быть минимально допустимая частота дискретизации аналогового сигнала с ограниченным спектром, верхняя частота которого f=20 кГц.
A) 80 кГц
B) 10 кГц
C) 40 кГц
D) 40 Гц
ANSWER: C
Вид искажения в радиотехнической системе при которой форма огибающей модулированного сигнала на выходе модулятора перестает повторять форму передаваемого сообщения называется:
A) демодуляцией
B) перемодуляцией
C) дисперсией
D) передискретизацией
ANSWER: B
Суть комбинационного метода проверки неисправностей состоит в:
A) проверке полной группы параметров, обеспечивающих однозначное выявление неработоспособного элемента
B) в последовательном разбиении на группы (содержащие неисправный элемент) и осуществлении серии проверок до определения неисправного элемента
C) последовательной проверке всех элементов по одному в определенной последовательности
ANSWER: A
Что произойдет с шириной спектра сигнала при увеличении его длительности в 2 раза?
A) увеличится в 4 раза
B) не измениться
C) увеличится в 2 раза
D) уменьшится в 2 раза
ANSWER: D
Фильтр низких частот (ФНЧ) предназначен для:
A) пропускания низких частот в спектре и обрезания высоких
B) пропускания высоких частот в спектре и обрезания низких
C) пропускании сигнала без изменений
D) пропускании спектральных составляющих сигнала в некоторой полосе частот
ANSWER: A
Чем отличается амплитудно-модулированный сигнал (АМ-сигнал) с балансной модуляцией от обычного АМ-сигнала:
A) в спектре отсутствуют составляющие справа от несущего колебания
B) в спектре отсутствуют составляющие на несущей частоте
C) в спектре отсутствуют составляющие слева от несущего колебания
D) спектр сигнала находится в области низких частот
ANSWER: B
Как называется процесс переноса спектра сигнала из области низких частот в область высоких частот при котором один или несколько параметров несущего колебания изменяются по закону передаваемого сообщения:
A) модуляция
B) демодуляция

C) кодирование
D) декодирование
ANSWER: A
Возможности (capabilities) потоков в Linux позволяют
A) Разделить возможности суперпользователя на несколько отдельных возможностей, которые могут быть разрешены независимо на уровне потока
B) Ограничить использование потоком процессорного времени
C) Разрешить прямой доступ к объектам ядра
ANSWER: A
При одновременном присутствии в списке контроля доступа разрешающей и запрещающей записи по одному и тому же виду доступа для одного и того же субъекта доступа в современных реализациях ОС MS Windows
A) Запрещающая запись имеет приоритет
B) Разрешающая запись имеет приоритет
C) Поведение системы не определено
ANSWER: A
В MS Windows под термином олицетворение (impersonation) понимают
A) Возможность выполнения потока в контексте безопасности, отличном от контекста безопасности своего процесса
B) Возможность идентифицировать владельца потока
C) Возможность удаленного запуска потока с использованием механизма RPC
ANSWER: A
Контроль учетных записей (User Account Control, UAC) в MS Windows реализует
A) Механизм защиты от вредоносных программ
B) Ограничение срока действия учетной записи
C) Контроль уровеня доверия к учетной записи
ANSWER: A
В UNIX-подлобных системах Sticky-bit (атрибут T) установленный для каталога имеет следующее действие
A) Не оказывает никакого действия для каталогов в современных реализациях операционных систем
B) Для новых файлов группой-владельцем становится группа-владелец каталога
C) Пользователь может удалять из каталога только файлы, которыми он владеет
D) Файлы из каталога нельзя объявить исполняемыми
ANSWER: C
В UNIX-подобных системах при вычислении хэша пароля используется дополнительный открытый ключ (соль), применение которого обеспечивает
A) Генерацию разного хэша для одинаковых паролей
B) Увеличение числа вариантов пароля
ANSWER: A
В UNIX-подобных системах атрибут разрешение исполнения (x) применительно к каталогу разрешает
A) Получить список имен файлов из каталога
B) Создавать файлы в каталоге
C) Удалять файлы в каталоге
D) Переходить в каталог
ANSWER: D
Для проверки подлинности данных, полученных через открытый канал или хранимых в ненадежном хранилище, может быть использован алгоритм

A) HMAC – hash-based message authentication code
B) HOTP – HMAC-Based One-Time Password Algorithm
C) TOTP – Time-based One-Time Password Algorithm
ANSWER: A
Политика безопасности это
A) Набор правил, регламентирующих порядок хранения и обработки информации
B) Перечень требуемых программ технической защиты информации и их настроек
C) Список ограничений на действия пользователей
ANSWER: A
Встроенный программный межсетевой экран в Linux и MS Windows обеспечивает
A) Фильтрацию сетевого трафика в соответствии с заданными правилами для предотвращения возможности использования злоумышленником уязвимостей сетевых протоколов и программного обеспечения
B) Шифрование и контроль целостности пакетов в сетевом трафике для защиты от подмены данных
ANSWER: A
Оценочный уровень доверия 1 обеспечивает
A) Минимальный уровень доверия, который подтверждает только наличие в составе ОС некоторых средств защиты
B) Уровень доверия от невысокого до умеренного, достигаемый при отсутствии доступа к полной документации по разработке ОС, основанный на анализе структуры ОС с использованием полученной от разработчика ОС дополнительной информации.
C) Умеренный уровень доверия, основанный на всестороннем методическом исследовании функций безопасности и процесса разработки ОС
D) Уровень доверия от умеренного до высокого в отношении уже существующей ОС общего назначения, основанный на всестороннем методическом тестировании и проверке реализации функций безопасности ОС, на уверенности в правильном использовании типовых методов при проектирования ОС.
E) Высокий уровень доверия для разрабатываемой ОС, основанный на использовании полуформальных методов при проектировании и тестировании ОС.
F) Уверенность в безопасности ОС при работе в условиях высокого риска, где ценность защищаемых данных оправдывает дополнительные затраты, основанную на использовании полуформальных методов при верификации и тестировании ОС
G) Уверенность в безопасности ОС при работе в условиях чрезвычайно высокого риска, где высокая ценность защищаемых данных оправдывает повышенные затраты, основанную на использовании формальных методов при верификации и тестировании ОС
ANSWER: A
Оценочный уровень доверия 4 (Наиболее высокий уровень доверия, достижимый при оценке существующих ОС общего назначения, так как боле высокий уровень доверия требует вмешательства в разработку ОС) обеспечивает
A) Некоторую уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией (в процессе реализации не были внесены неучтенные изменения)

B) Уверенность в том, что подсистема безопасности ОС реализована в соответствии с документацией

C) Высокую уверенность в том, что подсистема безопасности ОС реализована в соответствии с предъявляемыми требованиями

ANSWER: B

Выберите правильный вариант ответа:Совокупность методологических подходов к проблемам теоретической и практической философии, рассуждений о природе языка философии и его отношения к миру и человеку, состоящая в расчленении исследуемого явления на части – … .

A) философский синтез

B) философский анализ

C) исторический метод

D) логический метод

ANSWER: B

Выберите правильный вариант ответа:Какой вид познания основан на житейском опыте?

A) абстрактный

B) теоретический

C) обыденный

D) научный

ANSWER: C

Выберите правильный вариант ответа:Определенная целевая установка в решении научно-исследовательской проблемы – это … .

A) познавательная задача

B) познавательная проблема

C) метод решения

D) метод исследования

ANSWER: A

Выберите правильный вариант ответа:Что заставляет исследователя прийти в познавательном процессе к постановке новых проблем и задач?

A) противоречия в познании

B) успех

C) техника

D) неудачи

ANSWER: A

Выберите правильный вариант ответа:Мысленное решение задачи в особо трудной ситуации, когда нет твердой уверенности в положительном исходе, но есть некоторая надежда на успех, – это … .

A) риск

B) предположение

C) неопределённость

D) сложное решение

ANSWER: A

Выберите правильный вариант ответа:Что в системе познавательной деятельности является субъектом познания?

A) человек

B) материальные процессы

C) духовные процессы

D) природа

ANSWER: A

Выберите правильный вариант ответа:Какая форма в системе теоретического познания выполняет функцию предположения?

A) гипотеза

B) парадигма

C) проблема
D) теория
ANSWER: A
Выберите правильный вариант ответа:Абсолютная истина – это … .
A) полное, завершенное знание об объекте познания
B) знание на данном конкретно-историческом этапе общественного развития
C) знание в пределах одной научно-исследовательской парадигмы
D) неполное знание
ANSWER: A
Выберите правильный вариант ответа:Осознание человеком своей деятельности, мыслей, чувств, потребностей – это … .
A) самосознание
B) мировоззрение
C) миропонимание
D) бессознательное
ANSWER: A
Выберите пример, иллюстрирующий действие закона перехода количественных изменений в качественные:
A) социальная революция и переход к новой общественно-экономической формации
B) упавшая в землю семечка прорастает и дает жизнь дереву
C) смена поколений
D) нагревание воды приводит к ее кипению и переходу в парообразное состояние
ANSWER: D
Выберите правильный вариант ответа:Как называется сфера духовной жизни общества, основанная на вере в сверхъестественное?
A) мораль
B) право
C) духовность
D) религия
ANSWER: D
Выберите правильный вариант ответа:В рамках системного подхода синтез представляет собой … .
A) процесс сбора и интерпретации фактов, выявления проблемы и разложения системы на ее компоненты
B) соединение различных частей рассматриваемого сложного объекта в целостное образование
C) процесс восприятия предметов и явлений с целью их познания
D) процесс воздействия на реальный объект или его изучение в заданных условиях
ANSWER: B
Выберите правильный вариант ответа:В чем выражается самодостаточность общества как системы?
A) в способности к созданию всего необходимого для своего существования
B) в исключении из своей системы человека
C) в неизменности свойств на протяжении всего времени его существования
D) в статичности общества
ANSWER: A
Выберите правильный вариант ответа:Какую подсистему не включает общество как система?

A) социальную
B) политическую
C) духовную
D) эстетическую
ANSWER: D

Выберите правильный вариант ответа:В системе отношения человека и природы периодом господства природы над человеком является … .
A) мифологическая модель
B) научно-техническая модель
C) гуманистическая модель
D) информационная модель
ANSWER: A

Выберите правильный вариант ответа:Какое отношение характерно для эпохи ноосферы?
A) коэволюция человека и биосферы
B) подчинение человека природе
C) независимость человека от природы
D) господство человека над природой
ANSWER: A

Выберите правильный вариант ответа:Исходным отношением в системе познавательной деятельности является … .
A) оппозиция субъекта и объекта в процессе познания
B) зависимость субъекта от объекта познания
C) невозможность для субъекта выделить объект
D) познание объектом субъекта
ANSWER: A

Выберите правильный вариант ответа:Как называется метод генерировании нового знания, основанный на движении мысли от частного к частному, при котором учитывается сходство объектов в некоторых признаках?
A) дедукция
B) аналогия
C) индукция
D) анализ
ANSWER: B

Выберите правильный вариант ответа:Как называется метод исследования, основанный на мыслительном акте, приводящем к созданию идеальных объектов, не существующих в опыте и в действительности, однако необходимых для понимания сущности изучаемого объекта?
A) идеализация
B) исторический метод
C) аналогия
D) дедукция
ANSWER: A

Выберите правильный вариант ответа:В рамках какого направления в гносеологии отрицается принципиальная возможность познания мира?
A) агностицизм
B) скептицизм
C) оптимизм
D) гносеология
ANSWER: A

Выберите правильный вариант ответа:Чем по своим функциям в процессе познания является практика?
A) критерием истины

B) заменой мышления
C) способом бытия
D) способностью абстрагироваться от теоретического познания
ANSWER: A
Выберите правильный вариант ответа:К каком случае информацию можно считать полной?
A) если информация достаточна для понимания и принятия решения
B) если информация не решает познавательную неопределенность
C) если информация избыточна
D) если информация по данной теме отсутствует
ANSWER: A
Выберите правильный вариант ответа:Какую функции выполняет анализ проблемной ситуации с точки зрения системного подхода?
A) определяет цели и задачи системного анализа, методы принятия решений
B) ставит исследователя в тупик
C) позволяет отказаться от имеющихся методов исследования
D) ведет к смене научной парадигмы
ANSWER: A
Выберите правильный вариант ответа:Поскольку истина – это свойство знания, она … .
A) субъективна и зависит от человека
B) ненаучна
C) абсолютна
D) интертекстуальна
ANSWER: A
Выберите правильный вариант ответа:На основе какого метода в философии Ф. Бэкона развивался эмпиризм?
A) индукции
B) дедукции
C) анализа
D) синтеза
ANSWER: A
Выберите правильный вариант ответа:Как называется философская позиция, согласно которой в основе бытия лежит сознание?
A) идеализм
B) материализм
C) дуализм
D) плюрализм
ANSWER: A
Выберите правильный вариант ответа:Что является отличительной особенностью философского мышления в эпоху Возрождения?
A) теоцентризм
B) антропоцентризм
C) космоцентризм
D) сциентизм
ANSWER: B
Выберите правильный вариант ответа:Атеизм отрицает … .
A) Бога
B) человека
C) материю и сознание
D) сознательное и бессознательное
ANSWER: A

Выберите правильный вариант ответа:Что НЕ относится к чувственному познанию?

A) ощущение

B) восприятие

C) представление

D) понятие

ANSWER: D

Выберите правильный вариант ответа:В чем состоит сущность реляционной концепции пространства и времени?

A) время вечно, пространство бесконечно

B) время и пространство не зависят друг от друга

C) пространство и время относительны и зависят от материальных процессов

D) время и пространство – ноуменальные сущности

ANSWER: C

Укажите основной вопрос гносеологии:

A) что первично?

B) познаваем ли мир?

C) что такое человек?

D) что я должен делать?

ANSWER: B

Выберите правильный вариант ответа:Как может быть охарактеризована дуалистическая система?

A) утверждает наличие двух субстанций

B) утверждает наличие одной субстанции

C) утверждает веру в единого Бога

D) отрицает вселенную

ANSWER: A

Выберите философскую школу эпохи эллинизма:

A) экзистенциализм

B) позитивизм

C) эпикуреизм

D) номинализм

ANSWER: C

Выберите правильный вариант ответа:Принцип всеобщей связи и развития в системном подходе … .

A) позволяет реализовать взаимосвязь философских положений и методов конкретных наук

B) позволяет поставить вопрос о смысле существования

C) предполагает дифференциацию философских направлений

D) не имеет применения в системном подходе

ANSWER: A

Выберите правильный вариант ответа:Философская категория, выражающая протяженность и взаимное расположение объектов, – это ... .

A) пространство

B) время

C) движение

D) атрибутивность

ANSWER: A

Выберите правильный вариант ответа:Как называется направление, в котором провозглашается наличие множества субстанций?

A) монизм

B) одномерность

C) дуализм

D) плюрализм
ANSWER: D
Выберите правильный вариант ответа:Как в марксизме называется определенный этап развития человечества, отличающийся способом производства материальных благ?
A) культура
B) цивилизация
C) социокультурная суперсистема
D) общественно-экономическая формация
ANSWER: D
Выберите правильный вариант ответа:Какой фразой можно выразить роль философии в средние века?
A) «царица наук»
B) «наука наук»
C) «служанка богословия»
D) «учение о счастье»
ANSWER: C
Выберите правильный вариант ответа:Каким методом познания пользовались рационалисты Нового времени?
A) индукция
B) дедукция
C) аналогия
D) противоречие
ANSWER: B
Выберите правильный вариант ответа:В каком обществе научно-технические изобретения и открытия оказывают наиболее сильное воздействие на социальные изменения?
A) в примитивном
B) в традиционном
C) в индустриальном
D) в информационном
ANSWER: D
Выберите правильный вариант ответа:Уподобление общества как системы биологическому организму характерно для философии … .
A) позитивизма
B) экзистенциализма
C) идеализма
D) иррационализма
ANSWER: A
Выберите правильный вариант ответа:Аграрный сектор занимает наибольший удельный вес в структуре занятости … .
A) информационного общества
B) традиционного общества
C) индустриального общества
D) постиндустриального общества
ANSWER: B
Выберите наиболее характерный признак постиндустриального общества:
A) религия
B) информация
C) земля
D) великие географические открытия
ANSWER: B

Выберите правильный вариант ответа:Чем определялась ценность человеческой деятельности для гуманистов эпохи Возрождения?

A) заслугами перед Богом

B) происхождением

C) личными заслугами и творчеством

D) социальной принадлежностью

ANSWER: C

Выберите правильный вариант ответа:Принцип иерархии в системном подходе направлен на … .

A) установление порядка подчинения нижестоящих элементов и свойств вышестоящим по строго определенным ступеням и переход от низшего уровня к высшему

B) исследование объекта как единого целого

C) исследование объекта как части более крупной системы, в которой анализируемый объект находится с остальными системами в определенных отношениях

D) оценку количественные характеристики объектов

ANSWER: A

Выберите правильный вариант ответа:Какой из указанных законов НЕ относится к законам диалектики?

A) закон единства и борьбы противоположностей

B) закон перехода количественных изменений в качественные

C) закон отрицания отрицания

D) закон трех стадий

ANSWER: D

Выберите правильный вариант ответа:Традиция европейского рационализма связана с именем … .

A) Ф. Бэкона

B) Р. Декарта

C) Т. Гоббса

D) Дж. Локка

ANSWER: B

Выберите правильный вариант ответа:Оптимальное решение – это… .

A) решение, которое по тем или другим признакам предпочтительнее других

B) ситуация, не имеющая решения

C) тупиковая ситуация

D) условия, в которых отсутствует алгоритм решения проблемной ситуации

ANSWER: A

Выберите правильный вариант ответа:Представителями Римского клуба был поставлен вопрос о «пределах роста» цивилизации для решения какой проблемы?

A) роста численности населения и исчерпаемости природных ресурсов

B) экологической

C) метафизической

D) мировых войн

ANSWER: A

Выберите правильный вариант ответа:В чем заключается недостаток точки зрения Эпикура на проблему смерти?«Когда мы есть, то смерти еще нет, а когда смерть наступает, то нас уже нет. Таким образом, смерть не существует ни для живых, ни для мертвых, так как для одних она сама не существует, а другие для нее сами не существуют».

A) отсутствии проблематизации смерти, в связи с чем значимость этого феномена для бытия человека недооценивается

B) запугивании человека

C) расслаблении человека

D) отвлечении человека от земных помыслов

ANSWER: A

Выберите правильный вариант ответа:Что формирует образцы, следуя которым, человек раскрывает себя в мире?

A) культура

B) онтология

C) гносеология

D) логика

ANSWER: A

Выберите правильный вариант ответа:Что обуславливает поисковую деятельность в целях разрешения проблемной ситуации?

A) несоответствие фактов имеющимся теориям

B) иррациональное желание

C) стремление к научной деятельности

D) желание достичь успеха

ANSWER: A

Выберите правильный вариант ответа:Когда возникают проблемные ситуации?

A) при попытке самостоятельно достигнуть поставленные практические цели

B) при анализе противоречивых жизненных ситуаций

C) при выполнении практических заданий, в ходе которых появляются познавательные противоречия

D) все варианты верные

ANSWER: D

Выберите правильный вариант ответа:Какой метод решения проблемных ситуаций, применяемый в Античности, наиболее эффективно ориентировал на глубокое и прочное усвоение знаний при совместной работе философа и аудитории?

A) беседа

B) лекция

C) нравоучение

D) эксперимент

ANSWER: A

Выберите правильный вариант ответа:Словесным методом решения проблемных ситуаций является … .

A) объяснение

B) восприятие

C) чтение

D) повторение

ANSWER: A

Выберите правильный вариант ответа:В рамках системного подхода исследуемый объект рассматривается как … .

A) целое независимо от изучаемого аспекта объекта и с учетом выявления внутренних закономерностей развития объекта

B) одна из частей, обладающая своими уникальными характеристиками

C) анализируются частные проблемы в познании объекта

D) исследуется только лишь механизм функционирования объекта без выявления закономерностей его развития

ANSWER: A

Выберите правильный вариант ответа:Что относится к практическим методам решения проблемных ситуаций?

A) упражнения

B) решение проблемно-ориентированных задач

C) ситуативные игры

D) все ответы правильные

ANSWER: D

Укажите метод решения проблемных ситуаций, позволяющий расширить и углубить знания, развить мыслительную деятельность, выработать умение решать сложные вопросы посредством поискового диалога, выйти из сложных ситуаций и сформировать убеждения:

A) дискуссия

B) наблюдение

C) рассуждение

D) эксперимент

ANSWER: A

Выберите правильный вариант ответа:Что представляет собой поиск различных путей и способов решения проблемной ситуации для достижения целей?

A) разработку вариантов решения проблем

B) размышление

C) рассуждение

D) отказ от решения проблемы

ANSWER: A

Выберите правильный вариант ответа:С помощью чего, по мнению К. Маркса, решается проблема противоречия производительных сил производственных отношений?

A) социальной революции, которая приводит к смене общественно-экономической формации

B) размышления о способах решения проблемы

C) отвержения производительных сил

D) разрушения производственных отношений

ANSWER: A

Выберите правильный вариант ответа:Что является достоинством гуманистического мировоззрения?

A) ориентация на защиту достоинства и самоценности личности

B) отстаивание националистических идей

C) атеизм

D) возможность в рамках данного мировоззрения не обращать внимание на проблему свободы

ANSWER: A

Выберите правильный вариант ответа:Какой метод решения проблемных ситуаций используется в философском познании?

A) индуктивный

B) дедуктивный

C) проективный

D) все ответы правильны

ANSWER: D

Выберите правильный вариант ответа:Определенное видоизменение известных вариантов в условиях наличия в прошлом аналогов проблемных ситуаций является таким решением, как… .

A) решение-усовершенствование

B) стандартное решение

C) оригинальное решение

D) все ответы правильны
ANSWER: A

Выберите правильный вариант ответа:Какие решения необходимы в тупиковых проблемных ситуациях, когда все известные решения не могут быть реализованы на практике?
A) решения-усовершенствования
B) стандартные решения
C) оригинальные решения
D) все ответы правильны
ANSWER: C

Выберите правильный вариант ответа:Какие решения применяются в типовых проблемных ситуациях?
A) решения-усовершенствования
B) стандартные решения
C) оригинальные решения
D) все ответы правильны
ANSWER: B

Выберите правильный вариант ответа:Неразвитая проблема в гносеологии – это … .
A) проблема, у которой отсутствует алгоритм решения
B) плохо сформулированная проблема
C) отсутствующая проблема
D) решенная проблема
ANSWER: A

Выберите правильный вариант ответа:Как называется интеллектуальное затруднение, возникающее в ситуации неопределенности, когда человек не знает, как объяснить данное явление, факт, процесс действительности, не может достичь цель известным ему способом, что побуждает искать новый способ объяснения или способ действия?
A) проблемная ситуация
B) пограничная ситуация
C) противоречие
D) тупик
ANSWER: A

Выберите правильный вариант ответа:В каком эвристическом методе ошибка осмысливается в качестве источника новых знаний, способа обнаружения исключений из правил или предположений, противопоставленных общепринятым?
A) методе проб и ошибок
B) функциональном анализе
C) методе эвристических вопросов
D) методе аналогии
ANSWER: A

Выберите правильный вариант ответа:Какой эвристический метод переносит акцент исследования с содержания предмета или явления на его функции?
A) метод проб и ошибок
B) функциональный анализ
C) метод эвристических вопросов
D) метод аналогии
ANSWER: B

Выберите правильный вариант ответа:Какой эвристический метод использует проблемные вопросы для упорядочивания информации в ходе решения проблемы?

A) методе проб и ошибок
B) функциональный анализ
C) метод эвристических вопросов
D) метод аналогии
ANSWER: C

Укажите четыре причины бытия, на основании которых мы можем осмыслить проблему существования вещи, по мнению Аристотеля:
A) формальная, целевая, действующая, материальная
B) формальная, сущностная, целевая и движущая
C) материальная, протяженная, действующая, сосуществующая
D) материальная, пространственная, действующая, идеальная
ANSWER: A

Выберите правильный вариант ответа:Какой оптимальный метод решения проблемной ситуации используется в рационализме?
A) дедукция
B) индукция
C) аналогия
D) абдукция
ANSWER: A

Выберите правильный вариант ответа:В эмпиризме какой путь решения проблемных ситуаций в познании является наиболее приоритетным из предложенных?
A) опытный
B) метафизически
C) рациональный
ANSWER: A

Выберите правильный вариант ответа:В рамках системного подхода анализ представляет собой … .
A) процесс сбора и интерпретации фактов, выявления проблемы и разложения системы на ее компоненты
B) соединение различных частей рассматриваемого сложного объекта в целостное образование
C) процесс восприятия предметов и явлений с целью их познания
D) процесс воздействия на реальный объект или его изучение в заданных условиях
ANSWER: A

Выберите правильный вариант ответа:Как называется способ решения практических и теоретически задач, основанный на мысленном отвлечении от несущественных свойств изучаемого предмета и выделении одной или нескольких существенных характеристик?
A) аналогия
B) моделирование
C) абстрагирование
D) исторический метод
ANSWER: C

Выберите правильный вариант ответа:Что такое жизненный цикл проекта?
A) набор фаз, через которые проходит проект с момента его инициации до момента закрытия
B) точное и полное расписание проекта с учетом работ, их длительностей, необходимых ресурсов, которое служит основой для исполнения проекта
C) полный перечень работ проекта
D) период, в течение которого проект приносит прибыль

ANSWER: A

Выберите правильный вариант ответа:Структурная декомпозиция работ проекта — это …

A) графическое изображение иерархической структуры всех работ проекта

B) направления и основные принципы осуществления проекта

C) дерево ресурсов проекта

D) организационная структура команды проекта

ANSWER: A

Выберите правильный вариант ответа:На какой вопрос не дает ответ метод критического пути?

A) Каков срок окупаемости проекта?

B) На какое время можно отложить выполнение некритических работ, чтобы они не повлияли на сроки выполнения проекта?

C) Сколько времени потребуется на выполнение всего проекта?

D) Какие работы являются критическими и должны быть выполнены в точно определенное графиком время?

ANSWER: A

Выберите правильный вариант ответа:Какая работа называется критической?

A) Длительность которой максимальна в проекте

B) Стоимость которой максимальна в проекте

C) Работа с максимальными трудозатратами

D) Работа, для которой задержка ее начала приведет к задержке срока окончания проекта в целом

ANSWER: D

Выберите правильный вариант ответа:В чем заключается основное отличие бюджета от сметы проекта?

A) В бюджете затраты распределяются во времени, а в смете содержится только перечень затрат и их размер

B) Бюджет включает более широкий перечень затрат, чем смета

C) Бюджет включает плановые значения затрат, а смета - фактические

D) Ничем, эти понятия синонимы

ANSWER: A

Выберите правильный вариант ответа:Что называется точкой безубыточности?

A) объем производства продукции (оказания услуг), при котором предприятие получает запланированную прибыль

B) реальный объем выпуска продукции

C) разница между выручкой и затратами предприятия

D) объем реализации продукции, который позволит предприятию покрыть все расходы и выйти на нулевой уровень прибыли

ANSWER: D

Выберите правильный вариант ответа:Прибыль, остающаяся в распоряжении предприятия после уплаты всех налогов, называется …

A) валовая прибыль

B) чистая прибыль

C) балансовая прибыль

D) налогооблагаемая прибыль

ANSWER: B

Выберите правильный вариант ответа:При каком периоде окупаемости целесообразны инвестиции в проект?

A) период окупаемости не выходит за рамки жизненного цикла проекта

B) выходит за рамки жизненного цикла проекта

C) меньше 3 лет
D) не определен
ANSWER: A
Выберите правильный вариант ответа:Проект является убыточным, если его чистый дисконтированный доход (ЧДД, NPV, Net Present Value) …
A) отрицательный
B) положительный
C) равен нулю
D) не определен
ANSWER: A
Выберите правильный вариант ответа:Метод освоенного объема позволяет …
A) оптимизировать сроки выполнения проекта
B) определить отставание/опережение хода реализации работ по графику и перерасход/экономию бюджета проекта
C) определить продолжительность отдельных работ проекта
D) освоить максимальный объем бюджетных средств
ANSWER: B
Выберите правильный вариант ответа:Что является основной причиной конфликтов в проекте как системе?
A) противоречие потребностей сохранения существующей системы и реализации целевых установок
B) отсутствие взаимопонимания в трудовом коллективе
C) несовпадение целей участников процесса
ANSWER: C
Что из нижеследующего лучше всего описывает план управления проектом?
A) Распечатка из информационной системы по учету проектов
B) Диаграмма Ганта
C) Содержание, стоимость, риски, ресурсы и прочие планы
D) Содержание проекта
ANSWER: C
Выберите правильный вариант ответа:Матрица ответственности – это ...
A) структура ответственности всех лиц, принимающих участие в реализации задач проекта
B) штатное расписание проекта
C) система поощрений и наказаний сотрудников компании, принимающих участие в реализации проекта
D) распределение работников по группам для решения задач проекта
ANSWER: A
Выберите правильный вариант ответа:Кто является владельцем проекта и будущим потребитель его результатов?
A) инвестор
B) куратор проекта
C) команда проекта
D) заказчик проекта
ANSWER: D
Выберите правильный вариант ответа:Кто из членов команды управления проектом, лично отвечает за все результаты проекта?
A) руководитель проекта
B) куратор проекта
C) инициатор проекта
D) заказчик проекта
ANSWER: A

Выберите правильный вариант ответа:Управление коммуникациями проекта – это …

A) набор программно-компьютерных комплексов

B) управленческая функция, направленная на обеспечение своевременного сбора, генерации, распределения и сохранения необходимой проектной документации

C) набор документов, регламентирующих процессы обработки информации в проекте

D) правила взаимодействия между членами команды проекта

ANSWER: B

Какие из нижеперечисленных критериев позволяют оценить эффективность коммуникаций в проекте?

A) нагрузка на участников распределена в соответствии с планом работ

B) участники команды знают актуальные цели проекта и свою роль в команде

C) участники не отвлекают друг друга неважными и несрочными вопросами в рабочее время

D) все вышеперечисленное

ANSWER: D

Выберите условие, при котором целесообразно использовать гибкий (итеративный) подход к планированию проекта:

A) Бюджет проекта строго ограничен

B) Нужна детальная документация по всем процессам разработки

C) Продукт разрабатывается в сфере, подверженной постоянным изменениям

D) Продукт должен быть создан к конкретному сроку

ANSWER: C

Выберите правильный вариант ответа:В чем различие между скрамом и аджайлом?

A) Agile – это культура, включающая в себя различные подходы гибкого управления. Scrum – фреймворк, шаблон рабочего процесса, помогающий командам вести совместную работу

B) Это одно и то же

C) Скрам – это равносильное аджайлу направление в сфере гибких методологий, основанное на применении итеративного подхода с временным интервалом. В аджайле же основной упор – на равенство ролей в команде

D) Agile можно применять в различных сферах, а Scrum – исключительно в ИТ

ANSWER: A

При использовании гибких технологий управления проектом в спринт попадают задачи, которые …

A) имеют самый высокий приоритет

B) берет Scrum мастер

C) не являются сложными

D) имеют четко сформулированные и описанные требования

ANSWER: A

Выберите правильный вариант ответа:Как звучит основная идея Agile?

A) люди и взаимодействие важнее процессов и инструментов

B) работающий продукт важнее исчерпывающей документации

C) сотрудничество с заказчиком важнее согласования условий контракта

D) готовность к изменениям важнее следования первоначальному плану

E) все вышеперечисленное

ANSWER: E

Выберите правильный вариант ответа:Что из нижеперечисленного является наиболее универсальным инструментом канбан, который можно использовать в любом процессе и в любой отрасли?

A) канбан-доска

B) канбан-окно

C) канбан-тетрадь

D) канбан-задача

ANSWER: A

Выберите правильный вариант ответа:Могут ли фазы проекта перекрывать друг друга?

A) Да, если этого требует технология реализации проекта

B) Нет, фазы должны следовать одна за другой

C) В зависимости от объемов трудозатрат

D) В зависимости от наличия подрядных организаций

ANSWER: A

Выберите правильный вариант ответа:Легитимизация конфликта – это …

A) придание конфликту широкой огласки

B) достижение соглашения между конфликтующими сторонами по признанию и соблюдению установленных норм и правил поведения в конфликте

C) создание соответствующих органов и рабочих групп по регулированию конфликтного взаимодействия

D) определение места и времени переговоров по разрешению конфликта

ANSWER: B

Выберите правильный вариант ответа:Что такое "водопадный" тип жизненного цикла?

A) Жизненный цикл, при котором фазы связаны через ресурсы проекта

B) Жизненные цикл, при котором вехи проекта реализуются одна за другой

C) Жизненные цикл, при котором задачи проекта реализуются одна за другой

D) Жизненный цикл, при котором фазы проекта реализуются одна за другой

ANSWER: D

В проектном менеджменте вехой называют …

A) набор логически взаимосвязанных работ проекта, в процессе завершения которых достигается один из основных результатов проекта

B) полный набор последовательных работ проекта

C) ключевое событие проекта, используемое для осуществления контроля над ходом его реализации

D) начало выполнения проекта

ANSWER: C

Выберите правильный вариант ответа:Зачем используется метод критического пути?

A) для планирования рисков проекта

B) для планирования мероприятий по выходу из критических ситуаций

C) для оптимизации (сокращения) сроков реализации проекта

D) для определения продолжительности выполнения отдельных работ

ANSWER: C

Выберите правильный вариант ответа:Два события в сетевом графике могут быть соединены …

A) только одной работой

B) несколькими работами

C) одной или более работами

ANSWER: A

Выберите правильный вариант ответа:Что такое критический путь проекта?

A) Последовательность взаимосвязанных работ

B) Последовательность независимых работ

C) Самая короткая последовательность работ в проекте

D) Самая длинная последовательность работ

ANSWER: D

Выберите правильный вариант ответа:При необходимости подготовить коллектив к деятельности в экстремальной ситуации целесообразной формой социально-психологической работы с группой будет … .

A) деловая игра

B) тренинг переговоров

C) тренинг стрессоустойчивости

D) консультация руководителя группы по вопросам управления коллективом в экстремальных ситуациях

ANSWER: C

Какая модель командных ролей описывает восемь рабочих функций в процессе управления, анализирует типы задач, решаемых командой, и дает возможность оптимизировать управленческую деятельность?

A) концепция командных ролей Р.М. Белбина

B) «колесо команды» Марджерисона – Мак-Кена

C) модель управленческих ролей Т.Ю. Базарова

D) все перечисленные выше модели

ANSWER: B

Британский бизнес-консультант и психолог М.Вудкок разработал методику диагностики команды, которая была названа его именем – «Тест Вудкока». На оценку какого фактора направлена данная методика?

A) оценка эффективности работы в команде

B) оценка групповой конформности

C) оценка групповой идентичности

D) оценка распределения функциональных обязанностей в команде

ANSWER: A

Выберите правильный вариант ответа:Какова оптимальная численность человек в тренинговой группе?

A) 8-15

B) 3-4

C) 25

D) 1

ANSWER: A

Выберите правильный вариант ответа:Если в организации возникают проблемы, связанные с созданием или реформирование существующих организационных структур, то руководителю рекомендуется применять … .

A) проектировочные игры

B) имитационные игры

C) управленческие игры

D) терапевтические игры

ANSWER: A

Укажите оптимальную форму групповой работыдля ознакомления новых сотрудников с правилами и нормами организации:

A) деловая игра

B) тренинг командообразования

C) лекция о групповых правилах и нормах

D) коммуникативный тренинг

ANSWER: C

Выберите правильный вариант ответа:Межличностные отношения и общение, доверие и сплоченность составляют … .

A) деловой аспект групповой жизни

B) социальный аспект групповой жизни

C) управленческий аспект групповой жизни

D) групповое развитие

ANSWER: B

Какая роль относится к рабочей задаче «Консультирование» согласно модели командных ролей Марджерисона – Мак-Кена?

A) «Докладчик-консультант». Справляется со сбором информации. Избегает конфликтов и прямых столкновений

B) «Специалист по оценке и развитию». Испытывает желание продвигать идеи и внедрять нововведения, склонен к проектной деятельности

C) «Координатор-организатор». Склонен оказывать влияние на события, легко принимает решение, преодолевая конфликтные ситуации

D) «Инспектор-контролер». Предпочитает работать самостоятельно, его вклад будет виден и эффективен, если команда понимает, что от него требуется

ANSWER: A

Выберите правильный вариант ответа:Команда с большей вероятностью столкнется с конфликтами, если … .

A) цели и задачи компании не ясны или не доведены до всех членов

B) уменьшить на 1 час рабочую неделю

C) устраивать совместные корпоративы

D) увеличить премию

ANSWER: A

Выберите правильный вариант ответа:Что является главным средством поддержания сплоченности и внутренней стабильности группы по З. Фрейду?

A) аутгрупповая враждебность

B) устранение относительной депривации

C) перевод ситуации конкуренции в ситуацию кооперации

D) полимотивированность деятельности

ANSWER: A

Выберите правильный вариант ответа:Согласно Н.В. Семилету, интеракционные дискуссии – это … .

A) дискуссии, в которых обсуждаются значимые для всех участников тренинговой группы вопросы и проблемы

B) дискуссии, ориентированные на прошлый опыт, в которых анализируются трудности личной или профессиональной жизни отдельного участника

C) дискуссии, материалом которых служат структура и содержание взаимоотношений между участниками группы

D) дискуссии, материалом которых служит содержание отдельных упражнений и игр тренинга, в ходе которых необходимо выполнить какую-либо задачу

ANSWER: C

Выберите правильный вариант ответа:При диагностике социального аспекта групповой жизни малой группы и/или команды (межличностные отношения и общение) используют … .

A) методы и диагностики функционально-ролевых позиций в группе

B) методы диагностики ролевых конфликтов

C) метод социометрии, методы исследования групповой сплоченности

D) методики диагностики стилей руководства командой

ANSWER: C

Укажите стратегию ведения групповой дискуссии, при которой у ведущего есть четкий плана ее проведения (группе предлагаются темы для обсуждения и способы их проработки):

A) свободная форма

B) программированная форма

C) компромиссная форма

D) комбинированная форма

ANSWER: B

Выберите правильный вариант ответа:Дискуссионная группа – это… .

A) группа, собирающаяся для того, чтобы помочь участникам говорить о своих проблемах и решать их в атмосфере взаимной поддержки

B) группа для подготовки праздника

C) группа для выезда на пикник

D) шопинг-группа

ANSWER: A

Какая из командных стратегий (стилей руководства) наиболее эффективна при руководстве творческим коллективом или научной группой, где каждому члену присущи самостоятельность и творческая индивидуальность?

A) демократическая

B) либеральная

C) авторитарная

D) смешанная

ANSWER: B

Какая команда может быть создана для решения необычного разового задания, требующего уникальных креативных решений?

A) вертикальная

B) горизонтальная

C) специализированная

D) виртуальная

ANSWER: C

Укажите ролевые позиции в команде, выделенные в концепции Т. Ю. Базарова:

A) координатор – реализатор – контролер – мотиватор

B) организатор – администратор – контролер – мотиватор

C) организатор – администратор – управленец – руководитель

D) координатор-организатор-управленец-мотиватор

ANSWER: C

Выберите правильный вариант ответа:Для оценки специфики отношений в системе «индивид-группа (команда)» необходимо определить … .

A) степени выраженности ролевого конфликта в деятельности команды

B) личностные характеристики, влияющие на организационное и групповое поведение индивида

C) уровень развития группы как команды

D) отношение к работе, продуктивность

ANSWER: B

На какой из нижеперечисленных фаз тренинга формирование конструктивных стратегий взаимодействия происходит наиболее оптимально:

A) фаза неуверенности и зависимости (фаза ориентации)

B) фазы борьбы, бунта, напряжения и агрессии

C) фаза выработки групповых норм, развития и сотрудничества

D) рабочая фаза. Основные изменения личности и поведения участников. Достигаются цели активного социально-психологического обучения

ANSWER: D

Выберите правильный вариант ответа:В самом общем виде ролевую стратегию руководителя можно охарактеризовать как … .

A) родительскую или партнерскую

B) конфликтную

C) экспериментальную

D) компромиссную

ANSWER: A

Выберите правильный вариант ответа:Изучение делового аспекта групповой жизни команды включает в себя диагностику … .

A) межличностных отношений и общения

B) восприятия индивидом группы, конформизм и конформность

C) структуры функционального распределения ролей, отношения к работе, продуктивности, принятия решений

D) методов диагностики социально-психологического климата группы

ANSWER: C

Выберите несуществующий стиль руководства командой:

A) авторитарный

B) демократический

C) экспериментальный

D) либеральный

ANSWER: C

Выберите правильный вариант ответа:Когда зародилось командообразование как специальный вид деятельности?

A) в конце 15 века

B) во второй половине 20 века

C) в начале 16 века

D) во второй половине 14 века

ANSWER: B

Выберите правильный вариант ответа:Кто впервые обратил внимание на важность ролевого распределения внутри команды для максимально упрощенного и быстрого обмена информацией, а также выработки наиболее эффективных способов коммуникации между членами группы?

A) Т.В. Черниговская

B) Роршах

C) М. Белбин

D) Д. Карнеги

ANSWER: C

Выберите правильный вариант ответа:Для понимания особенностей выстраивания контакта при руководстве командой важно ориентироваться на сущность следующих фаз контакта, выделенных Ф. Перлзом:

A) преконтакт, контакт, финальный (полный) контакт, постконтакт

B) зарождение идеи, кодирование и выбор канала, передача, декодирование

C) отправитель, сообщение, канал связи, получатель

D) знакомство, решение совместной задачи, прерывание

ANSWER: A

Выберите правильный вариант ответа:Что является сутью организационных задач процесса управления, по Т.Ю. Базарову?

A) планирование и изменение положения организации на рынке

B) проектирование бизнес-процессов и организационной структуры, разработка мероприятий по достижению целей организации

C) управление ресурсами и их распределение

D) направление потенциала сотрудников, урегулирование человеческого фактора

ANSWER: B

Выберите правильный вариант ответа:Что необходимо знать о потребностях членов команды (с опорой на работы А. Маслоу) для эффективного руководства ими?

A) соотносятся ли они с духовным здоровьем

B) актуализированный и следующий в иерархии уровень потребностей

C) ограничения в удовлетворении ряда базовых потребностей

D) способы удовлетворения потребностей, доступные сотрудникам

ANSWER: B

Какая управленческая роль в команде, согласно модели Т.Ю. Базарова, имеет четкое видение итогового результата и способна проектировать этапы его достижения, гибко учитывать ограничения при проектировании структур и технологий?

A) организатор

B) управленец

C) руководитель

D) администратор

ANSWER: A

Выберите правильный вариант ответа:Самосознание личности в психологии – это … .

A) осознание индивидом собственных потребностей, способностей, мотивов поведения, мыслей

B) анализ совершенных поступков в разные периоды времени

C) установка на прохождение предначертанного жизненного пути

D) мера принятия или непринятия индивидом самого себя

ANSWER: A

Выберите правильный вариант ответа:Под саморазвитием в психологии понимают … .

A) процесс количественных и качественных изменений унаследованных и приобретенных свойств и качеств личности

B) это деятельность и способность личности, связанные с умением организовать себя

C) развитие, обусловленное внутренней активностью личности, характеристика внутренней способности личности к работе над собой, к росту, развитию

D) это процесс формирования целостного, относительно постоянного эмоционального отношения к себе

ANSWER: C

Выберите правильный вариант ответа:Какие умения в системе самоорганизации студентов характеризуют их самостоятельность в приобретении и использовании знаний из различных источников для решения практических задач?

A) организационные

B) информационные

C) интеллектуальные

D) деловые

ANSWER: B

Выберите правильный вариант ответа:Становление психодиагностики как самостоятельной области знаний происходит в … .

A) во второй половине 14 века
B) в конце 15 века
C) в начале 19 века
D) в начале 21 века
ANSWER: C

Выберите правильный вариант ответа:Какой автор рассматривает личность, как совокупность внутренних условий, через которые преломляются все внешние воздействия?
A) С.Л. Рубинштейн
B) И.П. Павлов
C) А.С. Макаренко
D) В.В. Виноградов
ANSWER: A

Выберите правильный вариант ответа:Какое направление психотерапии работает с проблемами и неврозами клиента через процедуры телесного контакта?
A) когнитивно-поведенческое
B) гештальт-терапия
C) экзистенциальная психология
D) телесно-ориентированное
ANSWER: D

Выберите правильный вариант ответа:Расхождение между текущим организмическим опытом и Я-концепцией, противоречие между реальным переживанием и тем, как человек себя воспринимает и проявляет, К.Р.Роджерс называет … .
A) конфликтом
B) некогруэнтностью
C) неврозом
D) низкой осознанностью
ANSWER: B

Выберите правильный вариант ответа:Эксперимент Вертхеймера, посвященный изучению восприятия кажущегося движения предметов, позволил установить явление, названное… .
A) гештальт
B) изоморфизм
C) фи-феномен
D) инсайт
ANSWER: C

Выберите правильный вариант ответа:Понятие «локус контроля» в научную терминологию ввел … .
A) К. Юнг
B) Дж. Роттер
C) З. Фрейд
D) К. Роджерс
ANSWER: B

Выберите правильный вариант ответа:Понятие «Пирамида потребностей» принадлежит … .
A) Роджерсу
B) Маслоу
C) Адлеру
D) Климову
ANSWER: B

Укажите представителя «постфрейдизма»:
A) С. Пинкер

B) З. Фрейд
C) Э. Фромм
D) Е. Климов
ANSWER: C

Выберите правильный вариант ответа:Сведения о том, что выбранная методика действительно измеряет то, для чего она предназначена, содержатся в понятии … .
A) надежность
B) валидность
C) репрезентативность
D) объективность
ANSWER: B

Выберите правильный вариант ответа:Классический психоанализ ... .
A) опирался на понятие фона и фигуры
B) сделал предметом бессознательные влечения человека
C) ввел в психологию «архетипы»
D) ввел в психологию понятие «Пирамида потребностей»
ANSWER: B

Выберите правильный вариант ответа:Метод парадоксальной интенции В. Франкла успешно применяется при работе … .
A) с фобиями
B) с заиканием
C) с инфантильностью
D) с прокрастинацией
ANSWER: A

Выберите правильный вариант ответа:В чем заключается метод парадоксальной интенции В. Франкла?
A) в освоении навыков расслабления за счет дыхания
B) в работе с разрешением когнитивного диссонанса
C) в концентрации на расслабленности/напряженности отдельных участков собственного тела
D) в попытках человека в случае фобии возжелать то, что составляет суть его опасений
ANSWER: D

Руководством Вашей компании было принято решение увеличить длительность рабочего дня ваших подчиненных на 1 час без увеличения заработной платы за дополнительное время. Задача донести эту информацию на подчиненных на оперативном совещании таким образом, чтобы оно было принято положительно. Какой из ответов считается наиболее приемлемым и правильным?
A) Руководитель 1. Уважаемые коллеги! У меня для вас не очень приятная новость. Для решения оперативных задач нам необходимо поработать более напряженно, чем обычно. В связи с этим, начиная с сегодняшнего дня на работе нужно оставаться на час дольше. Эта мера временная, вопрос дополнительной оплаты будем обсуждать с руководством по итогам нашей работы. Я также остаюсь на работе вместе с Вами анализировать то что мы наделали за день придется вечером, так что я буду на работе практически до ночи, кто хочет остаться дольше – присоединяйтесь!
B) Руководитель 2. На общем собрании: «Довожу до Вашего сведения, что был сделан расчет специалистами, на основании которого для дальнейшей прибыльной работы Общества необходимо увеличить длительность рабочего дня нашего отдела на 1 час без увеличения заработной платы за дополнительное время. При продолжении работы в настоящем режиме нас ждёт отрицательный доход и в дальнейшем – ликвидация

Общества. Я надеюсь, что увеличение длительности рабочего времени будет временным на 3-6 месяцев и наше Общество выйдет в ближайшее время из затруднительного положения. В нашем отделе работают порядочные сотрудники, на взаимовыручку которых руководство Общества надеется. Готова ответить на Ваши вопросы, предложения

C) Руководитель 3. Добрый день, коллеги! С завтрашнего дня мы будем с вами видеться чаще, общаться и обсуждать производственные вопросы активней и больше, и на это у нас есть 1 дополнительный рабочий час. И это все благодаря не переходу на «летнее» время. А исключительно во благо процветания нашей компании. Рабочее время увеличится, зарплата нет, но усилиями нашего сплоченного коллектива мы улучшим результаты нашей работы и заработаем богатую премию.

ANSWER: C

Выберите правильный вариант ответа:Выделение себя из среды; осознание себя, как субъекта, автономного от физической и социальной среды; осознание своего внутреннего опыта – это критерии… .

A) самосознания

B) самооценки

C) саморегуляции

D) самоконтроля

ANSWER: A

Выберите правильный вариант ответа:Какая основная функция самооценки в психической жизни личности?

A) осознание своего внутреннего опыта

B) выступает необходимым внутренним условием регуляции поведения и деятельности личности

C) защищает уникальность личности от угрозы ее нивелирования

D) обеспечивает потребность человека в признании себя обществом

ANSWER: B

Выберите правильный вариант ответа:Согласно гуманистическим теориям самореализация тесно связана … .

A) с комплексом превосходства

B) с самоуважением

C) с переоценкой собственного «Я»

D) со способностью любить

ANSWER: B

Укажите лишнее свойство личности:

A) активность

B) реактивность

C) направленность

D) самосознание

ANSWER: B

Выберите правильный вариант ответа:В рамках какой теории личность представляется как совокупность поведенческих реакций?

A) бихевиоризм

B) психоанализ

C) экзистенциализм

D) гуманизм

ANSWER: A

Выберите правильный вариант ответа:С точки зрения экзистенциальной психологии при наличии у человека отсутствия интереса к жизни, наличия у него апатии, работу желательно вести в направлении … .

A) приобретения навыков проявления агрессии

B) развития самооценки

C) развития коммуникативной компетентности

D) освобождения способности желать и облегчения проявления воли

ANSWER: D

Выберите правильный вариант ответа:Кто является автором теста структуры интеллекта (TSI)?

A) Л.В. Щеба

B) Р. Амтхауэр

C) И.А. Бодуэн де Куртенэ

D) А. Мейе

ANSWER: B

Выберите правильный вариант ответа:Если при самонаблюдении Вы отметили бы у себя те или иррациональные убеждения, выделенные А. Эллисом, к какой из указанных моделей работы Вы бы обратились для их проработки ... .

A) A-B-C (активирующее событие–иррациональное убеждение–эмоциональные или поведенческие паттерны)

B) биопсихосоциальной

C) модели последовательной или рационализирующей личности

D) структурной модели личности

ANSWER: A

Продолжите определение:Проективный метод – это … .

A) группа психодиагностических методик, задания которых представлены в виде вопросов или утверждений, а задачей испытуемого является самостоятельное сообщение о себе в форме ответов

B) целенаправленное, особым образом организованное и регистрируемое восприятие наблюдаемого явления

C) количественно-качественный анализ документальных и материальных источников, позволяющий изучать продукты человеческой деятельности

D) психодиагностический метод, предназначенный для диагностики личности, для которых характерен в большей мере глобальный подход к оценкеличности, а также использование в нем неопределенных стимулов, которые испытуемый должен сам дополнять, интерпретировать, развивать и т.д.

ANSWER: D

Выберите правильный вариант ответа:Кто является основателем «индивидуальной психологии»?

A) З. Фрейд

B) К. Юнг

C) А. Адлер

D) М. Вудкок

ANSWER: C

Выберите правильный вариант ответа:Желание человека стать тем, кем он может стать, связывается А. Маслоу с активацией какой потребности?

A) самоуважения

B) принадлежности и любви

C) самоактуализации

D) познания

ANSWER: C

Выберите правильный вариант ответа:В психологии под личностью понимается … .

A) человек, характеризуемый со стороны своих социально значимых отличий от других людей

B) отдельный представитель человеческой общности

C) существо, воплощающее высшую ступень развития личности

D) определяемое включенностью в общественные отношения системное качество индивида, формирующееся в совместной деятельности и общении

ANSWER: D

Выберите правильный вариант ответа:В рамках какого направления психологии появление дисфункциональных эмоций объясняется не влиянием «активирующих событий», а связывается с наличием иррациональных верований, формулируемых в форме абсолютистских требований или «долженствований»?

A) психодинамического

B) бихевиорального

C) рационально-эмоциональной психотерапии

D) клиент-центрированной психотерапии

ANSWER: C

Какой из перечисленных факторов является решающим в развитии личности?

A) наследственность (задатки)

B) среда

C) специально организованное воспитание и обучение

D) собственная активность личности (самовоспитание, самообразование)

ANSWER: D

Choose the correct alternative to complete the tip to be successful in a job interview.(Выберите правильный вариант совета, как добиться успеха на собеседовании при приеме на работу.)_Before the … find out as much as you can about the company.___

A) interview

B) lecture

C) lesson

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_I'm very reliable. I'm always on time to classes and meetings and when I can't make it, I let people … .ahead of time._

A) know

B) say

C) make

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_ I … speak several foreign languages.___

A) can

B) may

C) might

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_ _Salary is important for me … it is not the main point.____

A) but

B) so

C) as

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_ _I'm good at working and communicating within a … .to achieve shared goals.____

A) team

B) company

C) factory

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_ _I think working for your company would be …_ .___

A) fantastic

B) boring

C) challenging

ANSWER: A

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_Good morning, everyone! I'm Maria Ivanova, a second-year student of AMM faculty. Today I'm going to talk about.…_____

A) Introduction

B) The main part

C) Conclusion

ANSWER: A

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_Let's now move on to my next point.…_____

A) Introduction

B) The main part

C) Conclusion

ANSWER: B

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_Now I'd like to focus your attention on…_____

A) Introduction

B) The main part

C) Conclusion

ANSWER: B

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_Now I'll be happy to answer any questions you may have._____

A) Introduction

B) The main part

C) Conclusion

ANSWER: C

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_I've divided my presentation into three parts..._____

A) Introduction

B) The main part

C) Conclusion

ANSWER: A

Choose the correct alternative to complete the tip to be successful in a job interview.(Выберите правильный вариант совета, как добиться успеха на

собеседовании при приеме на работу.)___Think about … which the interviewer might ask you.___

A) questions

B) answers

C) sentences

ANSWER: A

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_Let me just start by introducing myself. My name is…_____

A) Introduction

B) The main part

C) Conclusion

ANSWER: A

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_Well, that brings me to the end of my presentation._____

A) Introduction

B) The main part

C) Conclusion

ANSWER: C

Match the sentences from a presentation with the correct category of the presentation plan.(Укажите категорию, к которой относится предложение из презентации.)_Let's now look at the next slide which shows…._____

A) Introduction

B) The main part

C) Conclusion

ANSWER: B

Choose the correct alternative to complete the tip to be successful in a job interview.(Выберите правильный вариант совета, как добиться успеха на собеседовании при приеме на работу.)_____Your answers should not be one word or one …. , but also should not be too long.___

A) sentence

B) message

C) question

ANSWER: A

Choose the correct alternative to complete the tip to be successful in a job interview.(Выберите правильный вариант совета, как добиться успеха на собеседовании при приеме на работу.)_____When answering questions, maintain … with the interviewer.___

A) eye contact

B) shaking hands

C) nodding

ANSWER: A

Choose the correct alternative to complete the tip to be successful in a job interview.(Выберите правильный вариант совета, как добиться успеха на собеседовании при приеме на работу.)_____Give clear, direct …. to questions. If you do not know something, say so.___

A) answers

B) suggestions

C) advice

ANSWER: A

Choose the correct alternative to complete the tip to be successful in a job interview.(Выберите правильный вариант совета, как добиться успеха на

собеседовании при приеме на работу.)_____Be …. and show enthusiasm for the job.___

A) positive

B) unhapppy

C) gloomy

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_____I think I … all necessary skills and experience to work for your company.___

A) have

B) had

C) had got

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_____I don't … working late or at weekends.___

A) mind

B) think

C) need

ANSWER: A

Choose the correct alternative to complete your answers in the job interview.(Выберите правильный вариант из предложенных для ответа на собеседовании при приеме на работу.)_I am also good … coming up with new ideas and suggesting alternative solutions._

A) at

B) in

C) on

ANSWER: A

Укажите, какой документ охарактеризован в определении:«ДОКУМЕНТ ИНФОРМАЦИОННОГО ТИПА, НАЦЕЛЕННЫЙ НА ОПИСАНИЕ СОЦИАЛЬНО ЗНАЧИМЫХ И НАИБОЛЕЕ ВАЖНЫХ СОБЫТИЙ ЖИЗНИ СОСТАВИТЕЛЯ ТЕКСТА. ПИШЕТСЯ ОТ ПЕРВОГО ЛИЦА В ХРОНОЛОГИЧЕСКОМ ПОРЯДКЕ»

A) резюме

B) сопроводительное письмо

C) автобиография

D) заявление

ANSWER: C

Укажите НЕВЕРНОЕ высказывание относительно правил ведения дискуссии.Оппоненты должны:

A) к концу дискуссии определить предмет спора

B) пользоваться одними и теми же понятиями

C) аргументировать свою позицию

D) проявлять уважительное отношение ко всем участникам спора

ANSWER: A

Укажите понятие, которое охарактеризовано в определении:ЧАСТЬ КОММУНИКАТИВНОГО ВЗАИМОДЕЙСТВИЯ, В КОТОРОЙ СЕРИЯ РАЗЛИЧНЫХ ВЕРБАЛЬНЫХ И НЕВЕРБАЛЬНЫХ СРЕДСТВ ИСПОЛЬЗУЕТСЯ ДЛЯ ДОСТИЖЕНИЯ ОПРЕДЕЛЕННОЙ КОММУНИКАТИВНОЙ ЦЕЛИ.

A) коммуникативный акт

B) коммуникативная тактика

C) коммуникативная стратегия

D) коммуникативное поведение

ANSWER: C

Выберите пример конструктивной критики.

A) Не огорчайтесь, сегодня Вы сделали не очень хорошо, завтра получится лучше.

B) Сколько раз можно было говорить – нельзя было так делать!

C) Какой дурак так делает!

D) Никогда вовремя не сделаете – всегда с задержкой.

ANSWER: A

Выберите правильный вариант ответа:КОНФЛИКТОГЕНЫ – ЭТО СЛОВА, ДЕЙСТВИЯ (БЕЗДЕЙСТВИЯ), КОТОРЫЕ … .

A) способствуют возникновению конфликта

B) препятствуют возникновению конфликта

C) помогают разрешить конфликт

ANSWER: A

Выберите правильный вариант ответа:Что из перечисленного НЕ относится к формам устной деловой коммуникации?

A) совещание

B) деловая беседа

C) лекция

D) переговоры

ANSWER: C

Выберите правильный вариант ответа:Как называется максима П. Грайса, которая гласит: "ГОВОРИ НЕ БОЛЬШЕ И НЕ МЕНЬШЕ ТОГО, ЧТО ТРЕБУЕТ СИТУАЦИЯ ОБЩЕНИЯ"?

A) максима ясности

B) максима качества

C) максима релевантности

D) максима количества

ANSWER: D

Выберите правильный вариант ответа:Как называется общение, которое направлено на извлечение выгоды с помощью таких приемов, как лесть, обман, запугивание и т.д.)?

A) речевое воздействие

B) манипулирование

C) убеждение

D) внушение

ANSWER: B

Выберите пример неконструктивной критики.

A) Сколько можно повторять – отчет надо сдавать в двух экземплярах!

B) В основном все правильно, но несколько ошибок придется устранить.

C) С вашим старанием в следующий раз вы добьетесь отличного результата.

ANSWER: A

Укажите, какие правила необходимо выполнять, ведя деловое общение по телефону.

A) быть лаконичным, информативным, доброжелательным

B) быть лаконичным, повторять сказанное несколько раз, разговаривать в присутствии третьих лиц

C) быть лаконичным, говорить громче обычного, прерывать разговор

ANSWER: A

Выберите правильный вариант ответа:Что из перечисленного не относится к распорядительным документам?

A) приказ

B) решение

C) представление
D) распоряжение
ANSWER: C
Выберите правильный вариант ответа:ПРИСПОСОБЛЕНИЕ – ЭТО … .
A) решение, удовлетворяющее интересы всех сторон
B) взаимные уступки
C) стремление выйти из конфликта, не решая его
D) сглаживание противоречий за счет своих интересов
E) все ответы неверны
ANSWER: D
Укажите, какой документ охарактеризован в определении:«ОФИЦИАЛЬНЫЙ ПИСЬМЕННЫЙ ДОКУМЕНТ, ОТРАЖАЮЩИЙ ХОД ОБЩЕСТВЕННОГО СОБРАНИЯ, СУДЕБНОГО СЛУШАНИЯ И ПРИНЯТЫЕ РЕШЕНИЯ»
A) аннотация
B) протокол
C) постановление
ANSWER: B
Выберите правильный вариант ответа:Для какого типа деловой культуры (по Д. Льюису) характерно:ПЛАНИРОВАНИЕ ПО СИТУАЦИИ,ОРИЕНТИРОВАННОСТЬ НА ЛЮДЕЙ,УМЕНИЕ СЛУШАТЬ,ИЗБЕГАНИЕ КОНФРОНТАЦИИ?
A) полиактивный
B) реактивный
C) моноактивный
ANSWER: B
Укажите правильную «формулу» критики.
A) похвала+критика+предложение
B) похвала+критика+ утешение
C) критика+помощь+похвала
ANSWER: A
Выберите правильный вариант ответа:СТРАТЕГИЯ ПОВЕДЕНИЯ, КОТОРАЯ ПОЗВОЛЯЕТ ВЫРАБОТАТЬ НАВЫКИ СЛУШАНИЯ, ПРИОБРЕСТИ ОПЫТ СОВМЕСТНОЙ РАБОТЫ, НАВЫКИ АРГУМЕНТАЦИИ, ВЫРАБОТАТЬ УМЕНИЕ СДЕРЖИВАТЬ СВОИ ЭМОЦИИ, – ЭТО… .
A) сотрудничество
B) избегание
C) приспособление
D) соперничество
ANSWER: A
УКАЖИТЕ ЛИШНЕЕ.Структура переговорной компетенции включает следующие составляющие:
A) организаторскую
B) языковую
C) коммуникативную
D) этическую
E) технологическую
F) информационную
ANSWER: B
Укажите явление, которое охарактеризовано в определении:ЭТО СОВОКУПНОСТЬ НАВЫКОВ И УМЕНИЙ ПО ПОДГОТОВКЕ И ПРОВЕДЕНИЮ РАЗЛИЧНЫХ ВИДОВ СОВРЕМЕННОГО ДЕЛОВОГО ОБЩЕНИЯ.
A) общение
B) технология общения

C) коммуникация
ANSWER: B
Выберите правильный вариант ответа:Что является главным условием эффективности делового общения?
A) обязательное достижение поставленной цели
B) создание основы для дальнейшего делового взаимодействия
C) демонстрация доминирования над собеседником
D) ослабление позиции собеседника
ANSWER: B
Выберите правильный вариант ответа:Что из перечисленного относится к организационным документам?
A) докладная записка
B) устав
C) служебная записка
D) представление
ANSWER: B
Выберите правильный вариант ответа:_При знакомстве … ._
A) женщина первая представляется мужчине
B) лица с более высоким статусом представляются людям со статусом более низким
C) младшие по возрасту представляются старшим
ANSWER: C
Выберите правильный вариант ответа:КУЛЬТУРА РЕЧИ ВКЛЮЧАЕТ В СЕБЯ … .
A) только нормативный аспект
B) нормативный, коммуникативный и этический аспекты
C) нормативный, коммуникативный и эстетический аспект
ANSWER: B
Укажите пример с неправильным употреблением падежной формы существительного с предлогом.
A) вопреки трудностям
B) благодаря поддержке руководства
C) согласно приказа ректора
D) по истечении срока
ANSWER: C
Укажите ошибку в согласовании прилагательных с географическими наименованиями.
A) древний Баку
B) незнакомое Тбилиси
C) широкая Миссисипи
D) огромный Мехико
ANSWER: B
Выберите правильный вариант ответа:ДЛЯ ТОГО ЧТОБЫ УЗНАТЬ, ЧЕМ РАЗЛИЧАЕТСЯ ЗНАЧЕНИЕ СЛОВ «ДИПЛОМАТ» И «ДИПЛОМАНТ», НУЖНО ОБРАТИТЬСЯ … .
A) к словарю иностранных слов
B) к словарю синонимов
C) к словарю паронимов
ANSWER: C
Выберите правильный вариант ответа:ПОНЯТИЕ «НОРМА» ПРИМЕНИМО … .
A) к языку в целом
B) к литературному языку
C) к языку художественной литературы

ANSWER: B

Выберите правильный вариант ответа:Что являлось основой политической системы Древней Греции?

A) полисы

B) номы

C) фемы

D) коммуны

ANSWER: A

Выберите правильный вариант ответа:Что из перечисленного было характерно для славянофилов в России XIX века?

A) идеализация истории допетровской Руси

B) идеализация капиталистического общества

C) стремление к возрождению старообрядчества

D) стремление к возрождению традиционных языческих культов

ANSWER: A

Выберите правильный вариант ответа:В какой стране к середине XIX века завершился промышленный переворот?

A) Англия

B) Германия

C) Россия

D) Франция

ANSWER: A

Выберите правильный вариант ответа:Какая из перечисленных реформ произошла в России в 1860-1870-х годах?

A) земская реформа

B) Столыпинская аграрная реформа

C) учреждение первых министерств

D) секуляризация церковных земель

ANSWER: A

Выберите правильный вариант ответа:Декрет о земле, принятый на II Всероссийском съезде Советов отменял … .

A) право частной собственности на землю

B) крепостное право

C) продразвёртку

D) крестьянскую общину

ANSWER: A

Выберите правильный вариант ответа:Кто в годы гражданской войны возглавлял в России Добровольческую армию?

A) Деникин А.И.

B) Брусилов А.А.

C) Каменев С.С.

D) Власов А.А.

ANSWER: A

Выберите правильный вариант ответа:Продовольственная диктатура, введенная в годы «военного коммунизма» предусматривала … .

A) принудительное изъятие излишков сельхозпродукции

B) создание колхозов

C) введение натурального сельскохозяйственного налога

D) ликвидацию помещичьих хозяйств

ANSWER: A

Выберите правильный вариант ответа:В каком году в Италии установился Фашистский режим?

A) 1922 г.

B) 1939 г.

C) 1914 г.
D) 1936 г.
ANSWER: A
Выберите правильный вариант ответа:В каком году была принята первая Конституция Советского Союза?
A) 1924 г.
B) 1922 г.
C) 1918 г.
D) 1936 г.
ANSWER: A
Выберите правильный вариант ответа:Какое положение из названных характеризует новую экономическую политику?
A) разрешение иностранных концессий
B) введение всеобщей трудовой повинности
C) отмена частной собственности на землю
D) установление продовольственной диктатуры
ANSWER: A
Выберите правильный вариант ответа:Что стало одной из причин свёртывания НЭПа?
A) несоответствие НЭПа идеологическим установкам большевиков
B) падение уровня жизни людей, по сравнению с периодом осуществления политики «военного коммунизма»
C) невозможность создания колхозов в условиях НЭПа
D) массовые крестьянские выступления с требованиями проведения сплошной коллективизации
ANSWER: A
Выберите правильный вариант ответа:К какому веку относится появление в славянских землях норманнов во главе с Рюриком?
A) IX век
B) XI век
C) X век
D) XII век
ANSWER: A
Выберите правильный вариант ответа:Крупнейшей стройкой первых пятилеток было … .
A) строительство Днепрогэса
B) строительство транссиба
C) освоение Донбасса
D) строительство Байконура
ANSWER: A
Выберите правильный вариант ответа:Благодаря советско-германскому договору от 1939 года в состав СССР вошла … .
A) Прибалтика
B) Украина
C) Болгария
D) Чехословакия
ANSWER: A
Выберите правильный вариант ответа:Главным вопросом Мюнхенской конференции 1938 года стал вопрос о … .
A) передаче Судетской области Германии
B) ненападении, между Чехословакией и Германией
C) объединении Австрии и Германии
D) заключении «Антикоминтерновского пакта»
ANSWER: A

Выберите правильный вариант ответа:В 1941 году немецкие войска были … .

A) разгромлены под Москвой

B) разгромлены под Смоленском

C) окружены в Сталинграде

D) разбиты в Ленинграде

ANSWER: A

Выберите правильный вариант ответа:В конце 40-х – начале 50-х преследовали «безродных космополитов» обвиняя людей в … .

A) преклонении перед Западом

B) коррупции

C) нелегальном пересечении границы

D) хищении государственного имущества

ANSWER: A

Выберите правильный вариант ответа:Что из нижеперечисленного связано с понятием «десталинизация»?

A) реабилитация политических заключённых

B) борьба с диссидентами

C) разрешение многопартийности

D) созыв съезда народных депутатов

ANSWER: A

Выберите правильный вариант ответа:Какое из приведенных событий произошло позже остальных?

A) ввод советских войск в Афганистан

B) Карибский кризис

C) ввод советских войск в Венгрию

D) создание НАТО

ANSWER: A

Выберите правильный вариант ответа:Кого в Советском Союза называли диссидентами?

A) борцов с существующим строем

B) злостных прогульщиков

C) агентов иностранной разведки

D) борцов с «космополитизмом»

ANSWER: A

Выберите правильный вариант ответа:Согласно решению XIX конференции КПСС высшим органом государственной власти в СССР становился … .

A) Съезд народных депутатов СССР

B) Совет Министров СССР

C) Государственная Дума СССР

D) Федеральное собрание

ANSWER: A

Укажите, что из перечисленного относится к реформам правительства Ельцина — Гайдара начала 1990-х гг.:

A) ваучерная приватизация

B) начало деятельности Съезда народных депутатов

C) реализация национальных проектов в социальной сфере и экономике

D) образование Государственного совета Российской Федерации

ANSWER: A

Выберите правильный вариант ответа:Ключевым принципом функционирования средневекового общества в Западной Европе был принцип … .

A) вассалитета

B) верховенства права
C) веротерпимости
D) демократического централизма
ANSWER: A

Выберите правильный вариант ответа:В соответствии с Конституцией Российской Федерации 1993 года высшим законодательным органом государственной власти стал двухпалатный парламент, получивший название … .

A) Федеральное собрание
B) Верховный Совет
C) Национальная ассамблея
D) Народное собрание
ANSWER: A

Выберите правильный вариант ответа:Когда впервые состоялся созыв Земского собора в России?

A) XVI век
B) XII век
C) XV век
D) XVII век
ANSWER: A

Выберите правильный вариант ответа:В европейской экономике XVI-XVII веков произошла … .

A) «революция цен»
B) промышленная революция
C) натурализация хозяйства
D) индустриализация
ANSWER: A

Выберите правильный вариант ответа:Какой из перечисленных городов был в XVII веке центром российской морской торговли со странами Западной Европы?

A) Архангельск
B) Рига
C) Кронштадт
D) Мурманск
ANSWER: A

Выберите правильный вариант ответа:Противником России, в ходе Северной войны была … .

A) Швеция
B) Польша
C) Пруссия
D) Дания
ANSWER: A

Выберите правильный вариант ответа:«Верховный тайный совет» играл определяющую роль в политической жизни России при … .

A) Петре II
B) Павле I
C) Екатерине II
D) Петре III
ANSWER: A

Выберите правильный вариант ответа:В число «просветителей», в европейской истории XVIII века, входил … .

A) Ж.-Ж. Руссо
B) Н. Макиавелли
C) Б. Спиноза

D) Ф. Аквинский
ANSWER: A
Выберите правильный вариант ответа:Физическая культура в вузе является…
A) средством активного отдыха
B) обязательной учебной дисциплиной
C) средством отвлечения от дурных привычек и безделья
D) уделом избранных
ANSWER: B
Выберите правильный вариант ответа:От какого ФАКТОРА больше всего зависит продолжительность жизни человека?
A) пол
B) наследственность
C) образ жизни
D) загрязненность окружающей среды
ANSWER: C
Выберите правильный вариант ответа:Специальными средствами воспитания быстроты являются … .
A) непрерывный длительный бег
B) спринтерский бег, стартовые ускорения, скоростные спурты
C) прыжки, многоскоки, скачки
D) упражнения с гантелями, гирей, штангой
ANSWER: B
Выберите правильный вариант ответа:Какая группа нижеперечисленных упражнений развивает общую выносливость?
A) спринт, прыжки, метания
B) акробатические, гимнастические, прыжки на батуте, в воду
C) плавание, лыжные гонки, бег на средние и длинные дистанции
D) спортивные игры, бокс, фехтование
ANSWER: C
Выберите правильный вариант ответа:За какое время выполняется испытание (тест) по выбору «Поднимание туловища из положения лёжа на спине»?
A) 30 секунд
B) 1 минута
C) 2 минуты
D) без учета времени
ANSWER: B
Выберите правильный вариант ответа:В комплекс ГТО входят … испытания.
A) обязательные и необязательные
B) обязательные и по выбору
C) обязательные и дополнительные
D) только обязательные
ANSWER: B
Выберите правильный вариант ответа:Что относится к скоростным способностям?
A) время реакции, быстроту одиночного движения, частоту движений
B) способность противостоять утомлению
C) способность преодолевать мышечное сопротивление
D) подвижность в суставах и позвоночнике
ANSWER: A
Выберите правильный вариант ответа:Какова масса гири при выполнении норматива «рывок гири» при сдаче ВФСК ГТО VI ступени?

A) 16 кг
B) 10 кг
C) 18 кг
D) 20 кг
ANSWER: A

Выберите правильный вариант ответа:Кто может проходить тестирование ГТО?
A) школьники
B) студенты
C) женщины и мужчины, достигшие совершеннолетия
D) все вышеперечисленные
ANSWER: D

Выберите правильный вариант ответа:На каких принципах основывается Всероссийский физкультурно-спортивный комплекс ГТО?
A) добровольности и обязательности медицинского контроля
B) экономичности проведения соревнований
C) равноправия женщин и мужчин
D) сознательности и активности
ANSWER: A

Выберите правильный вариант ответа:Какая возрастная группа охватывает шестую ступень?
A) 6-8 лет
B) 9-12 лет
C) 15-17 лет
D) 18-29 лет
ANSWER: D

Выберите правильный вариант ответа:Каким принципом создается необходимая предпосылка освоения движения?
A) системности
B) наглядности
C) сознательности и активности
D) доступности
ANSWER: B

Выберите правильный вариант ответа:Кого не допустят до сдачи нормативов ВФСК ГТО?
A) пенсионеров
B) дошкольников
C) лиц, не имеющих медицинского допуска
D) лиц, не имеющих спортивного разряда
ANSWER: C

Выберите правильный вариант ответа:Какой вид спорта в большей степени формирует координацию?
A) спортивная гимнастика
B) стрелковый спорт
C) тяжелая атлетика
D) шахматы
ANSWER: A

Выберите правильный вариант ответа:Кто имеет право принимать нормативы ВФСК ГТО?
A) преподаватель физической культуры
B) тренер или администрация спортивной школы
C) лица, прошедшие специальное обучение
D) все вышеперечисленные
ANSWER: C

Выберите правильный вариант ответа:Может ли иностранный гражданин принять участие в сдаче нормативов ГТО?

A) нет

B) могут все без исключения

C) могут те иностранные граждане, которые предоставят временную прописку

D) могут только из определенных стран

ANSWER: C

Выберите правильный вариант ответа:Каким стилем необходимо сдавать норматив по плаванию в ВФСК ГТО?

A) кроль

B) брасс

C) произвольный

D) устанавливает судейская коллегия при сдаче норматива

ANSWER: C

Выберите правильный вариант ответа:При какой ошибке во время выполнения норматива "метание снаряда на дальность" попытка будет засчитана?

A) метание произведено до линии разметки за 2-3 метра

B) снаряд не попал в сектор

C) попытка выполнена без команды спортивного судьи

D) просрочено время, выделенное на попытку

ANSWER: A

Выберите правильный вариант ответа:В течение какого времени достаточна фиксация при выполнении норматива «Наклон вперёд из положения стоя на гимнастической скамейке»?

A) фиксация не нужна

B) 1 секунда

C) 2 секунды

D) 3 секунды

ANSWER: C

Выберите правильный вариант ответа:Какие вещества выполняют функцию основного строительного материала для клеток человеческого организма?

A) белки

B) жиры

C) углеводы

D) витамины

ANSWER: A

Выберите правильный вариант ответа:Какие вещества являются наиболее подходящим источником для БЫСТРОГО получения энергии клетками человеческого организма?

A) белки

B) жиры

C) углеводы

D) витамины

ANSWER: C

Выберите правильный вариант ответа:По какой формуле можно рассчитать индивидуальную максимальную физическую нагрузку?

A) 180 - возраст

B) 200 - возраст

C) 220 - возраст

D) 300 - возраст

ANSWER: C

Выберите правильный вариант ответа:Какая из частей физической культуры является самой объемной?

A) двигательная реабилитация

B) физическое воспитание

C) спорт

D) физическая рекреация

ANSWER: B

Выберите правильный вариант ответа:Упражнение «Подъем туловища из положения лежа на спине» (количество раз за 1 минуту) выполняется следующим образом:

A) Руки сомкнуты в замок за головой, ноги согнуты в коленях. Осуществляется подъем туловища без подпрыгивания таза во время выполнения упражнения

B) Руки сомкнуты на груди, ноги выпрямлены. Подъем туловища осуществляется рывком

C) Руки в замке за головой на затылке, ноги согнуты в коленях под углом 90 градусов, локти во время подъема туловища касаются бедра и разводятся в стороны при опускании туловища в нижнее положение

D) Руки сомкнуты на груди, ноги выпрямлены. Подъем туловища осуществляется, пока угол между ногами и туловищем не будет равняться 90 градусам

ANSWER: C

Выберите правильный вариант ответа:Интенсивность физической нагрузки можно задать …

A) скоростью движения

B) длиной дистанции

C) количеством повторений

D) временем выполнения упражнений

ANSWER: D

Выберите правильный вариант ответа:Какая функция не входит в общекультурные социальные функции физической культуры?

A) коммуникативная

B) воспитательная

C) прагматическая

D) образовательная

ANSWER: C

Выберите правильный вариант ответа:Воспитание физической культуры личности – это ...

A) привитие чувства превосходства над другими людьми

B) воспитание неадекватной мотивации к занятиям физической культурой и спортом

C) воздействие на физические способности человека, на его чувства, сознание, психику и интеллект

D) воздействие на интеллект

ANSWER: C

Выберите правильный вариант ответа:Какой принцип предусматривает планомерное увеличение объема и интенсивности физической нагрузки по мере роста функциональных возможностей организма?

A) принцип научности

B) принцип доступности и индивидуализации

C) принцип непрерывности, систематичности

D) принцип наглядности

ANSWER: C

Выберите правильный вариант ответа:Какие документы необходимо иметь для прохождения тестирования комплекса ГТО?

A) заявку на соревнования

B) медицинский полис

C) СНИЛС

D) медицинскую справку и документ, удостоверяющий личность

ANSWER: D

Выберите правильный вариант ответа:Каковы действия судей, если участник переходит на шаг при выполнении нормативов «бег на 2000 м» и «бег на 3000 м» в ВФСК ГТО?

A) участник снимается с дистанции

B) судьи делают устное замечание

C) судейский корпус не применяет санкций

D) предлагают пересдать данную дисциплину на следующий день

ANSWER: A

Выберите правильный вариант ответа:Степень владения техникой действия, при которой управление движениями происходит автоматически и отличается надежностью исполнения, называется … .

A) техническим мастерством

B) двигательной одаренностью

C) двигательным умением

D) двигательным навыком

ANSWER: D

Выберите правильный вариант ответа:Какая цель НЕ ставится перед утренней гигиенической зарядкой?

A) усилить ток крови в кровяном русле

B) способствовать лучшему обмену веществ

C) ускорить приведение организма в рабочее состояние

D) способствовать развитию абсолютной силы путем применения упражнений статического характера

ANSWER: D

Выберите правильный вариант ответа:Спортивная тренировка приводит к ... .

A) увеличению полостей сердца и сердечной мышцы

B) изменению положения сердца

C) смещению сердца влево

D) уменьшению сердца

ANSWER: A

Выберите правильный вариант ответа:Что такое здоровье?

A) отсутствие заболеваний

B) состояние физического, психического, социального и душевного благополучия

C) хорошее самочувствие

D) состояние нормальной работоспособности

ANSWER: B

Выберите правильный вариант ответа:Какие упражнения необходимо включать в физкультурные занятия после учебного дня, если занятия проводились в малоподвижной позе?

A) упражнения статического характера

B) упражнения, дающие активную нагрузку на все группы мышц, способствующие активизации сердечно-сосудистой и дыхательной систем

C) упражнения на скоростную выносливость

D) упражнения с тяжестями предельной величины

ANSWER: B

Выберите правильный вариант ответа:Главная задача, решаемая на занятиях по физической культуре?

A) стать чемпионом

B) получить материальное вознаграждение

C) укрепить здоровье и общее физическое развитие

D) побить рекорд

ANSWER: C

Выберите правильный вариант ответа:Какая из приведенных целей больше всего присуща спорту высших достижений?

A) продление творческого долголетия

B) снятие нервно-эмоционального напряжения

C) социальная и физическая адаптация в обществе

D) достижение высоких спортивных результатов на крупнейших соревнованиях

ANSWER: D

Выберите правильный вариант ответа:Физическая нагрузка увеличивает … .

A) продолжительность сна

B) прочность суставов

C) количество суставов

D) длину суставов

ANSWER: A

Выберите правильный вариант ответа:Целью ГТО является … .

A) укрепление здоровья, гармоничное и всестороннее развитие личности, воспитание патриотизма

B) выполнение спортивных и массовых разрядов

C) получение максимального количества знаков отличия ГТО населением

D) обучение разным видам спорта и видам физической активности

ANSWER: A

Выберите правильный вариант ответа:Какие виды спортивных упражнений не входят в тесты ГТО?

A) бег

B) сгибание и разгибание рук в упоре на брусьях

C) бег на лыжах

D) плавание

ANSWER: B

Пострадавший внезапно потерял сознание. Дыхание присутствует. Выберите необходимое действие:

A) - следует уложить пострадавшего в устойчивое боковое положение (позу восстановления, стабильное боковое положение)

B) - для профилактики возможного вдыхания рвотных масс необходимо уложить пострадавшего на живот

C) - для профилактики возможного вдыхания рвотных масс следует повернуть голову пострадавшего набок

D) - для скорейшего восстановления сознания необходимо надавить пострадавшему на болевые точки (угол нижней челюсти, верхняя губа и т.д.)

E) - следует дать понюхать нашатырный спирт на ватке

F) - необходимо придать положение на спине с приподнятыми ногами для обеспечения лучшего кровоснабжения головного мозга пострадавшего

ANSWER: A

Выберите правильный вариант ответа:Если в ране находится инородный предмет, более правильным будет … .

A) - срочно извлечь из раны инородный предмет, остановить кровотечение доступными способами, вызвать скорую медицинскую помощь

B) - срочно извлечь из раны инородный предмет, остановить кровотечение доступными способами, вызвать скорую медицинскую помощь

C) - не предпринимать никаких действий до прибытия медицинских работников

D) - закрыть рану стерильной салфеткой, вызвать скорую медицинскую помощь, инородный предмет не извлекать

E) - аккуратно удалить инородный предмет, кровотечение из раны остановить путем заполнения ее стерильными салфетками, вызвать скорую медицинскую помощь, положить холод на место ранения

ANSWER: D

Укажите основную цель обзорного (быстрого) осмотра пострадавшего:

A) - оценить его общее состояние

B) - обнаружить явные признаки наружного кровотечения (прежде всего, артериального)

C) - попытаться обнаружить ранения различных областей тела

D) - определить, нуждается ли пострадавший в оказании первой помощи

ANSWER: B

Выберите последовательность подробного осмотра пострадавшего, находящегося в сознании:

A) - голова, шея, грудная клетка, живот, ноги и руки

B) - грудная клетка, голова и шея, ноги и руки, живот

C) - голова, грудная клетка, живот, шея, руки и ноги

D) - ноги и руки, голова и шея, грудная клетка и живот

ANSWER: A

Выберите правильный вариант ответа:Выведение в загородную зону рабочих и служащих, членов их семей, студентов вузов и ссузов организуется через предприятия, учреждения и учебные заведения при ... принципе эвакуации.

A) - территориальном

B) - территориально-производственном

C) - производственном

D) - бытовом

E) - территориально-локальном

ANSWER: B

Выберите правильный вариант ответа:Полную специальную обработку проводят … .

A) - после выхода из зоны загрязнения (заражения)

B) - до выхода из зоны загрязнения (заражения)

C) - до входа в зону загрязнения (заражения)

ANSWER: A

Выберите правильный вариант ответа:Для наложения окклюзионной (герметизирующей) повязки при открытом пневмотораксе можно использовать … .

A) - Индивидуальный противохимический пакет

B) - Пакет перевязочный медицинский

C) - Аптечку индивидуальную АИ-2

D) - Аптечку индивидуальную АИ-4

ANSWER: B

Выберите правильный вариант ответа:Трансмиссивные инфекции передаются от человека к человеку с помощью/через … .

A) - кровососущих членистоногих

B) - воду, пищу

C) - капельки мокроты и слизи в воздухе
D) - контакт кожных покровов или слизистых оболочек
E) - дышать через ткань или ватно-марлевую повязку, смоченную раствором пищевой соды
ANSWER: A
Выберите правильный вариант ответа:Массовое заболевание животных называется … .
A) - пандемия
B) - эпидемия
C) - эпифитотия
D) - эпизоотия
ANSWER: D
Выберите правильный вариант ответа:Для возникновения эпидемического процесса необходим (-о, -ы) … .
A) - любые бактерии, вирусы, грибы
B) - большое скопление людей
C) - патогенный микроорганизм
D) - холодное время года
ANSWER: C
Выберите правильный вариант ответа:РСЧС – это … .
A) - Единая государственная система предупреждения и ликвидации чрезвычайных ситуаций
B) - Российская система чрезвычайных ситуаций
C) - Российская служба чрезвычайных ситуаций
ANSWER: A
Выберите правильный вариант ответа:При полном отсутствии или недостатке кислорода в воздухе применяются ... СИЗОД.
A) - фильтрующие
B) - изолирующие
C) - табельные
D) - простейшие
ANSWER: B
Выберите правильный вариант ответа:В случае применения каких защитных сооружений нужно пользоваться средствами индивидуальной защиты, т.к. они не обеспечивают защиты от аварийно химически опасных веществ и бактериальных средств?
A) - простейших укрытий
B) - убежищ
C) - противорадиационных укрытий
D) - бомбоубежищ
ANSWER: A
Укажите, в каких случаях осуществляется экстренное извлечение пострадавшего из аварийного автомобиля:
A) во всех случаях, когда пострадавшему требуется немедленное оказание первой помощи
B) экстренное извлечение пострадавшего производится только силами сотрудников скорой медицинской помощи или спасателями МЧС
C) наличие угрозы для жизни и здоровья пострадавшего и невозможность оказания первой помощи в автомобиле
D) в случае, если у пострадавшего отсутствуют признаки серьезных травм
ANSWER: C
Выберите основные способы остановки кровотечения при ранении головы:

A) прямое давление на рану, наложение давящей повязки

B) наложение давящей повязки, пальцевое прижатие сонной артерии

C) пальцевое прижатие сонной артерии, наложение давящей повязки с использованием жгута

D) применение холода в области ранения, пальцевое прижатие сонной артерии

ANSWER: A

Выберите основные признаки закупорки инородным телом верхних дыхательных путей тяжелой степени у пострадавшего:

A) не может дышать или дыхание явно затруднено (шумное, хриплое), хватается за горло, не может говорить, только кивает

B) хватается за горло, кашляет, просит о помощи

C) надрывно кашляет, пытается что-то сказать, лицо багровеет

D) жалуется на наличие инородного тела в дыхательных путях, говорит, что «поперхнулся», просит постучать по спине

ANSWER: A

Выберите правильный вариант ответа:При проникающем ранении груди самое важное – это … .

A) - попытаться остановить кровотечение давящей повязкой

B) - не прикасаться к ране во избежание причинения вреда

C) - наложить на рану груди повязку, не пропускающую воздух (окклюзионную)

D) - своевременно обезболить пострадавшего

E) - постоянно контролировать дыхание и кровообращение пострадавшего

F) - придать пострадавшему устойчивое боковое положение

ANSWER: C

Выберите правильный вариант ответа:Что собой представляет страхование?

A) страхование выражает совокупность экономических отношений, возникающих между продавцом и покупателем страховой услуги

B) страхование – это взаимодействие между страховщиком и страхователем

C) страхование – это процесс передачи страхового полиса физическому или юридическому лицу

D) страхование представляет собой организационную форму предоставления страховой услуги

ANSWER: A

Выберите правильный вариант ответа:Что характеризует эффективность фирмы?

A) соотношение результатов хозяйственной деятельности и связанных с их достижением затрат

B) массу прибыли

C) суммарную стоимость материальных затрат к себестоимости продукции

D) выручку, приходящуюся на единицу проданных изделий

ANSWER: A

Выберите правильный вариант ответа:Предельная склонность к потреблению – это … .

A) соотношение между приростом потребления и приростом дохода

B) соотношение между приростом потребления и приростом сбережений

C) соотношение между приростом сбережения на единицу прироста дохода

D) соотношение между приростом дохода и приростом потребления

ANSWER: A

Выберите правильный вариант ответа:Диверсификация как метод управления инвестиционными рисками – это … .

A) включение в портфель ценных бумаг с различными параметрами риска и ожидаемой доходности

B) снижение доходов вследствие наличия противоречий в законодательной базе

C) реализация всех ценных бумаг с низким уровнем доходности

D) вложение всех средств в ценные бумаги одного предприятия

ANSWER: A

Укажите собственные средства предприятия для осуществления инвестиций:

A) прибыль

B) банковский кредит

C) средства муниципального бюджета

D) средства от продажи корпоративных облигаций

ANSWER: A

Выберите правильный вариант ответа:Какой из названных факторов экономического роста является интенсивным?

A) совершенствование технологий

B) рост количества рабочей силы на предприятии

C) покупка дополнительного оборудования, аналогичных уже имеющимся

D) увеличение объема инвестиций при сохранении существующего уровня технологии

ANSWER: A

Выберите правильный вариант ответа:Экономический рост, сопровождаемый повышением качества выпускаемой продукции, ростом производительности труда и ресурсосбережения, называется … .

A) интенсивным

B) экстенсивным

C) интегрированным

D) нейтральным

ANSWER: A

Выберите правильный вариант ответа:Какое из перечисленных явлений не соответствует периоду экономического спада?

A) уменьшение объема пособий по безработице

B) снижение инвестиций в оборудование с длительным сроком служб

C) сокращение налоговых поступлений

D) снижение прибылей предприятий

ANSWER: A

Выберите правильный вариант ответа:Подавленная (скрытая) инфляция проявляется … .

A) в дефиците товаров и услуг в стране

B) во все меньшем разрыве между ценой на товары, устанавливаемой государством, и рыночной ценой на эти же товары, складывающейся под влиянием спроса и предложения

C) в появлении у производителей стимулов к увеличению количества производимой продукции

D) в возникновении у производителей стимулов к повышению качества производимой продукции

ANSWER: A

Выберите правильный вариант ответа:Открытая инфляция характеризуется … .

A) постоянным повышением цен
B) ростом дефицита товаров
C) увеличением денежной массы
D) снижением качества выпускаемой продукции
ANSWER: A

Выберите правильный вариант ответа:Кривая Филлипса характеризует связь между … .
A) уровнем безработицы и уровнем инфляции
B) налоговыми ставками и объемом налоговых поступлений
C) нормой процента и денежной массой в обращении
D) уровнем безработицы и объемом ВНП
ANSWER: A

Выберите правильный вариант ответа:Страхование гражданской ответственности относится к … .
A) имущественному страхованию
B) личному страхованию
C) страхованию убытков
D) личному страхованию и страхованию убытков
ANSWER: A

Выберите правильный вариант ответа:Полная занятость связана с … .
A) естественным уровнем безработицы
B) полным отсутствием безработных
C) гиперинфляцией
D) циклической безработицей
ANSWER: A

Выберите правильный вариант ответа:Спрос на факторы производства является производным, так как … .
A) определяется спросом на готовую продукцию
B) без факторов производства невозможно производство товаров
C) от количества приобретаемых факторов производства зависит объем производства
D) все факторы производства между собой взаимосвязаны
ANSWER: A

Выберите правильный вариант ответа:Субъектами предложения на рынке труда являются … .
A) домашние хозяйства
B) государство
C) фирмы
D) некоммерческие организации
ANSWER: A

Выберите правильный вариант ответа:Как, согласно экономической теории, рост заработной платы влияет на предложение труда работника?
A) количество часов работы может как вырасти, так и сократиться, это зависит от предпочтений индивида
B) количество часов работы однозначно растет
C) количество часов работы однозначно сокращается
D) количество часов работы не изменится
ANSWER: A

Какое из нижеперечисленных положений относительно трудового договора и договора гражданско-правового характера (ГПХ), заключающиеся при трудоустройстве на работу, является верным?
A) Предмет договора ГПХ – конечный результат работы или оказания услуги, который работодатель принимает в срок, установленный договором, процесс выполнения работы заказчика, как правило, не интересует

B) Ни при трудовом договоре, ни при ГПХ не положен ежегодный оплачиваемый отпуск и учебный отпуск

C) Период работы по договору ГПХ не включается в страховой стаж, дающий право на страховую пенсию по старости, так как работодатель не обязан перечислять страховые взносы с вознаграждения по договору ГПХ

D) Работа по трудовому договору и по договору ГПХ регулируется трудовым кодексом РФ

ANSWER: A

Какое из нижеперечисленных положений о минимальном размере оплате труда (МРОТ) является верным?

A) МРОТ не может быть ниже величины прожиточного минимума трудоспособного населения

B) МРОТ служит только для определения размеров пособий по временной нетрудоспособности

C) Регионы устанавливают свой МРОТ, который может быть ниже федерального

D) Согласно методике расчета, МРОТ составляет 62% от средней заработной платы

ANSWER: A

Иванов И.И. планировал отправиться в путешествие в Бразилию. Целый год он откладывал определённую часть зарплаты для последующего приобретения туристической путёвки. Какую функцию денег иллюстрирует данный пример?

A) средство накопления

B) мера стоимости

C) мировые деньги

D) средство обращения

ANSWER: A

Выберите правильный вариант ответа:К функциям ЦБ не относится … .

A) выдача кредитов населению

B) эмиссия денежных знаков

C) регулирование денежного обращения в соответствии с потребностями экономики

D) хранение золотовалютных резервов страны

ANSWER: A

Выберите правильный вариант ответа:Денежно-кредитная политика проводится … .

A) Центральным банком страны

B) правительством страны

C) всеми финансово-кредитными учреждениями страны

D) министерством финансов

ANSWER: A

Выберите правильный вариант ответа:К инструментам денежно-кредитной политики не относится … .

A) изменение налоговых ставок

B) регулирование учетной ставки

C) регулирование нормы обязательных резервов

D) операции на открытом рынке

ANSWER: A

Выберите правильный вариант ответа:Пенсия – это … .

A) регулярная денежная выплата, которую человек начинает получать при признании его нетрудоспособным, при утрате близкого человека, доход которого является единственным средством существования, а также за выслугу лет и особые заслуги перед государством

B) регулярная денежная выплата, которая является средством существования

C) страхование работающих от утраты трудоспособности

D) регулярная денежная выплата, которую человек начинает получать при признании его нетрудоспособным

ANSWER: A

Выберите правильный вариант ответа:В чем состоит разница между кредитом и займом?

A) Кредиты выдают банки, а МФО и ломбарды выдают займы

B) Деньги, полученные по договору займа, возвращать не обязательно

C) Заём может выдавать только один гражданин другому гражданину

D) Заём выдается только на сумму не более 100 тыс. рублей

ANSWER: A

Выберите правильный вариант ответа:Кредитная карта в общем случае позволяет своему владельцу … .

A) получить доступ к дополнительному источнику заемных средств

B) контролировать свои расходы и воздержаться от спонтанных, ненужных покупок

C) снимать наличные средства в банкомате без дополнительных комиссий

D) обеспечить более надежную защиту от несанкционированного доступа к своим средствам, чем дебетовая карта

ANSWER: A

Выберите однозначно правильный вариант ответа:Чем безналичные расчеты могут быть удобнее наличных?

A) Быстрота совершения операций, даже с контрагентами, находящимися вне оперативной доступности

B) Анонимность и конфиденциальность

C) Отсутствие комиссий

D) Невозможность потерять

ANSWER: A

Укажите правильное утверждение касательно криптовалюты:

A) Криптовалюта – это цифровые деньги, существующие только в виртуальном пространстве интернет

B) Криптовалюту можно приобрести в обменном пункте, как любую другую валюту

C) Существует только одна криптовалюта – биткойн, остальные являются подделкой

D) Существует орган, который контролирует цифровые монеты криптовалют, влияет на их курс и объем в сети, а также может заблокировать транзакции, счета и так далее

ANSWER: A

Выберите правильный вариант ответа:Что такое Агентство по страхованию вкладов?

A) организация, которая обеспечивает осуществление страховых выплат при отзыве лицензии у банка или его банкротстве

B) организация, осуществляющая надзор за деятельностью страховых компаний

C) банк, через который страховые компании выплачивают страховые возмещения своим клиентам

D) государственный орган, в задачи которого входит обеспечение устойчивости национальной валюты и платежной системы

ANSWER: A

Продолжите утверждение:Чем выше ставка рефинансирования, тем … .

A) больше процентов по депозиту получит вкладчик
B) дешевле будет взять кредит на автомобиль
C) больше бизнесмены будут инвестировать
D) дешевле для коммерческого банка будет кредит в ЦБ
ANSWER: A
Укажите неверное утверждение:
A) Годовая процентная ставка по займам в МФО существенно ниже, чем по банковским кредитам
B) Кредит лучше брать в той валюте, в которой вы получаете зарплату
C) Проценты по кредитам обычно выше, чем проценты по вкладам
D) Для некоторых кредитных карт предусмотрен беспроцентный период
ANSWER: A
Выберите правильный вариант ответа:Какой вид страхования является обязательным для заемщика при взятии ипотечного кредита?
A) страхование недвижимого имущества, являющегося предметом залога
B) добровольное медицинское страхование
C) страхование жизни и/или здоровья заемщика
D) накопительное страхование жизни
ANSWER: A
Выберите правильный вариант ответа:К доходам государственного бюджета не относятся … .
A) зарплата государственных служащих
B) доходы от приватизации
C) акцизы
D) доходы от продажи государственных ценных бумаг
ANSWER: A
Выберите правильный вариант ответа:Какой налог из перечисленных относится к косвенным налогам?
A) налог на добавленную стоимость
B) налог на прибыль
C) таможенная пошлина
D) транспортный налог
ANSWER: A
Выберите правильный вариант ответа:Какие бывают пенсионные системы по характеру участия?
A) обязательные и добровольные
B) распределительные и накопительные
C) распределительные и добровольные
D) обязательные и накопительные
ANSWER: A
Выберите правильный вариант ответа:Фискальная функция налогов проявляется в том, что они … .
A) обеспечивают доходами казну (бюджет) государства
B) сдерживают экономический рост
C) позволяют контролировать доходы населения
D) нет верного ответа
ANSWER: A
Выберите правильный вариант ответа:В каком случае из перечисленных ниже вы не должны самостоятельно составить и подать налоговую декларацию о полученных доходах и уплатить с них НДФЛ?
A) зарплата, полученная от работодателя в рамках трудового контракта
B) выигрыш в лотерею в размере 10000 руб.
C) арендная плата, полученная от сдачи квартиры

D) дивиденды, полученные по ценным бумагам, которые по договору доверительного управления приобрел для вас банк

ANSWER: A

Выберите правильный вариант ответа:Какие виды дохода не подлежат налогообложению?

A) стипендии

B) доходы от продажи квартиры, которая находилась в собственности 2 года

C) заработная плата в случае, если ее размер не превышает 20000 руб.

D) доходы, полученные лицами-нерезидентами РФ

ANSWER: A

Выберите правильный вариант ответа:Какая организация осуществляет регулирование страхового рынка в России?

A) Банк России

B) Министерство экономического развития

C) Министерство финансов

D) Торгово-промышленная палата

ANSWER: A

Выберите правильный вариант ответа:Какой результат отражает прибыль от реализации продукции предприятия?

A) финансовый результат, полученный от основной деятельности предприятия

B) денежное выражение всей стоимости товаров

C) материальный результат производства продукции

D) социально-экономический результат

ANSWER: A

Выберите правильный вариант ответа:Механизм денежного возмещения износа основного капитала называется … .

A) амортизацией основного капитала

B) кругооборотом капитала

C) авансированием капитала

D) оборотом капитала

ANSWER: A

Выберите правильный вариант ответа:Период, в течение которого фирма может изменить количество всех используемых ею производственных ресурсов, называется … .

A) долгосрочным

B) краткосрочным

C) мгновенным

D) среднесрочным

ANSWER: A

Выберите правильный вариант ответа:Чистая прибыль не используется для формирования какого из фондов?

A) фонд заработной платы

B) фонд накопления

C) фонд инвестирования

D) резервный фонд

ANSWER: A

Выберите правильный вариант ответа:Что не является коррупцией?

A) отказ в выполнении неправомерного поручения

B) злоупотребление служебным положением

C) дача взятки

ANSWER: A

Выберите правильный вариант ответа:Решение комиссии по соблюдению требований к служебному поведению принимается … .

A) тайным голосованием

B) открытым голосованием

C) возможны оба варианта

ANSWER: A

Выберите правильный вариант ответа:Государственный служащий обязан уведомить представителя нанимателя … .

A) обо всех случаях совершенных коррупционных действий

B) только о склонении к коррупционным действиям лично государственного служащего

C) только о факте коррупционных действий в отношении государственного служащего

ANSWER: A

Выберите правильный вариант ответа:К взысканиям, которые предусмотрены за совершение коррупционных действий, независимо от их тяжести относятся … .

A) дисциплинарные взыскания в виде замечания, выговора, предупреждения о неполном должностном соответствии, либо увольнения

B) отмена выплаты премии

C) дисциплинарные взыскания в виде замечания, выговора, строгого выговора

ANSWER: A

Выберите правильный вариант ответа:Государственный служащий обязан предоставлять сведения о доходах каких членов семьи?

A) супруги (супруга) и несовершеннолетних детей

B) всех близких родственников, включая родителей, а также сестер и братьев

C) супруги (супруга) и родителей

ANSWER: A

Выберите правильный вариант ответа:Утрата доверия государственного лица за совершенные коррупционные действия возможна … .

A) при установленном факте получении взятки

B) при опоздании на работу

C) при отказе в выполнении неправомерного поручения

ANSWER: A

Выберите пример коррупционных действий:

A) использование служебного положения для получения выгоды в отношении родственников

B) получение любого подарка

C) отказ в выполнении неправомерного поручения

ANSWER: A

Выберите правильный вариант ответа:Кто является субъектом коррупционной деятельности?

A) физические и юридические лица

B) только государственные служащие

C) органы публичной власти

ANSWER: A

Выберите правильный вариант ответа:Какова основная цель Национальной стратегии противодействия коррупции?

A) искоренение причин и условий, порождающих коррупцию в российском обществе

B) формирование у субъекта определённого отношения к коррупционным проявлениям

C) формирование у субъекта негативного отношения к коррупционным проявлениям

ANSWER: A

Выберите правильный вариант ответа:Кто может быть привлечен к уголовной ответственности за совершение коррупционных преступлений?

A) лицо, которое получает взятку; лицо, которое дает взятку; лицо, которое передает взятку взяткополучателю

B) только лицо, получающее взятку

C) лицо, дающее взятку

ANSWER: A

Выберите правильный вариант ответа:Что запрещается гражданскому служащему в связи с прохождением гражданской службы?

A) заниматься предпринимательской деятельностью лично или через доверенных лиц

B) нет запретов

C) заниматься творческой деятельностью

ANSWER: A

Выберите правильный вариант ответа:Профилактика коррупции – это … .

A) деятельность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, институтов гражданского общества, организаций и физических лиц в пределах их полномочий по предупреждению коррупции, в том числе по выявлению и последующему устранению причин коррупции

B) деятельность институтов гражданского общества, организаций и физических лиц по выявлению и последующему устранению причин коррупции

C) деятельность институтов гражданского общества по выявлению и последующему устранению причин коррупции

ANSWER: A

Выберите правильный вариант ответа:Какая сумма признается крупным размером взятки (а также стоимость ценных бумаг, иного имущества или выгод имущественного характера)?

A) от 150 тысяч рублей до 1 миллиона рублей

B) от 25 до 150 тысяч рублей

C) от 1 миллиона до 5 миллионов рублей

ANSWER: A

Выберите правильный вариант ответа:Задачей федеральных государственных органов в области информационных технологий для профилактики коррупции является … .

A) обеспечение наличия полноты сведений, содержащихся на сайтах государственных органов, по вопросам профилактики и противодействия коррупции и иным правонарушениям

B) внедрение современных информационных технологий

C) обеспечение государственной защиты государственных служащих

ANSWER: A

Выберите правильный вариант ответа:Органом, ответственным за реализацию в России положений Конвенции против коррупции 2003 г. по всем вопросам взаимной правовой помощи (за исключением гражданско-правовых вопросов), является … .

A) Генеральная прокуратура Российской Федерации

B) Следственный комитет Российской Федерации

C) ФСБ Российской Федерации

ANSWER: A

Выберите правильный вариант ответа:В случае, если государственный служащий владеет ценными бумагами, акциями (долями участия, паями в уставных (складочных) капиталах организаций), обязан ли он в целях предотвращения конфликта интересов передать принадлежащие ему ценные бумаги, акции (доли участия, паи в уставных (складочных) капиталах организаций) в доверительное управление?

A) да, обязан

B) нет, не обязан

C) обязан в случаях, установленных законом

ANSWER: A

Выберите действие, являющееся коррупционным нарушением:

A) получение должностным лицом в качестве подарка скидки, ссуды, бесплатной услуги от физических лиц и организаций, в отношении которых осуществлял государственные функции

B) получение премии за добросовестное выполнение служебных обязанностей

C) получение любого подарка

ANSWER: A

Выберите правильный вариант ответа:Является ли должностной (служебной) обязанностью государственного служащего уведомление о фактах обращения к нему в целях склонения к совершению коррупционных правонарушений?

A) да, является его обязанностью

B) нет, не является обязанностью, а только рекомендовано антикоррупционным законодательством

C) нет, не является

ANSWER: A

Выберите правильный вариант ответа:Что относится к конфликту интересов (в соответствии с Федеральным законом от 25.12.2008 № 273-ФЗ «О противодействии коррупции»)?

A) ситуация, при которой личная заинтересованность (прямая или косвенная) лица, замещающего должность, замещение которой предусматривает обязанность принимать меры по предотвращению и урегулированию конфликта интересов, влияет или может повлиять на надлежащее, объективное и беспристрастное исполнение им должностных (служебных) обязанностей

B) наличие завышенных требований к лицу, предъявляемых для реализации принадлежащего ему права

C) противоречия, в том числе внутренние, между нормами, создающие для государственных органов, органов местного самоуправления или организаций (их должностных лиц) возможность произвольного выбора норм, подлежащих применению в конкретном случае

ANSWER: A

Выберите правильный вариант ответа:В течение какого периода после увольнения с государственной службы граждане, замещавшие должности государственной гражданской службы, перечень которых устанавливается нормативными правовыми актами Российской Федерации, обязаны при заключении трудовых договоров сообщать работодателю сведения о последнем месте службы?

A) в течение двух лет

B) в течение 12 месяцев

C) в течение пяти лет

ANSWER: A

Выберите правильный вариант ответа:Кто обязан предоставлять сведения о своих доходах, об имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера своих супруги (супруга) и несовершеннолетних детей?

A) граждане, претендующие на замещение должностей государственной гражданской службы

B) граждане, претендующие на замещение должностей гражданской службы, включенных в перечни, установленные нормативными правовыми актами Российской Федерации

C) граждане, иностранные граждане, претендующие на замещение должностей гражданской службы

ANSWER: A

Выберите правильный вариант ответа:Личная заинтересованность гражданского служащего, которая влияет или может повлиять на надлежащее исполнение им должностных (служебных) обязанностей – это … .

A) конфликт интересов

B) коррупция

C) коррупциогенный фактор

ANSWER: A

Выберите правильный вариант ответа:Предотвращение или урегулирование конфликта интересов на гражданской службе может состоять … .

A) в отказе гражданского служащего от выгоды, явившейся причиной возникновения конфликта интересов

B) в понижении гражданского служащего в должности

C) в прекращении государственной гражданской службы

ANSWER: A

Выберите правильный вариант ответа:Непринятие гражданским служащим, являющимся стороной конфликта интересов, мер по предотвращению или урегулированию конфликта интересов является … .

A) правонарушением, влекущим увольнение гражданского служащего с гражданской службы

B) несоблюдением требований к служебному поведению, влекущим наложение дисциплинарного взыскания

C) преступлением

ANSWER: A

Выберите правильный вариант ответа:В какой форме обязан уведомить гражданский служащий о возникшем конфликте интересов или о возможности его возникновения?

A) в письменной

B) в устной

C) допускаются обе формы уведомления

ANSWER: A

Выберите правильный вариант ответа:Вправе ли гражданский служащий выполнять иную оплачиваемую работу?

A) вправе, если это не повлечет за собой конфликта интересов

B) не вправе

C) вправе

ANSWER: A

Выберите правильный вариант ответа:Вправе ли государственный служащий публично высказываться, в том числе в СМИ и давать оценки либо высказывать свои суждения?

A) да, если это входит в его должностные обязанности

B) нет

C) да
ANSWER: A
Управление – это:
A) A) процесс планирования, организации, мотивации и контроля для достижения целей организации;
B) Б) процесс достижения высокой прибыли организации;
C) В) процесс принятия решений;
D) Г) процесс построения структуры организации
ANSWER: A
Важнейшей задачей менеджмента является:
A) A) организация производства товаров и услуг с учетом интересов потребителей на основе имеющихся ресурсов и обеспечение рентабельности предприятия и его стабильного положения на рынке;
B) Б)получение прибыли
C) В)реализация достигнутых целей;
D) Г) реализация товаров и услуг
ANSWER: A
Целью классической школы управления было
A) A) создание мотивации рабочих
B) Б)создание универсальных принципов управления
C) В)разработка стратегии поведения;
D) Г) разработка системы оплаты труда рабочих
ANSWER: B
Создателем школы человеческих отношений в управлении является
A) A) М. Вебер
B) Б) Э. Мэйо
C) В) Ф. Тейлор;
D) Г) А. Файоль
ANSWER: B
14 универсальных принципов управления разработал
A) A) У. Оучи
B) Б) А. Файоль
C) В) Э. Мэйо
D) Г) Д. МакГрегор
ANSWER: B
Характерной особенностью структуры организации является
A) A) разделение труда
B) Б) контроль
C) В) уровни подчинения
D) Г) принятие решений
ANSWER: A
К основным компонентам внешней среды относится
A) A) потребители и технологии
B) Б) политические факторы и цели
C) В) конкуренты и поставщики
D) Г) социокультурные факторы и структура организации
ANSWER: C
Система, имеющая жесткие фиксированные границы, действия которой относительно независимы от окружающей среды, называется
A) A) закрытой
B) Б) открытой
C) В) гибкой
D) Г) жесткой
ANSWER: A

Выбор альтернативы это
A) А) коммуникации
B) Б) решения
C) В) планирование
D) Г) организация
ANSWER: B

На какой стадии процесса управленческого решения осуществляется разработка и оценка альтернативных решений, отбор критериев выбора оптимального решения
A) А) на стадии подготовки
B) Б) на стадии реализации решений
C) В) на стадии принятия решений
D) Г) ни на одной из этих стадий
ANSWER: A

Цель организации – это
A) А) работа людей для достижения прибыли
B) Б) конкретные конечные состояния, или желаемый результат, которого стремиться добиться группа, работая вместе
C) В) взаимодействие людей для достижения целей руководства
D) Г) решение конкретных задач производства
ANSWER: B

К основным характеристикам организации не относится:
A) А) ресурсы;
B) Б) зависимость от внешней среды;
C) В) адаптивность
D) Г) разделение труда
ANSWER: B

Структура организации – это
A) А) количество уровней управления
B) Б) количество уровней подразделений
C) В) взаимоотношение уровней управления и подразделений, построенные в такой форме, которая позволяет наиболее эффективно достигать целей организации
D) Г) взаимоотношение руководителей и подчиненных, построенные в виде жесткой иерархической структуры управления
ANSWER: C

Сфера контроля – это
A) А) число лиц, подчиненных одному руководителю
B) Б) число лиц, подчиненных организации в целом
C) В) число лиц, контроль над которыми осуществляет руководитель
D) Г) число лиц, имеющих право контролировать подчиненных
ANSWER: C

Проблема информационных перегрузок характерна для процесса
A) А) планирования
B) Б) мотивации
C) В) организации
D) Г) коммуникации
ANSWER: D

Какие бывают уровни организационных решений
A) А) индивидуальные и организационные
B) Б) общественные и личные
C) В) массовые и частные
D) Г) возможные и невозможные
ANSWER: A

Процесс побуждения себя и других к деятельности для достижения целей организации – это

A) А) процесс планирования
B) Б) процесс мотивации
C) В) процесс принятия решений
D) Г) процесс коммуникации
ANSWER: B

К содержательным теориям мотивации относятся
A) А) теории Маслоу и Герцберга
B) Б) теория ожиданий Врума
C) В) теория справедливости
D) Г) модель Портера-Лоулера
ANSWER: A

Общая цель предприятия, выражающая причину его существования, – это

A) А) миссия
B) Б) призвание
C) В) план
D) Г) стратегия
ANSWER: A

Неверным является утверждение, что миссия
A) А) влияет на имидж фирмы
B) Б) является основой для выработки целей фирмы
C) В) определяется стратегией фирмы
D) Г) оказывает влияние на формирование организационной культуры фирмы
ANSWER: C

Тактические планы разрабатываются на уровне руководителей
A) А) среднего звена
B) Б) высшего звена
C) В) низового и среднего звена
D) Г) высшего и среднего звена
ANSWER: A

Тактика разрабатывается на уровне
A) А) руководства низшего звена
B) Б) руководства высшего звена
C) В) руководства среднего звена
D) Г) ни на одном из этих уровней
ANSWER: C

Функцией менеджмента не является:
A) А) планирование;
B) Б) организация;
C) В) мотивация;
D) Г) управление
ANSWER: D

Различают три основных вида контроля
A) А) стратегический, тактический и единовременный
B) Б) прогнозируемый, планируемый и программируемый
C) В) долгосрочный, среднесрочный, краткосрочный
D) Г) предварительный, текущий и заключительный
ANSWER: D

Важнейшим средством предварительного контроля финансовых ресурсов является

A) А) анализ прибыли

B) Б) бюджет
C) В) установление стандартов
D) Г) учет издержек
ANSWER: D

Выработка стандартов и критериев, сопоставление с ними реальных результатов и принятие необходимых корректирующих мер – этапы
A) А) планирования
B) Б) управления
C) В) контроля
D) Г) программирования
ANSWER: D

Система контроля на фирме должна включать
A) А) стратегический, оперативно-тактический контроль
B) Б) аудиторский и стратегический контроль
C) В) ревизионный и аудиторский контроль
D) Г) ревизионный и оперативно-тактический контроль
ANSWER: A

Характеристиками эффективного контроля являются
A) А) оперативная направленность и частота
B) Б) периодичность и определенность
C) В) частота и скорость проведения
D) Г) стратегическая направленность и гибкость
ANSWER: D

Конечная цель контроля состоит в том, чтобы
A) А) решить задачи, стоящие перед организацией
B) Б) установить стандарты
C) В) выявить проблемы в организации
D) Г) провести измерения и оповестить об их результатах
ANSWER: A

Функции по проведению оперативного тактического контроля возлагаются на менеджеров
A) А) среднего и высшего звеньев управления
B) Б) среднего и низового звеньев управления
C) В) только низового управления
D) Г) только среднего звена управления
ANSWER: B

Процесс передачи полномочий нижестоящим руководителям на выполнение специальных заданий – это
A) А) сужение полномочий
B) Б) распределение полномочий
C) В) делегирование полномочий
D) Г) снятие полномочий
ANSWER: C

Как называется один из основных факторов эффективности, который определяется как отношение количества продукции компании и количества затрат на ее выпуск
A) А) экономичность
B) Б) действенность
C) В) прибыльность
D) Г) производительность
ANSWER: D

Как называется один из основных факторов эффективности, который отражает степень достижения поставленных перед организацией целей
A) А) экономичность

B) Б) действенность
C) В) прибыльность
D) Г) производительность
E) Д) качество
ANSWER: B
4. Связующей функцией менеджмента является функция:
A) А) коммуникации;
B) Б) планирование;
C) В) контроль;
D) Г) мотивация
ANSWER: A
Информация об исполнении команд и состоянии объекта управления, поступающая от объекта к субъекту управления, в менеджменте называется
A) А) интегральная связь
B) Б) прямая связь
C) В) обратная связь
D) Г) коммуникационная сеть
E) Д) качество
ANSWER: C
Выбор, обусловленный знаниями или накопленным опытом, – это:
A) А) решение, основанное на суждении
B) Б) интуитивное решение
C) В) рациональное решение
D) Г) профессиональное решение
ANSWER: A
Решения, являющиеся результатом реализации определенной последовательности действий, имеющие конкретный механизм реализации
A) А) осторожные решения
B) Б) рациональные решения
C) В) запрограммированные решения
D) Г) незапрограммированные решения
ANSWER: C
Какие функции присущи для субъектов управленческих решений?
A) А) определение эффективности управленческого решения
B) Б) защита организации от внешнего воздействия
C) В) психологическое влияние на персонал с целью достижения собственных выгод
ANSWER: C
Групповое принятие решений имеет ряд преимуществ по сравнению с индивидуальным. Выберите их:
A) А) более полное информационное обеспечение процесса принятия решений
B) Б) более высокая обоснованность и меньший процент ошибок
C) В) более высокий уровень творчества
D) Г) как правило, требуют меньше времени
E) Д) все перечисленные
ANSWER: E
По степени и уровню информационной обеспеченности выделяют следующие управленческие решения:
A) А)глобальные и локальные
B) Б) перспективные и текущие
C) В) запрограммированные и незапрограммированные
D) Г) единоличные, консультативные и совместные
E) Д) детерминированные, вероятностные и неопределенные

F) E) директивные и рекомендательные
ANSWER: E

Благодаря выполнению какого требования, предъявляемых к управленческим решениям, должно быть возможным изменять цель и (или) алгоритм достижения цели при изменении внешних и внутренних условий:
A) A) обоснованность
B) Б) своевременность
C) B) четкость формулировок
D) Г) эффективность
E) Д) реальная осуществимость
F) E) гибкость
ANSWER: F

На каком этапе разработки и принятия управленческих решений наиболее эффективными методами являются «мозговая атака» («мозговой штурм») и метод «Дельфи»:
A) A) формулировка задачи
B) Б) разработка вариантов решения (поиск решения)
C) B) оценка вариантов решения и выбор оптимального
D) Г) принятие решения
E) Д) реализация и контроль
F) E) оценка принятого решения
ANSWER: C

Проведите соответствиеУправленческое решение это
A) A) Предмет труда
B) Б) Результат труда
C) B) Средства труда
ANSWER: B

Проведите соответствиеТехнические средства обработки информации это
A) A) Предмет труда
B) Б) Результат труда
C) B) Средства труда
ANSWER: C

Основателем школы научного управления является:
A) A) А. Смит;
B) Б) Ф. Тейлор;
C) B) А. Файоль;
D) Г) Д. МакГрегор
ANSWER: D

Опыт, навыкиТехнические средства обработки информации это
A) A) Предмет труда
B) Б) Результат труда
C) B) Средства труда
ANSWER: A

Проведите соответствиеИнтеллектуальные способности это
A) A) Предмет труда
B) Б) Результат труда
C) B) Средства труда
ANSWER: A

Проведите соответствиеИнформация о проблемах это
A) A) Предмет труда
B) Б) Результат труда
C) B) Средства труда
ANSWER: A

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМОриентирован на создание структуры, выработку правил, внутренних стандартов и правил функционирования системы

A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: A

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМФормирует цели и пути их достижения. Оперирует системами в целом – предприятиями, организациями, государственными структурами

A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: B

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМНапоминает стратегический, но работает на уровне отдельных подразделений или подсистем. Тактическим менеджментом занимаются управленцы среднего звена

A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: C

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМИспользуется для решения текущих задач, стоящих перед системой. Основная функция – грамотное распределение ресурсов и контроль над выполнением поставленных задач

A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: D

Определите, к какой школе управления относятся приведенные ниже тезисы1. Применение приемов управления межличностными отношениями для повышения степени удовлетворенности и производительности.2. Применение наук о человеческом поведении к управлению и формированию организации таким образом, чтобы каждый работник мог быть полностью использован в соответствии с его потенциалом.

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: A

Определите, к какой школе управления относятся приведенные ниже тезисы1. Использование научного анализа для определения лучших способов выполнения задачи.2. Отбор работников, лучше всего подходящих для выполнения задач, и обеспечение их обучения.3. Обеспечение работников ресурсами, требуемыми для эффективного выполнения задач.4. Систематическое и правильное использование материального стимулирования для повышения производительности.5. Отделение планирования и обдумывания от самой работы.

A) Школа человеческих отношений

B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: B

Определите, к какой школе управления относятся приведенные ниже тезисы1. Углубление понимания сложных управленческих проблем благодаря разработке и применению моделей.2. Развитие и использование количественных методов руководителями, которым они помогают в принятии сложных решений

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: C

В соответствии с принципами школы научного управления:

A) А) оплата труда рабочих должна соответствовать полученному результату;
B) Б) оплата труда рабочих не зависит от полученных результатов;
C) В) оплата труда зависит от количества рабочего времени;
D) Г) оплата труда рабочих должна соответствовать выслуге лет
ANSWER: A

Определите, к какой школе управления относятся приведенные ниже тезисы1. Развитие принципов управления.2. Описание функций управления.3. Систематизированный подход к управлению всей организации

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: D

М. Вебер разработал:

A) А) систему бюрократического построения организации;
B) Б) принципы менеджмента;
C) В) иерархическую систему управления;
D) Г) теорию потребностей
ANSWER: A

Процессный подход рассматривает управление как:

A) А) непрерывную серию взаимосвязанных управленческих функций;
B) Б) совокупность элементов организации;
C) В) систему отдельных подсистем организации;
D) Г) пригодность методов управления определяется ситуацией
ANSWER: A

Под менеджментом понимается:

A) А) управление условиями обеспечения ресурсами;
B) Б) управление государством
C) В) управление организацией, действующей в рыночных условиях;
D) Г) управление людьми
ANSWER: C

Управление – это:

A) А) процесс планирования, организации, мотивации и контроля для достижения целей организации;
B) Б) процесс достижения высокой прибыли организации;
C) В) процесс принятия решений;
D) Г) процесс построения структуры организации
ANSWER: A

Важнейшей задачей менеджмента является:

A) А) организация производства товаров и услуг с учетом интересов потребителей на основе имеющихся ресурсов и обеспечение рентабельности предприятия и его стабильного положения на рынке;

B) Б)получение прибыли

C) В)реализация достигнутых целей;

D) Г) реализация товаров и услуг

ANSWER: A

Целью классической школы управления было

A) А) создание мотивации рабочих

B) Б)создание универсальных принципов управления

C) В)разработка стратегии поведения;

D) Г) разработка системы оплаты труда рабочих

ANSWER: B

Создателем школы человеческих отношений в управлении является

A) А) М. Вебер

B) Б) Э. Мэйо

C) В) Ф. Тейлор;

D) Г) А. Файоль

ANSWER: B

14 универсальных принципов управления разработал

A) А) У. Оучи

B) Б) А. Файоль

C) В) Э. Мэйо

D) Г) Д. МакГрегор

ANSWER: B

Характерной особенностью структуры организации является

A) А) разделение труда

B) Б) контроль

C) В) уровни подчинения

D) Г) принятие решений

ANSWER: A

К основным компонентам внешней среды относится

A) А) потребители и технологии

B) Б) политические факторы и цели

C) В) конкуренты и поставщики

D) Г) социокультурные факторы и структура организации

ANSWER: C

Система, имеющая жесткие фиксированные границы, действия которой относительно независимы от окружающей среды, называется

A) А) закрытой

B) Б) открытой

C) В) гибкой

D) Г) жесткой

ANSWER: A

Выбор альтернативы это

A) А) коммуникации

B) Б) решения

C) В) планирование

D) Г) организация

ANSWER: B

На какой стадии процесса управленческого решения осуществляется разработка и оценка альтернативных решений, отбор критериев выбора оптимального решения

A) А) на стадии подготовки
B) Б) на стадии реализации решений
C) В) на стадии принятия решений
D) Г) ни на одной из этих стадий
ANSWER: A

Цель организации – это
A) А) работа людей для достижения прибыли
B) Б) конкретные конечные состояния, или желаемый результат, которого стремиться добиться группа, работая вместе
C) В) взаимодействие людей для достижения целей руководства
D) Г) решение конкретных задач производства
ANSWER: B

К основным характеристикам организации не относится:
A) А) ресурсы;
B) Б) зависимость от внешней среды;
C) В) адаптивность
D) Г) разделение труда
ANSWER: B

Структура организации – это
A) А) количество уровней управления
B) Б) количество уровней подразделений
C) В) взаимоотношение уровней управления и подразделений, построенные в такой форме, которая позволяет наиболее эффективно достигать целей организации
D) Г) взаимоотношение руководителей и подчиненных, построенные в виде жесткой иерархической структуры управления
ANSWER: C

Сфера контроля – это
A) А) число лиц, подчиненных одному руководителю
B) Б) число лиц, подчиненных организации в целом
C) В) число лиц, контроль над которыми осуществляет руководитель
D) Г) число лиц, имеющих право контролировать подчиненных
ANSWER: C

Проблема информационных перегрузок характерна для процесса
A) А) планирования
B) Б) мотивации
C) В) организации
D) Г) коммуникации
ANSWER: D

Какие бывают уровни организационных решений
A) А) индивидуальные и организационные
B) Б) общественные и личные
C) В) массовые и частные
D) Г) возможные и невозможные
ANSWER: A

Процесс побуждения себя и других к деятельности для достижения целей организации – это
A) А) процесс планирования
B) Б) процесс мотивации
C) В) процесс принятия решений
D) Г) процесс коммуникации
ANSWER: B

К содержательным теориям мотивации относятся
A) А) теории Маслоу и Герцберга

B) Б) теория ожиданий Врума
C) В) теория справедливости
D) Г) модель Портера-Лоулера
ANSWER: A

Общая цель предприятия, выражающая причину его существования, – это
A) А) миссия
B) Б) призвание
C) В) план
D) Г) стратегия
ANSWER: A

Неверным является утверждение, что миссия
A) А) влияет на имидж фирмы
B) Б) является основой для выработки целей фирмы
C) В) определяется стратегией фирмы
D) Г) оказывает влияние на формирование организационной культуры фирмы
ANSWER: C

Тактические планы разрабатываются на уровне руководителей
A) А) среднего звена
B) Б) высшего звена
C) В) низового и среднего звена
D) Г) высшего и среднего звена
ANSWER: A

Тактика разрабатывается на уровне
A) А) руководства низшего звена
B) Б) руководства высшего звена
C) В) руководства среднего звена
D) Г) ни на одном из этих уровней
ANSWER: C

Функцией менеджмента не является:
A) А) планирование;
B) Б) организация;
C) В) мотивация;
D) Г) управление
ANSWER: D

Различают три основных вида контроля
A) А) стратегический, тактический и единовременный
B) Б) прогнозируемый, планируемый и программируемый
C) В) долгосрочный, среднесрочный, краткосрочный
D) Г) предварительный, текущий и заключительный
ANSWER: D

Важнейшим средством предварительного контроля финансовых ресурсов является
A) А) анализ прибыли
B) Б) бюджет
C) В) установление стандартов
D) Г) учет издержек
ANSWER: D

Выработка стандартов и критериев, сопоставление с ними реальных результатов и принятие необходимых корректирующих мер – этапы
A) А) планирования
B) Б) управления
C) В) контроля

D) Г) программирования
ANSWER: D
Система контроля на фирме должна включать
A) А) стратегический, оперативно-тактический контроль
B) Б) аудиторский и стратегический контроль
C) В) ревизионный и аудиторский контроль
D) Г) ревизионный и оперативно-тактический контроль
ANSWER: A
Характеристиками эффективного контроля являются
A) А) оперативная направленность и частота
B) Б) периодичность и определенность
C) В) частота и скорость проведения
D) Г) стратегическая направленность и гибкость
ANSWER: D
Конечная цель контроля состоит в том, чтобы
A) А) решить задачи, стоящие перед организацией
B) Б) установить стандарты
C) В) выявить проблемы в организации
D) Г) провести измерения и оповестить об их результатах
ANSWER: A
Функции по проведению оперативного тактического контроля возлагаются на менеджеров
A) А) среднего и высшего звеньев управления
B) Б) среднего и низового звеньев управления
C) В) только низового управления
D) Г) только среднего звена управления
ANSWER: B
Процесс передачи полномочий нижестоящим руководителям на выполнение специальных заданий – это
A) А) сужение полномочий
B) Б) распределение полномочий
C) В) делегирование полномочий
D) Г) снятие полномочий
ANSWER: C
Как называется один из основных факторов эффективности, который определяется как отношение количества продукции компании и количества затрат на ее выпуск
A) А) экономичность
B) Б) действенность
C) В) прибыльность
D) Г) производительность
ANSWER: D
Как называется один из основных факторов эффективности, который отражает степень достижения поставленных перед организацией целей
A) А) экономичность
B) Б) действенность
C) В) прибыльность
D) Г) производительность
E) Д) качество
ANSWER: B
4. Связующей функцией менеджмента является функция:
A) А) коммуникации;
B) Б) планирование;
C) В) контроль;

D) Г) мотивация
ANSWER: A

Информация об исполнении команд и состоянии объекта управления, поступающая от объекта к субъекту управления, в менеджменте называется
A) А) интегральная связь
B) Б) прямая связь
C) В) обратная связь
D) Г) коммуникационная сеть
E) Д) качество
ANSWER: C

Выбор, обусловленный знаниями или накопленным опытом, – это:
A) А) решение, основанное на суждении
B) Б) интуитивное решение
C) В) рациональное решение
D) Г) профессиональное решение
ANSWER: A

Решения, являющиеся результатом реализации определенной последовательности действий, имеющие конкретный механизм реализации
A) А) осторожные решения
B) Б) рациональные решения
C) В) запрограммированные решения
D) Г) незапрограммированные решения
ANSWER: C

Какие функции присущи для субъектов управленческих решений?
A) А) определение эффективности управленческого решения
B) Б) защита организации от внешнего воздействия
C) В) психологическое влияние на персонал с целью достижения собственных выгод
ANSWER: C

Групповое принятие решений имеет ряд преимуществ по сравнению с индивидуальным. Выберите их:
A) А) более полное информационное обеспечение процесса принятия решений
B) Б) более высокая обоснованность и меньший процент ошибок
C) В) более высокий уровень творчества
D) Г) как правило, требуют меньше времени
E) Д) все перечисленные
ANSWER: E

По степени и уровню информационной обеспеченности выделяют следующие управленческие решения:
A) А)глобальные и локальные
B) Б) перспективные и текущие
C) В) запрограммированные и незапрограммированные
D) Г) единоличные, консультативные и совместные
E) Д) детерминированные, вероятностные и неопределенные
F) Е) директивные и рекомендательные
ANSWER: E

Благодаря выполнению какого требования, предъявляемых к управленческим решениям, должно быть возможным изменять цель и (или) алгоритм достижения цели при изменении внешних и внутренних условий:
A) А) обоснованность
B) Б) своевременность
C) В) четкость формулировок
D) Г) эффективность

E) Д) реальная осуществимость
F) Е) гибкость
ANSWER: F

На каком этапе разработки и принятия управленческих решений наиболее эффективными методами являются «мозговая атака» («мозговой штурм») и метод «Дельфи»:
A) А) формулировка задачи
B) Б) разработка вариантов решения (поиск решения)
C) В) оценка вариантов решения и выбор оптимального
D) Г) принятие решения
E) Д) реализация и контроль
F) Е) оценка принятого решения
ANSWER: C

Проведите соответствиеУправленческое решение это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: B

Проведите соответствиеТехнические средства обработки информации это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: C

Основателем школы научного управления является:
A) А) А. Смит;
B) Б) Ф. Тейлор;
C) В) А. Файоль;
D) Г) Д. МакГрегор
ANSWER: D

Опыт, навыкиТехнические средства обработки информации это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: A

Проведите соответствиеИнтеллектуальные способности это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: A

Проведите соответствиеИнформация о проблемах это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: A

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМОриентирован на создание структуры, выработку правил, внутренних стандартов и правил функционирования системы
A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: A

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМФормирует цели и пути их достижения. Оперирует системами в целом – предприятиями, организациями, государственными структурами

A) Организационный

B) Стратегический

C) тактический

D) Оперативный

ANSWER: B

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМНапоминает стратегический, но работает на уровне отдельных подразделений или подсистем. Тактическим менеджментом занимаются управленцы среднего звена

A) Организационный

B) Стратегический

C) тактический

D) Оперативный

ANSWER: C

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМИспользуется для решения текущих задач, стоящих перед системой. Основная функция – грамотное распределение ресурсов и контроль над выполнением поставленных задач

A) Организационный

B) Стратегический

C) тактический

D) Оперативный

ANSWER: D

Определите, к какой школе управления относятся приведенные ниже тезисы1. Применение приемов управления межличностными отношениями для повышения степени удовлетворенности и производительности.2. Применение наук о человеческом поведении к управлению и формированию организации таким образом, чтобы каждый работник мог быть полностью использован в соответствии с его потенциалом.

A) Школа человеческих отношений

B) Школа научного управления

C) Школа количественных методов

D) Школа научного управления

ANSWER: A

Определите, к какой школе управления относятся приведенные ниже тезисы1. Использование научного анализа для определения лучших способов выполнения задачи.2. Отбор работников, лучше всего подходящих для выполнения задач, и обеспечение их обучения.3. Обеспечение работников ресурсами, требуемыми для эффективного выполнения задач.4. Систематическое и правильное использование материального стимулирования для повышения производительности.5. Отделение планирования и обдумывания от самой работы.

A) Школа человеческих отношений

B) Школа научного управления

C) Школа количественных методов

D) Школа научного управления

ANSWER: B

Определите, к какой школе управления относятся приведенные ниже тезисы1. Углубление понимания сложных управленческих проблем благодаря разработке и применению моделей.2. Развитие и использование

количественных методов руководителями, которым они помогают в принятии сложных решений

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: C

В соответствии с принципами школы научного управления:

A) А) оплата труда рабочих должна соответствовать полученному результату;
B) Б) оплата труда рабочих не зависит от полученных результатов;
C) В) оплата труда зависит от количества рабочего времени;
D) Г) оплата труда рабочих должна соответствовать выслуге лет
ANSWER: A

Определите, к какой школе управления относятся приведенные ниже тезисы1. Развитие принципов управления.2. Описание функций управления.3. Систематизированный подход к управлению всей организации

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: D

М. Вебер разработал:

A) А) систему бюрократического построения организации;
B) Б) принципы менеджмента;
C) В) иерархическую систему управления;
D) Г) теорию потребностей
ANSWER: A

Процессный подход рассматривает управление как:

A) А) непрерывную серию взаимосвязанных управленческих функций;
B) Б) совокупность элементов организации;
C) В) систему отдельных подсистем организации;
D) Г) пригодность методов управления определяется ситуацией
ANSWER: A

Под менеджментом понимается:

A) А) управление условиями обеспечения ресурсами;
B) Б) управление государством
C) В) управление организацией, действующей в рыночных условиях;
D) Г) управление людьми
ANSWER: C

Управление – это:

A) А) процесс планирования, организации, мотивации и контроля для достижения целей организации;
B) Б) процесс достижения высокой прибыли организации;
C) В) процесс принятия решений;
D) Г) процесс построения структуры организации
ANSWER: A

Важнейшей задачей менеджмента является:

A) А) организация производства товаров и услуг с учетом интересов потребителей на основе имеющихся ресурсов и обеспечение рентабельности предприятия и его стабильного положения на рынке;
B) Б)получение прибыли
C) В)реализация достигнутых целей;
D) Г) реализация товаров и услуг

ANSWER: A

Целью классической школы управления было

A) А) создание мотивации рабочих

B) Б)создание универсальных принципов управления

C) В)разработка стратегии поведения;

D) Г) разработка системы оплаты труда рабочих

ANSWER: B

Создателем школы человеческих отношений в управлении является

A) А) М. Вебер

B) Б) Э. Мэйо

C) В) Ф. Тейлор;

D) Г) А. Файоль

ANSWER: B

14 универсальных принципов управления разработал

A) А) У. Оучи

B) Б) А. Файоль

C) В) Э. Мэйо

D) Г) Д. МакГрегор

ANSWER: B

Характерной особенностью структуры организации является

A) А) разделение труда

B) Б) контроль

C) В) уровни подчинения

D) Г) принятие решений

ANSWER: A

К основным компонентам внешней среды относится

A) А) потребители и технологии

B) Б) политические факторы и цели

C) В) конкуренты и поставщики

D) Г) социокультурные факторы и структура организации

ANSWER: C

Система, имеющая жесткие фиксированные границы, действия которой относительно независимы от окружающей среды, называется

A) А) закрытой

B) Б) открытой

C) В) гибкой

D) Г) жесткой

ANSWER: A

Выбор альтернативы это

A) А) коммуникации

B) Б) решения

C) В) планирование

D) Г) организация

ANSWER: B

На какой стадии процесса управленческого решения осуществляется разработка и оценка альтернативных решений, отбор критериев выбора оптимального решения

A) А) на стадии подготовки

B) Б) на стадии реализации решений

C) В) на стадии принятия решений

D) Г) ни на одной из этих стадий

ANSWER: A

Цель организации – это

A) А) работа людей для достижения прибыли

B) Б) конкретные конечные состояния, или желаемый результат, которого стремиться добиться группа, работая вместе
C) В) взаимодействие людей для достижения целей руководства
D) Г) решение конкретных задач производства
ANSWER: B
К основным характеристикам организации не относится:
A) А) ресурсы;
B) Б) зависимость от внешней среды;
C) В) адаптивность
D) Г) разделение труда
ANSWER: B
Структура организации – это
A) А) количество уровней управления
B) Б) количество уровней подразделений
C) В) взаимоотношение уровней управления и подразделений, построенные в такой форме, которая позволяет наиболее эффективно достигать целей организации
D) Г) взаимоотношение руководителей и подчиненных, построенные в виде жесткой иерархической структуры управления
ANSWER: C
Сфера контроля – это
A) А) число лиц, подчиненных одному руководителю
B) Б) число лиц, подчиненных организации в целом
C) В) число лиц, контроль над которыми осуществляет руководитель
D) Г) число лиц, имеющих право контролировать подчиненных
ANSWER: C
Проблема информационных перегрузок характерна для процесса
A) А) планирования
B) Б) мотивации
C) В) организации
D) Г) коммуникации
ANSWER: D
Какие бывают уровни организационных решений
A) А) индивидуальные и организационные
B) Б) общественные и личные
C) В) массовые и частные
D) Г) возможные и невозможные
ANSWER: A
Процесс побуждения себя и других к деятельности для достижения целей организации – это
A) А) процесс планирования
B) Б) процесс мотивации
C) В) процесс принятия решений
D) Г) процесс коммуникации
ANSWER: B
К содержательным теориям мотивации относятся
A) А) теории Маслоу и Герцберга
B) Б) теория ожиданий Врума
C) В) теория справедливости
D) Г) модель Портера-Лоулера
ANSWER: A
Общая цель предприятия, выражающая причину его существования, – это
A) А) миссия

B) Б) призвание
C) В) план
D) Г) стратегия
ANSWER: A

Неверным является утверждение, что миссия
A) А) влияет на имидж фирмы
B) Б) является основой для выработки целей фирмы
C) В) определяется стратегией фирмы
D) Г) оказывает влияние на формирование организационной культуры фирмы
ANSWER: C

Тактические планы разрабатываются на уровне руководителей
A) А) среднего звена
B) Б) высшего звена
C) В) низового и среднего звена
D) Г) высшего и среднего звена
ANSWER: A

Тактика разрабатывается на уровне
A) А) руководства низшего звена
B) Б) руководства высшего звена
C) В) руководства среднего звена
D) Г) ни на одном из этих уровней
ANSWER: C

Функцией менеджмента не является:
A) А) планирование;
B) Б) организация;
C) В) мотивация;
D) Г) управление
ANSWER: D

Различают три основных вида контроля
A) А) стратегический, тактический и единовременный
B) Б) прогнозируемый, планируемый и программируемый
C) В) долгосрочный, среднесрочный, краткосрочный
D) Г) предварительный, текущий и заключительный
ANSWER: D

Важнейшим средством предварительного контроля финансовых ресурсов является
A) А) анализ прибыли
B) Б) бюджет
C) В) установление стандартов
D) Г) учет издержек
ANSWER: D

Выработка стандартов и критериев, сопоставление с ними реальных результатов и принятие необходимых корректирующих мер – этапы
A) А) планирования
B) Б) управления
C) В) контроля
D) Г) программирования
ANSWER: D

Система контроля на фирме должна включать
A) А) стратегический, оперативно-тактический контроль
B) Б) аудиторский и стратегический контроль
C) В) ревизионный и аудиторский контроль
D) Г) ревизионный и оперативно-тактический контроль

ANSWER: A

Характеристиками эффективного контроля являются

A) А) оперативная направленность и частота

B) Б) периодичность и определенность

C) В) частота и скорость проведения

D) Г) стратегическая направленность и гибкость

ANSWER: D

Конечная цель контроля состоит в том, чтобы

A) А) решить задачи, стоящие перед организацией

B) Б) установить стандарты

C) В) выявить проблемы в организации

D) Г) провести измерения и оповестить об их результатах

ANSWER: A

Функции по проведению оперативного тактического контроля возлагаются на менеджеров

A) А) среднего и высшего звеньев управления

B) Б) среднего и низового звеньев управления

C) В) только низового управления

D) Г) только среднего звена управления

ANSWER: B

Процесс передачи полномочий нижестоящим руководителям на выполнение специальных заданий – это

A) А) сужение полномочий

B) Б) распределение полномочий

C) В) делегирование полномочий

D) Г) снятие полномочий

ANSWER: C

Как называется один из основных факторов эффективности, который определяется как отношение количества продукции компании и количества затрат на ее выпуск

A) А) экономичность

B) Б) действенность

C) В) прибыльность

D) Г) производительность

ANSWER: D

Как называется один из основных факторов эффективности, который отражает степень достижения поставленных перед организацией целей

A) А) экономичность

B) Б) действенность

C) В) прибыльность

D) Г) производительность

E) Д) качество

ANSWER: B

4. Связующей функцией менеджмента является функция:

A) А) коммуникации;

B) Б) планирование;

C) В) контроль;

D) Г) мотивация

ANSWER: A

Информация об исполнении команд и состоянии объекта управления, поступающая от объекта к субъекту управления, в менеджменте называется

A) А) интегральная связь

B) Б) прямая связь

C) В) обратная связь

D) Г) коммуникационная сеть
E) Д) качество
ANSWER: C

Выбор, обусловленный знаниями или накопленным опытом, – это:
A) А) решение, основанное на суждении
B) Б) интуитивное решение
C) В) рациональное решение
D) Г) профессиональное решение
ANSWER: A

Решения, являющиеся результатом реализации определенной последовательности действий, имеющие конкретный механизм реализации
A) А) осторожные решения
B) Б) рациональные решения
C) В) запрограммированные решения
D) Г) незапрограммированные решения
ANSWER: C

Какие функции присущи для субъектов управленческих решений?
A) А) определение эффективности управленческого решения
B) Б) защита организации от внешнего воздействия
C) В) психологическое влияние на персонал с целью достижения собственных выгод
ANSWER: C

Групповое принятие решений имеет ряд преимуществ по сравнению с индивидуальным. Выберите их:
A) А) более полное информационное обеспечение процесса принятия решений
B) Б) более высокая обоснованность и меньший процент ошибок
C) В) более высокий уровень творчества
D) Г) как правило, требуют меньше времени
E) Д) все перечисленные
ANSWER: E

По степени и уровню информационной обеспеченности выделяют следующие управленческие решения:
A) А)глобальные и локальные
B) Б) перспективные и текущие
C) В) запрограммированные и незапрограммированные
D) Г) единоличные, консультативные и совместные
E) Д) детерминированные, вероятностные и неопределенные
F) Е) директивные и рекомендательные
ANSWER: E

Благодаря выполнению какого требования, предъявляемых к управленческим решениям, должно быть возможным изменять цель и (или) алгоритм достижения цели при изменении внешних и внутренних условий:
A) А) обоснованность
B) Б) своевременность
C) В) четкость формулировок
D) Г) эффективность
E) Д) реальная осуществимость
F) Е) гибкость
ANSWER: F

На каком этапе разработки и принятия управленческих решений наиболее эффективными методами являются «мозговая атака» («мозговой штурм») и метод «Дельфи»:
A) А) формулировка задачи

B) Б) разработка вариантов решения (поиск решения)
C) В) оценка вариантов решения и выбор оптимального
D) Г) принятие решения
E) Д) реализация и контроль
F) Е) оценка принятого решения
ANSWER: C
Проведите соответствиеУправленческое решение это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: B
Проведите соответствиеТехнические средства обработки информации это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: C
Основателем школы научного управления является:
A) А) А. Смит;
B) Б) Ф. Тейлор;
C) В) А. Файоль;
D) Г) Д. МакГрегор
ANSWER: D
Опыт, навыкиТехнические средства обработки информации это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: A
Проведите соответствиеИнтеллектуальные способности это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: A
Проведите соответствиеИнформация о проблемах это
A) А) Предмет труда
B) Б) Результат труда
C) В) Средства труда
ANSWER: A
КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМОриентирован на создание структуры, выработку правил, внутренних стандартов и правил функционирования системы
A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: A
КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМФормирует цели и пути их достижения. Оперирует системами в целом – предприятиями, организациями, государственными структурами
A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: B

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМНапоминает стратегический, но работает на уровне отдельных подразделений или подсистем. Тактическим менеджментом занимаются управленцы среднего звена

A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: C

КАКОЙ ВИД УПРАВЛЕНИЯ МОЖНО ОПИСАТЬ СЛЕДУЮЩИМ ОБРАЗОМИспользуется для решения текущих задач, стоящих перед системой. Основная функция – грамотное распределение ресурсов и контроль над выполнением поставленных задач

A) Организационный
B) Стратегический
C) тактический
D) Оперативный
ANSWER: D

Определите, к какой школе управления относятся приведенные ниже тезисы1. Применение приемов управления межличностными отношениями для повышения степени удовлетворенности и производительности.2. Применение наук о человеческом поведении к управлению и формированию организации таким образом, чтобы каждый работник мог быть полностью использован в соответствии с его потенциалом.

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: A

Определите, к какой школе управления относятся приведенные ниже тезисы1. Использование научного анализа для определения лучших способов выполнения задачи.2. Отбор работников, лучше всего подходящих для выполнения задач, и обеспечение их обучения.3. Обеспечение работников ресурсами, требуемыми для эффективного выполнения задач.4. Систематическое и правильное использование материального стимулирования для повышения производительности.5. Отделение планирования и обдумывания от самой работы.

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: B

Определите, к какой школе управления относятся приведенные ниже тезисы1. Углубление понимания сложных управленческих проблем благодаря разработке и применению моделей.2. Развитие и использование количественных методов руководителями, которым они помогают в принятии сложных решений

A) Школа человеческих отношений
B) Школа научного управления
C) Школа количественных методов
D) Школа научного управления
ANSWER: C

В соответствии с принципами школы научного управления:

A) А) оплата труда рабочих должна соответствовать полученному результату;

B) Б) оплата труда рабочих не зависит от полученных результатов;

C) В) оплата труда зависит от количества рабочего времени;

D) Г) оплата труда рабочих должна соответствовать выслуге лет

ANSWER: A

Определите, к какой школе управления относятся приведенные ниже тезисы1. Развитие принципов управления.2. Описание функций управления.3. Систематизированный подход к управлению всей организации

A) Школа человеческих отношений

B) Школа научного управления

C) Школа количественных методов

D) Школа научного управления

ANSWER: D

М. Вебер разработал:

A) А) систему бюрократического построения организации;

B) Б) принципы менеджмента;

C) В) иерархическую систему управления;

D) Г) теорию потребностей

ANSWER: A

Процессный подход рассматривает управление как:

A) А) непрерывную серию взаимосвязанных управленческих функций;

B) Б) совокупность элементов организации;

C) В) систему отдельных подсистем организации;

D) Г) пригодность методов управления определяется ситуацией

ANSWER: A

Под менеджментом понимается:

A) А) управление условиями обеспечения ресурсами;

B) Б) управление государством

C) В) управление организацией, действующей в рыночных условиях;

D) Г) управление людьми

ANSWER: C

Что такое защита информации?

A) Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

B) Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физиче-ского, духовного и интеллектуального развития, а также защи-та информации, обеспечивающая личную безопасность

C) Деятельность, направленная на предотвращение НСД к информации

D) Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию

ANSWER: D

Концептуальная комплексность включает:

A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы

B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла

C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства

D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода

ANSWER: D

Техническая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных ипрограммно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: A

Физическая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: C

Правовая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: D

Криптографическая защита информации – это:

A) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств

B) защита информации с помощью ее криптографического преобразования

C) защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты

D) защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением

ANSWER: B

Способ защиты информации – это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) заранее намеченный результат защиты информации

C) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации

D) порядок и правила применения определенных принципов и средств защиты информации

ANSWER: D

Какие из перечисленных угроз относятся к случайным угрозам компьютерной информации:

A) несанкционированный доступ к информации, вредительские программы, ошибки при разработке компьютерной системы

B) электромагнитные излучения и наводки, несанкционированная модификация структур компьютерной системы

C) стихийные бедствия и аварии, сбои и отказы технических средств, ошибки пользователей и обслуживающего персонала

D) технические каналы утечки информации

ANSWER: C

Замысел защиты информации – это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) деятельность по обеспечению защиты информации не криптографическими методами от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию

C) совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация

D) реализация конституционных прав человека и гражданина на до-ступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность

ANSWER: A

Технический канал утечки информации – это:

A) совокупность объекта разведки, средства разведки, среды распространения сигнала

B) возможность доступа к информации с нарушением правил разграничения доступа

C) совокупность ресурсов автоматизированной системы и человека

D) возможность доступа к информации с помощью штатных средств автоматизированной системы

ANSWER: A

Несанкционированный доступ (НСД) к информации – это:

A) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)

B) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств

C) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа

D) совокупность объекта разведки, средства разведки, среды распространения сигнала

ANSWER: A

Безопасность информации – это:

A) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)

B) состояние защищенности информации (данных) при котором обеспечивается ее (их) конфиденциальность, доступность и целостность

C) реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физиче-ского, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность

D) деятельность, направленная на предотвращение НСД к информации

ANSWER: B

Структурная комплексность включает:

A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы

B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла

C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства

D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода

ANSWER: C

Временная комплексность включает:

A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы

B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла

C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства

D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода

ANSWER: B

Целевая комплексность включает:

A) обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы

B) обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла

C) защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства

D) комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода

ANSWER: A

К источникам угроз безопасности информации относятся:

A) нарушитель

B) вредоносная программа

C) программно-аппаратная (аппаратная) закладка

D) все перечисленное.

ANSWER: D

Какая функция решается подсистемой регистрации событий безопасности информации?

A) идентификация и аутентификация пользователей, являющихся работниками оператора

B) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

C) сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

ANSWER: C

В ходе анализа защищенности информационной системы реализуются

A) обновление базы данных признаков вредоносных компьютерных программ (вирусов);

B) выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

C) контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

D) контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

E) функции б), в), г)

F) все функции

ANSWER: E

Принятие решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется

A) оператором информационной системы

B) владельцем информационной системы

C) федеральным органом исполнительной власти

ANSWER: B

При обеспечении защиты на этапе эксплуатации осуществляются

A) управление (администрирование) системой защиты информации информационной системы
B) выявление инцидентов и реагирование на них
C) управление конфигурацией информационной системы и ее системы защиты информации
D) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе
E) все перечисленное
ANSWER: E
Какой вид не относится к стратегиям защиты информации в компьютерной сети?
A) стратегия периметровой защиты
B) стратегия отступления
C) стратегия пресечения
D) стратегия адаптивной защиты
ANSWER: B
Какой вид не относится к стратегиям защиты информации в компьютерной сети?
A) стратегия периметровой защиты
B) стратегия отступления
C) стратегия пресечения
D) стратегия адаптивной защиты
ANSWER: B
Недостаток (слабость) информационной системы – это:
A) ошибки в программном обеспечении
B) ошибки в параметрах настройки
C) ошибки технологии обработки (передачи) информации
D) все перечисленное
ANSWER: D
Сколько всего классов защищенности автоматизированных систем?
A) 3
B) 6
C) 9
D) 12
ANSWER: C
Сколько всего классов защиты государственных информационных систем?
A) 3
B) 6
C) 9
D) 12
ANSWER: A
Сколько всего классов защиты средств вычислительной техники?
A) 3
B) 6
C) 9
D) 12
ANSWER: B
Уязвимость характеризуется:
A) слабостью
B) недостатком
C) слабостью и (или) недостатком
D) условиями и факторами
ANSWER: C

Угроза характеризуется
A) слабостью
B) недостатком
C) слабостью и (или) недостатком
D) условиями и факторами
ANSWER: D
ERP – система это:
A) система управления ресурсами предприятия
B) система регистрации событий безопасности информации
C) система управления инцидентами безопасности информации
D) система управления доступом
ANSWER: A
Какие функции не выполняет подсистема идентификации и аутентификации:
A) идентификация и аутентификация пользователей, являющихся работниками оператора
B) идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
C) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
D) ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
ANSWER: D
Какие функции не выполняет подсистема управления доступом?
A) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
B) управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
C) реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
D) управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
E) правильный ответ отсутствует
ANSWER: B
Информационная безопасность Российской Федерации – это:
A) состояние защищенности информации, циркулирующей в обществе;
B) состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;
C) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;
D) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.
ANSWER: D
Служебная информация ограниченного распространения – это:

A) акт законодательства, устанавливающий правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

B) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

C) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

D) информация, основанная на документах, фактах.

ANSWER: B

Допуск гражданина к сведениям, составляющим государственную тайну, может быть прекращен в случае:

A) перевода и приема гражданина на работу в подразделение по защите государственной тайны, шифровальные или мобилизационные органы;

B) возвращения из длительных (свыше 6 месяцев) заграничных командировок;

C) однократного нарушения им предусмотренных трудовым договором (контрактом) обязательств, связанных с сохранением государственной тайны;

D) вступления гражданина в брак, за исключением случаев, когда оба супруга работают в одной организации и имеют допуск по второй или третьей форме.

ANSWER: C

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация – это:

A) сведения (сообщения, данные) независимо от формы их представления;

B) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

C) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

D) сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.

ANSWER: A

Каким нормативным правовым документом утверждены правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?

A) Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203;

B) Указ Президента Российской Федерации от 6 марта 1997 г. № 188;

C) Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870;

D) Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

ANSWER: C

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под персональными данными понимается:

A) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту

персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

B) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

C) зафиксированная на материальном носителе информация о личности с реквизитами, позволяющими ее идентифицировать;

D) сведения, касающиеся личности, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности.

ANSWER: B

Какие категории персональных данных выделяет Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?

A) общедоступные персональные данные, специальные категории персональных данных, категории персональных данных, обрабатываемые в информационных системах персональных данных, биометрические персональные данные;

B) общедоступные персональные данные, специальные категории персональных данных, биометрические персональные данные и иные;

C) общедоступные персональные данные, категории персональных данных, обрабатываемые в информационных системах персональных данных;

D) данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

ANSWER: B

В соответствии с п. 3 ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» по категории доступа информация делится на:

A) общедоступную информацию и информацию с ограниченным доступом (информация ограниченного доступа);

B) открытую и конфиденциальную;

C) конфиденциальную и секретную;

D) служебную информацию ограниченного доступа и общедоступную.

ANSWER: A

Соблюдение каких правил входит в защиту правомочий обладателя информации?

A) соблюдение конфиденциальности информации – свойство информационной технологии (ИТ) обеспечивать раскрытие информации только в соответствии с правилами разграничения доступа (право распоряжения);

B) соблюдение целостности информации – свойство ИТ обеспечивать предоставление права модификации (уничтожения) информации только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность информации в условиях случайных ошибок или стихийных бедствий (право владения);

C) соблюдение доступности информации – свойство ИТ обеспечивать свободный доступ к информации по мере возникновения необходимости (право пользования);

D) соблюдение всех перечисленных правил.

ANSWER: D

Какая из перечисленных видов тайн относится к категории конфиденциальной информации?

A) государственная тайна, персональные данные, коммерческая тайна, служебная тайна;

B) персональные данные, коммерческая тайна, служебная тайна;

C) государственная тайна, коммерческая тайна, служебная тайна;

D) секретные сведения, совершенно секретные сведения, сведения особой важности.

ANSWER: B

Каков срок засекречивания сведений, составляющих государственную тайну?

A) 10 лет;

B) 20 лет;

C) 30 лет;

D) 40 лет.

ANSWER: C

Каким нормативным правовым документом утверждена Доктрина информационной безопасности?

A) Указ Президента РФ №136 от 16.03.2015 г.

B) ФЗ от 27.07.2006 г. №152

C) Постановление Правительства РФ №1233 от 3.11.1993 г.

D) Указ Президента РФ №646 от 6.12.2016 г.

ANSWER: D

Как часто органы государственной власти должны пересматривать перечни сведений, подлежащих засекречиванию?

A) каждые 3 года;

B) каждые 5 лет;

C) каждые 7 лет;

D) каждые 10 лет.

ANSWER: B

Что из перечисленного является основанием для рассекречивания сведений, составляющих государственную тайну:

A) отсутствие в органах государственной власти Перечня сведений, составляющих государственную тайну;

B) принятие на себя обязательств перед государством по нераспространению сведений, составляющих государственную тайну;

C) взятие на себя Россией обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;

D) отсутствие специальных помещений для хранения документов, содержащих сведения, составляющие государственную тайну.

ANSWER: C

Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных:

A) осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник;

B) необходима в связи с осуществлением правосудия;

C) необходима в связи с выездом за пределы Российской Федерации;

D) необходима в соответствии с оперативно-розыскной деятельностью.

ANSWER: C

Режим документированной информации – это:

A) электронный документ с электронной подписью;

B) выделенная информация по определенной цели;

C) выделенная информация в любой знаковой форме;

D) электронная информация, позволяющая ее идентифицировать.

ANSWER: A

В правовой режим документированной информации входит:

A) государственная тайна;

B) банковская тайна;

C) персональные данные;

D) электронная цифровая подпись.

ANSWER: D

Засекречиванию подлежат сведения о:

A) фактах нарушения прав и свобод человека и гражданина;

B) состоянии демографии;

C) силах и средствах гражданской обороны;

D) состоянии преступности.

ANSWER: C

Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:

A) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно;

B) для доставки почтовых отправлений;

C) в целях профессиональной деятельности журналиста;

D) в целях профессиональной деятельности оператора.

ANSWER: D

Открытость информации в архивных фондах обеспечивается:

A) различными режимами доступа к информации и переходом информации из одной категории доступа в другую;

B) различными режимами доступа к информации;

C) переходом информации из одной категории доступа в другую;

D) правовым статусом архивного фонда.

ANSWER: A

К государственной тайне не относятся сведения, защищаемые государством, распространение которых может нанести ущерб государству:

A) в экономической области;

B) в контрразведывательной деятельности;

C) в оперативно-розыскной деятельности;

D) о частной жизни политических деятелей.

ANSWER: D

Обработка персональных данных – это:

A) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

B) накопление, хранение и передача персональных данных;

C) размещение персональных данных в информационных системах;

D) только передача персональных данных.

ANSWER: A

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в:

A) Конституции РФ;

B) Гражданском кодексе РФ

C) Доктрине информационной безопасности РФ;

D) Федеральном законе «Об информации, информационных технологиях и о защите информации».

ANSWER: C

Срок хранения персональных данных, осуществляемого в форме, позволяющей определить субъекта персональных данных:

A) 1 год

B) 5 лет

C) Не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено законом или договором;

D) 3 года.

ANSWER: C

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные системы не включают в себя:

A) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

B) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

C) иные информационные системы;

D) частные информационные системы.

ANSWER: D

Базовым законом, регулирующим информационные отношения является:

A) ФЗ «О коммерческой тайне»;

B) Закон РФ «Об авторском праве и смежных правах»;

C) ФЗ «Об информации, информационных технологиях и защите информации»;

D) ФЗ «Об архивном деле».

ANSWER: C

Понятие информационной инфраструктуры Российской Федерации закреплено в:

A) Конституции РФ;

B) Федеральном законе от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

C) Доктрине информационной безопасности РФ;

D) не закреплено в нормативных правовых документах.

ANSWER: C

В соответствии с частью 3 статьи 29 Конституции Российской Федерации каждый имеет право свободно:

A) искать и распространять информацию любым способом

B) искать, получать, передавать, производить и распространять информацию любым законным способом;

C) искать, получать, передавать, производить и распространять информацию любым способом;

D) получать и распространять информацию любым способом

ANSWER: B

Федеральный закон от 27 июля2006 г. «О персональных данных» не регулирует отношения, возникающие при:

A) обработке персональных данных, отнесенных к государственной тайне;

B) хранении, комплектовании, учете и использовании архивных документов;

C) обработке персональных данных, отнесенных к служебной тайне;

D) включении в Единый государственный реестр индивидуальных предпринимателей.

ANSWER: C

Каким нормативным правовым документом утвержден перечень сведений конфиденциального характера?

A) Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203;

B) Указом Президента Российской Федерации от 6 марта 1997 г. № 188;

C) Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870;

D) Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

ANSWER: B

К МЕТОДАМ АНАЛИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОТНОСЯТ

A) Метод экспериментов

B) Статический метод

C) Динамический метод

D) Все предложенные выше методы

ANSWER: D

ОВЕРЛЕЙНАЯ ПРОГРАММА ЭТО:

A) которая полностью размещается в оперативной памяти

B) которая размещает в оперативной памяти только фрагменты кода, которые выполняются в данный момент

C) которая не использует для запуска оперативную память

D) которая полностью размещается в файле подкачки

ANSWER: B

КОНСОЛЬНАЯ ПРОГРАММА ИМЕЕТ:

A) одну точку входа

B) две точки входа

C) три точки входа

D) не имеет точек входа, точку входа имеет только программа с графическим интерфейсом

ANSWER: A

СИСТЕМНЫЙ ОТЛАДЧИК ИСПОЛЬЗУЕТСЯ ДЛЯ:

A) анализа консольных программ

B) анализа кода, выполняющегося в режиме ядра

C) анализа кода графических программ

D) такого отладчика не существует

ANSWER: B

ЯДЕРНЫЙ ОТЛАДЧИК ИСПОЛЬЗУЕТСЯ ДЛЯ:

A) анализа консольных программ

B) анализа кода, выполняющегося в режиме ядра

C) анализа кода графических программ

D) такого отладчика не существует

ANSWER: D

ГРАФИЧЕСКИЙ ОТЛАДЧИК ИСПОЛЬЗУЕТСЯ ДЛЯ:

A) анализа консольных программ

B) анализа кода, выполняющегося в режиме ядра

C) анализа кода графических программ

D) такого отладчика не существует

ANSWER: D

МЕТОД ВКЛЮЧЕНИЯ СРЕДСТВ ЗАЩИТЫ ОТ АНАЛИЗА В ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

A) встроенная защита

B) пристыковочная защита
C) встроенная и пристыковочная защиты
D) ничего из вышеперечисленного
ANSWER: C
ДИНАМИЧЕСКОЕ ИЗМЕНЕНИЕ КОДА ПРОГРАММЫ ЗАКЛЮЧАЕТСЯ В ТОМ, ЧТО:
A) код программы, за исключением распаковщика, хранится в исполняемом файле в искаженном виде, а преобразуется к нормальному в оперативной памяти
B) код программы, за исключением распаковщика, хранится в исполняемом файле в нормальном виде, преобразуется к искаженному в оперативной памяти
C) код программы, за исключением распаковщика, хранится в исполняемом файле в нормальном виде, в оперативной памяти по коду каждый раз генерится разный ассемблерный код
D) код программы может храниться только в оперативной памяти
ANSWER: A
МЕТОД ИСКУССТВЕННОГО УСЛОЖНЕНИЯ ПРОГРАММЫ:
A) использует обычную команду call для передачи управления из одной функции в другую
B) не использует обычную команду call для передачи управления из одной функции в другую
C) генерирует пустые функции в которые передается управления с помощью команды call
D) генерирует пустые функции в которые передается управления с помощью команды отличной от call
ANSWER: B
ОБРАЩЕНИЕ К СИСТЕМНЫМ ФУНКЦИЯМ ИЗ ПРОГРАММЫ МОЖЕТ ПРОИСХОДИТЬ ПОСРЕДСТВОМ:
A) динамического импорта
B) статического импорта
C) мы не можем использовать системные функции , так как они инкапсулированы
D) динамический и статический импорт
ANSWER: D
ИСКУССТВЕННОЕ УСЛОЖНЕНИЕ АЛГОРИТМА ОБРАБОТКИ ДАННЫХ ЗАКЛЮЧАЕТСЯ В:
A) многократное копирование данных с места на место
B) создание большого количества копий одних и тех же данных
C) применение к данным сложных преобразований
D) все из вышеперечисленного
ANSWER: D
МЕТОД ЭКСПЕРИМЕНТОВ С «ЧЕРНЫМ ЯЩИКОМ»:
A) подразумевает решение задачи построения автомата, эквивалентного данному на основе анализа его входа и выхода
B) метод проб и ошибок, так как основной функционал не описан и является для нас «черным ящиком»
C) такого метода не существует
ANSWER: A
В БОЛЬШИНСТВЕ СЛУЧАЕВ ВЗАИМОДЕЙСТВИЕ ПРОГРАММНОЙ ЗАКЛАДКИ С АТАКУЕМОЙ КОМПЬЮТЕРНОЙ СИСТЕМОЙ ОПИСЫВАЕТСЯ С ПОМОЩЬЮ ФОРМАЛЬНОЙ МОДЕЛИ:
A) наблюдатель
B) перехват

C) искажение
D) все из вышеперечисленного
ANSWER: D
МОДЕЛЬ НАБЛЮДАТЕЛЬ ПРИМЕНЯЕТСЯ ДЛЯ:
A) внедрения других программных закладок
B) анализ сетевого трафика
C) такой модели не существуе
ANSWER: A
В РОЛИ ОБЪЕКТА В МОДЕЛИ ПЕРЕХВАТ ВЫСТУПАЕТ:
A) клавиатура, файловые системы, физические и логические устройства сети
B) оперативная память, центральный процессор
C) такой модели не существует
ANSWER: A
В МОДЕЛИ ИСКАЖЕНИЕ:
A) программная закладка встраивается в программное обеспечение, обслуживающее сетевые потоки определенного класса
B) программная закладка встраивается в программное обеспечение, обслуживающее информационные потоки определенного класса
C) такой модели не существует
ANSWER: B
ТИПИЧНЫЕ УЯЗВИМОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ:
A) переполнение буферов
B) отсутствие необходимых проверок входных данных
C) другое
D) переполнение буферов и отсутствие необходимых проверок входных данных
ANSWER: D
ВИРУС:
A) программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, компьютерных сетей, осуществлять деструктивные действия
B) программа для уничтожения информации в компьютерной системе
C) программа для утечки информации в компьютерной системе
D) программа для искажения информации в компьютерной системе
ANSWER: A
АЛГОРИТМ ФУНКЦИОНИРОВАНИЯ ОНЛАЙН-ВИРУСА ВКЛЮЧАЕТ В СЕБЯ:
A) сканирование ip-адреса жертвы
B) сканирование серийного номера сетевого устройства
C) сканирование ip-адреса жертвы только в протоколе ipv4, так как в ipv6 данная уязвимость была закрыта
ANSWER: A
СИГНАТУРНОЕ СКАНИРОВАНИЕ:
A) поиск в файлах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов
B) поиск в файловых системах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов
C) поиск в операционных системах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов
D) поиск в браузерах сигнатур или масок, особых участков кода и данных, характерных для некоторых вирусов
ANSWER: A
ЕСЛИ ИЗВЕСТНА ДЛИНА ТЕЛЕ ВИРУСА И ЗНАЧЕНИЯ НЕКОТОРЫХ БАЙТОВ ТЕЛА ВИРУСА, ТО ПРИЗНАКАМИ ЗАРАЖЕНИЯ ФАЙЛА ЯВЛЯЮТСЯ:

A) наличие в первых байтах проверяемого файла команды перехода на адрес длина_файла — длина_тела_вируса

B) наличие в конце проверяемого файла определенных байт

C) все из вышеперечисленного

D) ничего из вышеперечисленного

ANSWER: C

ЭВРИСТИЧЕСКОЕ СКАНИРОВАНИЕ:

A) поиск сигнатур, типичных не для конкретных образцов компьютерных вирусов и(или) программных закладок, а для вредоносного программного обеспечения вообще

B) поиск сигнатур, не типичных не для конкретных образцов компьютерных вирусов и(или) программных закладок, а для вредоносного программного обеспечения вообще

C) поиск сигнатур, не типичных для конкретных образцов компьютерных вирусов

D) поиск сигнатур, не типичных для конкретных образцов к программных закладок

ANSWER: A

ПРИ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ АЛГОРИТМОВ ДИЗАССЕМБЛИРОВАНИЯ ВОЗНИКАЮТ СЛЕДУЮЩИЕ ПРОБЛЕМЫ:

A) проблема восстановления символических имен

B) проблема различения программ и данных

C) проблема определения границы машинной команды

D) все описанные проблемы

ANSWER: D

КОНТРОЛЬ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ОСУЩЕСТВЛЯЕТСЯ ЗА СЧЕТ:

A) хранения длины файла

B) хранения контрольной суммы

C) хранения длины файла и контрольной суммы

D) закрытия исходного кода файла криптографическими протоколами

ANSWER: C

ДИНАМИЧЕСКИЙ МЕТОД АНАЛИЗА ПРОГРАММНЫХ РЕАЛИЗАЦИЙ:

A) основан на использовании программных отладочных средств

B) использует оперативную память как динамическую систему для анализа

C) использует в качестве анализа BIOS

D) ничего из вышеперечисленного не верно

ANSWER: A

ОТЛАДЧИК ЭТО:

A) программа, которая загружает в память другую программу и предоставляет пользователю возможность наблюдать за ходом выполнения этой программы

B) программа, которая предоставляет пользователю возможность наблюдать за ходом выполнения запущенных процессов в операционной системе, но сама ничего не загружает

C) программа для загрузки других программ в память

ANSWER: A

ФЛАГ ТРАССИРОВКИ:

A) когда равен 1, процессор после выполнения каждой машинной команды вызывает прерывание 5

B) когда равен 1, процессор после выполнения каждой машинной команды вызывает прерывание 48

C) когда равен 1, процессор после выполнения каждой машинной команды вызывает прерывание 1

D) такого флага не существует

ANSWER: C

В АНАЛИЗ ПРОГРАММЫ МЕТОДИЧЕСКИМ МЕТОДОМ ВКЛЮЧАЕТСЯ:

A) поиск подходов к интересующим функциям программы

B) поиск интересующих функций программы

C) анализ интересующих функций программы

D) все из вышеперечисленного

ANSWER: D

В МЕТОДЕ МАЯКОВ, МАЯКИ ЭТО:

A) точки входа в программу для анализа

B) точки выхода из программы

C) точки программы, в которых программа выполняет действия, легко понимаемые без знания контекста, в котором эти действия выполняются

D) точки программы, в которых программа выполняет действия, не понимаемые без знания контекста, в котором эти действия выполняются

ANSWER: C

МЕТОД STEP-TRACE МОЖЕТ БЫТЬ ИСПОЛЬЗОВАН ДЛЯ ПОИСКА В ПРОГРАММЕ ФУНКЦИИ X, ДЛЯ КОТОРОЙ ВЫПОЛНЯЕТСЯ УСЛОВИЕ:

A) реализует интересующие аналитика алгоритмы

B) легко обнаруживается по внешним проявлениям программы

C) может быть запущена в режиме Step (пошагово)

D) реализует интересующие аналитика алгоритмы и легко обнаруживается по внешним проявлениям программы

ANSWER: D

Информационная безопасность Российской Федерации – это:

A) состояние защищенности информации, циркулирующей в обществе;

B) состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;

C) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;

D) состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

ANSWER: D

Служебная информация ограниченного распространения – это:

A) акт законодательства, устанавливающий правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

B) несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами;

C) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

D) информация, основанная на документах, фактах.

ANSWER: B

Допуск гражданина к сведениям, составляющим государственную тайну, может быть прекращен в случае:

A) перевода и приема гражданина на работу в подразделение по защите государственной тайны, шифровальные или мобилизационные органы;

B) возвращения из длительных (свыше 6 месяцев) заграничных командировок;

C) однократного нарушения им предусмотренных трудовым договором (контрактом) обязательств, связанных с сохранением государственной тайны;

D) вступления гражданина в брак, за исключением случаев, когда оба супруга работают в одной организации и имеют допуск по второй или третьей форме.

ANSWER: C

В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информация – это:

A) сведения (сообщения, данные) независимо от формы их представления;

B) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

C) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;

D) сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.

ANSWER: A

Каким нормативным правовым документом утверждены правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности?

A) Указ Президента Российской Федерации от 30 ноября 1995 г. № 1203;

B) Указ Президента Российской Федерации от 6 марта 1997 г. № 188;

C) Постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870;

D) Постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

ANSWER: C

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под персональными данными понимается:

A) любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

B) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

C) зафиксированная на материальном носителе информация о личности с реквизитами, позволяющими ее идентифицировать;

D) сведения, касающиеся личности, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности.

ANSWER: B

Какие категории персональных данных выделяет Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»?

A) общедоступные персональные данные, специальные категории персональных данных, категории персональных данных, обрабатываемые в информационных системах персональных данных, биометрические персональные данные;

B) общедоступные персональные данные, специальные категории персональных данных, биометрические персональные данные и иные;

C) общедоступные персональные данные, категории персональных данных, обрабатываемые в информационных системах персональных данных;

D) данные о расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

ANSWER: B

В соответствии с п. 3 ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» по категории доступа информация делится на:

A) общедоступную информацию и информацию с ограниченным доступом (информация ограниченного доступа);

B) открытую и конфиденциальную;

C) конфиденциальную и секретную;

D) служебную информацию ограниченного доступа и общедоступную.

ANSWER: A

Соблюдение каких правил входит в защиту правомочий обладателя информации?

A) соблюдение конфиденциальности информации – свойство информационной технологии (ИТ) обеспечивать раскрытие информации только в соответствии с правилами разграничения доступа (право распоряжения);

B) соблюдение целостности информации – свойство ИТ обеспечивать предоставление права модификации (уничтожения) информации только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность информации в условиях случайных ошибок или стихийных бедствий (право владения);

C) соблюдение доступности информации – свойство ИТ обеспечивать свободный доступ к информации по мере возникновения необходимости (право пользования);

D) соблюдение всех перечисленных правил.

ANSWER: D

Какая из перечисленных видов тайн относится к категории конфиденциальной информации?

A) государственная тайна, персональные данные, коммерческая тайна, служебная тайна;

B) персональные данные, коммерческая тайна, служебная тайна;

C) государственная тайна, коммерческая тайна, служебная тайна;

D) секретные сведения, совершенно секретные сведения, сведения особой важности.

ANSWER: B

Каков срок засекречивания сведений, составляющих государственную тайну?

A) 10 лет;

B) 20 лет;

C) 30 лет;

D) 40 лет.
ANSWER: C
Каким нормативным правовым документом утверждена Доктрина информационной безопасности?
A) Указ Президента РФ №136 от 16.03.2015 г.
B) ФЗ от 27.07.2006 г. №152
C) Постановление Правительства РФ №1233 от 3.11.1993 г.
D) Указ Президента РФ №646 от 6.12.2016 г.
ANSWER: D
Как часто органы государственной власти должны пересматривать перечни сведений, подлежащих засекречиванию?
A) каждые 3 года;
B) каждые 5 лет;
C) каждые 7 лет;
D) каждые 10 лет.
ANSWER: B
Что из перечисленного является основанием для рассекречивания сведений, составляющих государственную тайну:
A) отсутствие в органах государственной власти Перечня сведений, составляющих государственную тайну;
B) принятие на себя обязательств перед государством по нераспространению сведений, составляющих государственную тайну;
C) взятие на себя Россией обязательств по открытому обмену сведениями, составляющими в РФ государственную тайну;
D) отсутствие специальных помещений для хранения документов, содержащих сведения, составляющие государственную тайну.
ANSWER: C
Обработка специальных категорий персональных данных в отношении религиозных или философских убеждений допускается в случае, когда обработка персональных данных:
A) осуществляется в медицинских целях для установления диагноза при условии, что ее осуществляет профессиональный медицинский работник;
B) необходима в связи с осуществлением правосудия;
C) необходима в связи с выездом за пределы Российской Федерации;
D) необходима в соответствии с оперативно-розыскной деятельностью.
ANSWER: C
Режим документированной информации – это:
A) электронный документ с электронной подписью;
B) выделенная информация по определенной цели;
C) выделенная информация в любой знаковой форме;
D) электронная информация, позволяющая ее идентифицировать.
ANSWER: A
В правовой режим документированной информации входит:
A) государственная тайна;
B) банковская тайна;
C) персональные данные;
D) электронная цифровая подпись.
ANSWER: D
Засекречиванию подлежат сведения о:
A) фактах нарушения прав и свобод человека и гражданина;
B) состоянии демографии;
C) силах и средствах гражданской обороны;
D) состоянии преступности.
ANSWER: C

Согласие субъекта персональных данных на их обработку требуется, когда обработка персональных данных осуществляется:

A) для защиты жизненно важных интересов субъекта персональных данных, если получить его согласие невозможно;

B) для доставки почтовых отправлений;

C) в целях профессиональной деятельности журналиста;

D) в целях профессиональной деятельности оператора.

ANSWER: D

Открытость информации в архивных фондах обеспечивается:

A) различными режимами доступа к информации и переходом информации из одной категории доступа в другую;

B) различными режимами доступа к информации;

C) переходом информации из одной категории доступа в другую;

D) правовым статусом архивного фонда.

ANSWER: A

К государственной тайне не относятся сведения, защищаемые государством, распространение которых может нанести ущерб государству:

A) в экономической области;

B) в контрразведывательной деятельности;

C) в оперативно-розыскной деятельности;

D) о частной жизни политических деятелей.

ANSWER: D

Обработка персональных данных – это:

A) любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

B) накопление, хранение и передача персональных данных;

C) размещение персональных данных в информационных системах;

D) только передача персональных данных.

ANSWER: A

Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в:

A) Конституции РФ;

B) Гражданском кодексе РФ

C) Доктрине информационной безопасности РФ;

D) Федеральном законе «Об информации, информационных технологиях и о защите информации».

ANSWER: C

Срок хранения персональных данных, осуществляемого в форме, позволяющей определить субъекта персональных данных:

A) 1 год

B) 5 лет

C) Не дольше, чем этого требуют цели обработки персональных данных, если иное не установлено законом или договором;

D) 3 года.

ANSWER: C

В соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» информационные системы не включают в себя:

A) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

B) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

C) иные информационные системы;

D) частные информационные системы.

ANSWER: D

Базовым законом, регулирующим информационные отношения является:

A) ФЗ «О коммерческой тайне»;

B) Закон РФ «Об авторском праве и смежных правах»;

C) ФЗ «Об информации, информационных технологиях и защите информации»;

D) ФЗ «Об архивном деле».

ANSWER: C

Понятие информационной инфраструктуры Российской Федерации закреплено в:

A) Конституции РФ;

B) Федеральном законе от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

C) Доктрине информационной безопасности РФ;

D) не закреплено в нормативных правовых документах.

ANSWER: C

В соответствии с частью 3 статьи 29 Конституции Российской Федерации каждый имеет право свободно:

A) искать и распространять информацию любым способом

B) искать, получать, передавать, производить и распространять информацию любым законным способом;

C) искать, получать, передавать, производить и распространять информацию любым способом;

D) получать и распространять информацию любым способом

ANSWER: B

Федеральный закон от 27 июля2006 г. «О персональных данных» не регулирует отношения, возникающие при:

A) обработке персональных данных, отнесенных к государственной тайне;

B) хранении, комплектовании, учете и использовании архивных документов;

C) обработке персональных данных, отнесенных к служебной тайне;

D) включении в Единый государственный реестр индивидуальных предпринимателей.

ANSWER: C

Каким нормативным правовым документом утвержден перечень сведений конфиденциального характера?

A) Указом Президента Российской Федерации от 30 ноября 1995 г. № 1203;

B) Указом Президента Российской Федерации от 6 марта 1997 г. № 188;

C) Постановлением Правительства Российской Федерации от 4 сентября 1995 г. № 870;

D) Постановлением Правительства Российской Федерации от 3 ноября 1994 г. № 1233.

ANSWER: B

Диапазон частот ПЭМИН:

A) 9 КГц – 10 ГГц

B) 20 Гц – 20 КГц

C) 300 Гц – 300 КГц

D) 2 ГГц – 20 ГГц

ANSWER: A

При индуктивном подключении телефонного закладочного устройства к телефонной линии общее сопротивление:

A) возрастет

B) уменьшится

C) останется без изменений

D) изменится в соответствии с гармоническим законом

ANSWER: C

Параметрический канал утечки информации образуется:

A) в результате высокочастотного облучения ОТСС

B) в результате изменения параметров среды распространения сигнала

C) в результате изменения параметров окружающей среды

D) в результате высокочастотного облучения ВТСС

ANSWER: A

Видимый диапазон длин волн:

A) 0,4 – 0,7 мкм

B) 0,4 – 1,2 мкм

C) 3 – 5 мкм

D) 8 – 14 мкм

ANSWER: A

Учетные записи локальных пользователей в системе Dallas Lock 8.0:

A) создаются в системе Dallas Lock только пользователями наделенными соответствующими полномочиями

B) создаются в операционной системе только пользователями, наделенными соответствующими полномочиями

C) создаются только администраторами безопасности системы Dallas Lock

D) создаются любым пользователем системы Dallas Lock

ANSWER: A

Межсетевой экран применяется для:

A) обнаружения сетевых атак или подозрительных намерений злоумышленника

B) разграничения доступа между двумя сетями с различными требованиями по обеспечению безопасности

C) контроля почтового трафика и Web-трафика

D) организации шифрованного сетевого соединения

ANSWER: B

Какой принцип управления межсетевым экраном предпочтительнее в компьютерной системе, обрабатывающей конфиденциальную информацию?

A) разрешено все, что не запрещено

B) запрещено все, что не разрешено

C) выборочной фильтрации трафика

D) контроля сетевых соединений

ANSWER: B

Защита информации в VPN (виртуальных частных сетях) обеспечивается с помощью:

A) межсетевых экранов и шифрования трафика

B) физической защиты информационных линий связи

C) инкапсуляции и декапсуляции сетевых пакетов

D) журналирования событий безопасности

ANSWER: C

Механизм замкнутой программной среды в системе Dallas Lock 8.0:

A) позволяет явно указать с какими программами пользователь может работать

B) позволят производить разграничение доступа пользователя к настройкам операционной системы

C) позволяет производить блокировку работы пользователя при НСД

D) позволяет осуществлять кодирование файлов и папок

ANSWER: A

Защита информации от непреднамеренного воздействия – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: A

Защита информации от НСД – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение

(затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: B

Защита информации от НСВ – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: D

Защита информации от утечки – это:

A) защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

B) защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации

C) защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации иностранными разведками и другими заинтересованными субъектами

D) защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации

ANSWER: C

Способ защиты информации – это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) заранее намеченный результат защиты информации

C) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации

D) порядок и правила применения определенных принципов и средств защиты информации

ANSWER: D

Специальное исследование (объекта защиты информации) – это:

A) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ

B) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации

C) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации

D) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств

ANSWER: C

Специальная проверка – это:

A) деятельность, заключающаяся в проверке (экспертизе) возможностей юридического лица выполнять работы в области защиты информации в соответствии с установленными требованиями и выдаче разрешения на выполнение этих работ

B) форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров. К объектам оценки могут относиться: средство защиты информации, средство контроля эффективности защиты информации

C) исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных правовых документов в области безопасности информации

D) проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств

ANSWER: D

Контроль целостности в системе Secret Net предназначен для:

A) слежения за неизменностью контролируемых объектов

B) выявления НСД

C) выявления вредоносного программного обеспечения

D) выявления нештатного подключения внешних устройств

ANSWER: A

Идентификация – это:

A) проверка принадлежности субъекту доступа предъявленного им идентификатора

B) установление соответствия реального объекта представленной на него документации, названию во избежание подмены одного объекта другим

C) присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

D) совокупность мероприятий по установлению и подтверждению достоверности сведений о пользователях с использованием оригиналов документов и (или) надлежащим образом заверенных копий

ANSWER: C

Какие основные способы разграничения доступа применяются в компьютерных системах?

A) дискреционный и мандатный

B) по специальным спискам и многоуровневый

C) по группам пользователей и специальным разовым разрешениям

D) парольное разграничение доступа и иерархическое

ANSWER: A

Что такое аудит безопасности компьютерной системы?

A) инструмент политики безопасности, позволяющий контролировать процесс загрузки системных драйверов

B) инструмент политики безопасности, позволяющий отслеживать действия пользователей и системные события и регистрировать их в журнале

C) инструмент политики безопасности, позволяющий наблюдать динамические изменения технического состояния аппаратных компонентов компьютера (температура материнской платы, скорость вращения вентилятора на процессоре и т.д.)

D) инструмент политики безопасности, направленный на проверку реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности

ANSWER: B

Замысел защиты информации - это:

A) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации

B) деятельность по обеспечению защиты информации не криптографическими методами от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию

C) совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация

D) реализация конституционных прав человека и гражданина на до-ступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность

ANSWER: A

Несанкционированный доступ (НСД) к информации – это:

A) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)

B) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств

C) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа

D) совокупность объекта разведки, средства разведки, среды распространения сигнала

ANSWER: A

Системы анализа уязвимостей позволяют:

A) выявить злоумышленника, работающего в компьютерной сети

B) выявить уязвимости проектируемой системы защиты информации

C) выявить уязвимости действующей системы защиты информации

D) выявить уязвимости по результатам журнала аудита безопасности

ANSWER: C

Акустические закладочные устройства – это:

A) специальные миниатюрные электронные устройства перехвата акустической (речевой) информации

B) специальные миниатюрные электронные устройства для перехвата информации в проводных линиях связи

C) специальные миниатюрные электронные устройства для съема видеоинформации

D) специальные миниатюрные электронные устройства для съема акустической информации, передаваемой по линиям связи

ANSWER: A

Радиозакладочными устройствами называют:

A) акустические закладки, передающие информацию по радиоканалу

B) акустические закладки, передающие информацию по проводным линиям связи

C) акустические закладки, передающие информацию по ИК-каналу

D) акустические закладки, передающие информацию по ВОЛС-линиям

ANSWER: A

Диапазон частот работы сканирующего приемника ar-8200:

A) 50 кГц…1500 МГц

B) 100 кГц… 1000 МГц

C) 1000МГц … 5200МГц

D) 500 кГц...2040 МГц

ANSWER: D

Цели защиты информации от технических средств разведки:

A) предотвращение утечки, хищения, утраты, искажения, подделки информации

B) предотвращение угроз безопасности личности, общества, государства

C) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации

D) все вышеперечисленные цели

ANSWER: D

Электрические каналы утечки информации образуются за счет:

A) наводок электромагнитных излучений технических средств передачи информации на соединительные линии вспомогательных технических средств

связи и посторонние проводники, выходящие за пределы контролируемой зоны

B) просачивания информационных сигналов в цепи электропитания технических средств передачи информации

C) просачивания информационных сигналов в цепи заземления технических средств передачи информации

D) все ответы верны

ANSWER: D

К какому классу устройств относится устройство AR8200?

A) индикатор поля

B) сканирующий приемник

C) анализатор спектра

D) нет правильных ответов

ANSWER: B

Комплекс радиомониторинга и выявления каналов утечки информации «Навигатор» предназначен для решения следующих задач:

A) оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации

B) оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства, системы и их коммуникации

C) оценки защищенности вспомогательных технических средств и систем, предназначенных для обработки, хранения и передачи по линиям связи конфиденциальной информации

D) оценки защищенности конфиденциальной информации от утечки по виброакустическому каналу

ANSWER: B

Мощность какого множества модели ХРУ больше: субъектов или объектов ?

A) субъектов

B) объектов

ANSWER: B

Какая ролевая модель реализует статическое разделение обязанностей?

A) модель с иерархической организацией ролей

B) модель с ограничениями на одновременное использование ролей в одном сеансе

C) модель со взаимоисключающими ролями

ANSWER: C

Какими понятиями замещается понятие «субъект» в ролевой модели?

A) объект

B) пользователь

C) сущность

D) роль

ANSWER: B

Что означает правило управления доступом user в ролевой модели?

A) для каждого сеанса определяет пользователя, который осуществляет этот сеанс работы с системой

B) для каждого сеанса задает набор доступных в нем полномочий, который определяется как совокупность полномочий всех ролей, задействованных в этом сеансе

C) для каждого сеанса определяет набор ролей, которые могут быть одновременно доступны пользователю в этом сеансе

ANSWER: A

Какая ролевая модель реализует динамическое разделение обязанностей?

A) модель с иерархической организацией ролей

B) модель с ограничениями на одновременное использование ролей в одном сеансе

C) модель со взаимоисключающими ролями

ANSWER: B

К какому классу моделей безопасности относится модель Take-Grant?

A) дискреционные модели безопасности

B) мандатные модели безопасности

C) ролевые модели безопасности

ANSWER: A

К какому классу моделей безопасности относится модель типизированной матрицы доступа?

A) дискреционные модели безопасности

B) мандатные модели безопасности

C) ролевые модели безопасности

ANSWER: A

К какому классу моделей безопасности относится модель Белла-ЛаПадулы?

A) дискреционные модели безопасности

B) мандатные модели безопасности

C) ролевые модели безопасности

ANSWER: B

К какому классу моделей безопасности относится модель безопасности переходов?

A) дискреционные модели безопасности

B) мандатные модели безопасности

C) ролевые модели безопасности

ANSWER: B

Сколько примитивных (элементарных) операций используется в классической модели ХРУ?

A) 4

B) 6

C) 5

D) 7

ANSWER: B

К какому классу операций относится операция Create классической модели ХРУ?

A) монотонная

B) немонотонная

ANSWER: A

Сколько основных множеств использует ролевая модель для описания системы?

A) 5

B) 4

C) 3

D) 7

ANSWER: B

В каком случае задача проверки безопасности системы ХРУ является разрешимой?

A) система команд не содержит элементарных операций «удалить» и «уничтожить»

B) команды являются монооперационными
C) команды системы являются одноусловными и монотонными
ANSWER: C

Сколько функций уровня безопасности используется в модели безопасности переходов?
A) 3
B) 2
C) 1
ANSWER: B

Состояние в модели Белла-ЛаПадулы называется безопасным по чтению, если
A) уровень безопасности субъекта не ниже уровня безопасности объекта
B) уровень безопасности объекта не ниже уровня безопасности субъекта
ANSWER: A

Система ХРУ называется монооперационной, если
A) система команд не содержит элементарных операций «удалить» и «уничтожить»
B) каждая команда системы содержит одну элементарную операцию
C) команды системы являются одноусловными
ANSWER: B

Удовлетворяет ли функция перехода Z-системы ограничениям основной теоремы безопасности Белла-ЛаПадулы?
A) да
B) нет
ANSWER: A

Ячейка матрицы доступа модели ХРУ является
A) строкой
B) множеством
C) числом
ANSWER: B

Какое дополнительное отношение на множестве ролей вводится в ролевой модели с иерархической организацией ролей?
A) отношение строгого порядка
B) отношение эквивалентности
C) отношение толерантности
D) отношение нестрогого порядка
ANSWER: D

Какое количество базовых представлений включают в себя модели безопасности?
A) 4
B) 6
C) 7
D) 5
ANSWER: B

Существует ли алгоритм проверки безопасности произвольной системы ХРУ?
A) да
B) нет
ANSWER: B

Приложение 10.1

Календарный график освоения элементов образовательной программы

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
УК-1						Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Б1.О.01Философия		Б2.О.03(Н) Производственная практика (научно-исследовательская работа)		Б2.О.04(Пд)Производственная практика (преддипломная)
УК-2								Б1.О.09Проектный менеджмент			

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
УК-3			Б1.В.ДВ.02.03Психолого-педагогическое сопровождение лиц с ограниченными возможностями здоровья		Б1.В.ДВ.01.03Правовые и организационные основы добровольческой (волонтерской) деятельности Б1.В.ДВ.01.04Основы конструктивного взаимодействия лиц с ограниченными возможностями здоровья в образовательном процессе	Б1.О.07Современные теории и технологии развития личности Б2.О.01(У) Учебная практика (экспериментально-исследовательская)					

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
УК-4	Б1.О.03Иностранный язык	Б1.О.03Иностранный язык	Б1.О.03Иностранный язык	Б1.О.03Иностранный язык							Б1.О.06Коммуникативные технологии профессионального общения
УК-5	Б1.О.12Основы российской государственности	Б1.О.02История России			Б1.В.ДВ.01.05Общественный проект "Обучение служением"						
УК-6						Б1.О.07Современные теории и технологии развития личности					Б2.О.04(Пд)Производственная практика (преддипломная)
УК-7	Б1.О.05Физическая культура и спорт	Б1.В.07.ДВ.01.01Легкая атлетика	Б1.В.07.ДВ.01.01Легкая атлетика	Б1.В.07.ДВ.01.01Легкая атлетика	Б1.В.07.ДВ.01.01Легкая атлетика	Б1.В.07.ДВ.01.01Легкая атлетика					
УК-8								Б1.О.04Безопасность жизнедеятельности			

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
УК-9							Б1.О.10Экономика и финансовая грамотность				
УК-10		Б1.О.08Правовые и организационные основы противодействия противоправному поведению									
ОПК-1	Б1.О.11Введение в специальность		Б1.О.39Основы информационной безопасности								

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-2	Б1.О.31Информатика Б1.О.36Введение в программирование	Б1.О.22Аппаратные средства вычислительной техники Б1.О.55Дисциплины специализации	Б1.О.35Объектно-ориентированное программирование Б1.О.37Методы программирования	Б1.О.37Методы программирования	Б1.О.32Операционные системы	Б2.О.01(У) Учебная практика (экспериментально-исследовательская) Б1.О.55Дисциплины специализации		Б1.О.50Инсталляция и настройка программного обеспечения ФТД.02Реляционные системы управления базами данных	Б1.О.55Дисциплины специализации		Б1.О.55Дисциплины специализации

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-3	Б1.О.19Геометрия Б1.О.31Информатика Б1.О.18Математический анализ	Б1.О.23Линейная алгебра Б1.О.18Математический анализ Б1.О.25Дискретная математика	Б1.О.26Дифференциальные уравнения Б1.О.25Дискретная математика Б1.О.20Теория вероятностей и математическая статистика	Б1.О.21Алгебра Б1.О.27Методы вычислений Б1.О.54Комплексный анализ Б1.О.53Уравнения математической физики Б1.О.20Теория вероятностей и математическая статистика	Б1.О.24Математическая логика и теория алгоритмов						
ОПК-4		Б1.О.13Механика и оптика Б1.О.22Аппаратные средства вычислительной техники	Б1.О.14Электричество и магнетизм		Б1.О.17Электроника и схемотехника	Б1.О.16Квантовая теория Б2.О.01(У) Учебная практика (экспериментально-исследовательская)	Б1.О.15Термодинамика	Б1.О.50Инсталляция и настройка программного обеспечения		Б1.О.52Теория радиотехнических систем	

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-5	Б1.О.11Введение в специальность		Б1.О.39Основы информационной безопасности	Б1.О.49Организационное и правовое обеспечение информационной безопасности	Б1.О.48Управление ресурсами в системах информационной безопасности	Б1.О.51Защита информации от утечки по техническим каналам		Б1.О.44Защита программ и данных		Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	
ОПК-6				Б1.О.49Организационное и правовое обеспечение информационной безопасности	Б1.О.48Управление ресурсами в системах информационной безопасности	Б1.О.51Защита информации от утечки по техническим каналам Б1.О.40Модели безопасности компьютерных систем				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-7	Б1.О.36Введение в программирование	Б1.О.55.05 Алгоритмы и структуры данных Б1.О.55Дисциплины специализации	Б1.О.35Объектно-ориентированное программирование Б1.О.37Методы программирования	Б1.О.37Методы программирования	Б1.О.28Методы оптимизации	Б1.О.55Дисциплины специализации		Б1.О.443ащита программ и данных	Б2.О.03(Н) Производственная практика (научно-исследовательская работа) Б1.О.55Дисциплины специализации		Б1.О.55Дисциплины специализации Б1.О.55.04 Интеллектуальные системы обработки информации
ОПК-8						Б1.О.40Модели безопасности компьютерных систем	Б1.О.30Технологии обработки информации	Б1.О.42Основы построения защищенных компьютерных сетей	Б1.О.47Теоретико-числовые методы в криптографии Б2.О.03(Н) Производственная практика (научно-исследовательская работа)		

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-9						Б1.О.51Защита информации от утечки по техническим каналам Б1.О.33Сети и системы передачи информации Б1.О.41Защита в операционных системах		Б1.О.42Основы построения защищенных компьютерных сетей Б1.О.43Основы построения защищенных баз данных	Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности Б1.О.52Теория радиотехнических систем	Б2.О.04(Пд)Производственная практика (преддипломная)

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-10	Б1.О.31Информатика				Б1.О.29Теория информации		Б1.О.45Методы и средства криптографической защиты информации		Б1.О.47Теоретико-числовые методы в криптографии	Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности Б1.О.46Криптографические протоколы Б1.О.52Теория радиотехнических систем	

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-1.1						Б1.О.55.03 Методы и стандарты оценки защищенности компьютерных систем				Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	
ОПК-11						Б1.О.40Модели безопасности компьютерных систем Б1.О.413ащита в операционных системах		Б1.О.42Основы построения защищенных компьютерных сетей		Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-1.2										Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Б1.О.55.02 Алгоритмы кодирования и сжатия информации
ОПК-12					Б1.О.32Операционные системы	Б1.О.413Защита в операционных системах		Б1.О.50Инсталляция и настройка программного обеспечения		Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-1.3									Б1.О.55.01 Методы верификации	Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	
ОПК-13	Б1.О.36Введение в программирование	Б1.О.55.05 Алгоритмы и структуры данных	Б1.О.35Объектно-ориентированное программирование Б1.О.37Методы программирования	Б1.О.37Методы программирования		Б1.О.413ащита в операционных системах		Б1.О.443ащита программи данных	Б2.О.03(Н) Производственная практика (научно-исследовательская работа)	Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	Б2.О.04(Пд)Производственная практика (преддипломная)

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-14							Б1.О.38Системы управления базами данных	Б1.О.43Основы построения защищенных баз данных		Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	
ОПК-15		Б1.О.22Аппаратные средства вычислительной техники					Б1.О.34Компьютерные сети	Б1.О.42Основы построения защищенных компьютерных сетей Б1.О.50Инсталляция и настройка программного обеспечения		Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ОПК-16								Б1.О.42Основы построения защищенных компьютерных сетей Б1.О.50Инсталляция и настройка программного обеспечения Б1.О.44Защита программ и данных		Б1.О.52Теория радиотехнических систем Б2.О.06(П) Производственная практика по получению профессиональных умений и навыков в области профессиональной деятельности	
ОПК-17		Б1.О.02История России									

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ПК-1			Б1.В.ДВ.02.01Языки программирования Б1.В.ДВ.02.02Алгоритмы машинной графики		Б1.В.ДВ.01.01Язык программирования Java Б1.В.ДВ.01.02Язык программирования C# Б1.В.ДВ.05.01Разработка приложений на C++ Б1.В.ДВ.05.02Обработка изображений	Б1.В.01Стеганография и цифровые водяные знаки	Б1.В.02Моделирование систем	Б1.В.03Технологии защищенного документооборота и блокчейн	Б1.В.ДВ.03.02Язык HTML Б1.В.ДВ.03.01Биометрические методы идентификации личности	Б1.В.ДВ.04.01Параллельные алгоритмы обработки данных Б1.В.ДВ.04.02Технологии интернет вещей	Б2.В.01(П) Производственная практика (технологическая)
ПК-2							Б1.В.02Моделирование систем			Б1.В.04Методология экспериментальных исследований и испытаний	Б2.В.01(П) Производственная практика (технологическая)

	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	А семестр	В семестр
ПК-3						Б1.В.01Стеганография и цифровые водяные знаки		Б1.В.03Технологии защищенного документооборота и блокчейн	ФТД.01Защита персональных данных	Б1.В.05Анализ уязвимостей программного обеспечения	Б2.В.01(П) Производственная практика (технологическая)

Приложение 10.2

Календарный график формирования компетенций

Компетенции	1 курс		2 курс		3 курс		4 курс		5 курс		6 курс
	1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр	9 семестр	10 семестр	11 семестр
Универсальные	УК-4 УК-5 УК-7	УК-4 УК-5 УК-7 УК-10	УК-3 УК-4 УК-7	УК-4 УК-7	УК-3 УК-5 УК-7	УК-1 УК-3 УК-6 УК-7	УК-1 УК-9	УК-2 УК-8	УК-1		УК-1 УК-4 УК-6
Общепрофессиональные	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ОПК-7 ОПК-10 ОПК-13	ОПК-2 ОПК-3 ОПК-4 ОПК-7 ОПК-13 ОПК-15 ОПК-17	ОПК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-7 ОПК-13	ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-13	ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-6 ОПК-7 ОПК-10 ОПК-12	ОПК-2 ОПК-4 ОПК-5 ОПК-6 ОПК-8 ОПК-9 ОПК-11 ОПК-12 ОПК-13 ОПК-1.1	ОПК-4 ОПК-8 ОПК-10 ОПК-12 ОПК-14 ОПК-15	ОПК-2 ОПК-4 ОПК-5 ОПК-7 ОПК-8 ОПК-9 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-15 ОПК-16	ОПК-7 ОПК-8 ОПК-9 ОПК-10 ОПК-13 ОПК-1.3	ОПК-4 ОПК-5 ОПК-6 ОПК-9 ОПК-10 ОПК-11 ОПК-12 ОПК-13 ОПК-14 ОПК-15 ОПК-16 ОПК-1.1 ОПК-1.2 ОПК-1.3	ОПК-7 ОПК-9 ОПК-13 ОПК-1.2
Профессиональные			ПК-1		ПК-1	ПК-1 ПК-3	ПК-1 ПК-2	ПК-1 ПК-3	ПК-1 ПК-3	ПК-1 ПК-2 ПК-3	ПК-1 ПК-2 ПК-3