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

УТВЕРЖДАЮ

декан факультета прикладной
математики, информатики
и механики
С.Н. Медведев
26.05.2023

ПРОГРАММА ПРАКТИКИ
Б2.О.06(П) Производственная практика (проектно-эксплуатационная)

Код и наименование(тип) практики/НИР в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

математические методы защиты информации

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию практики: Кибербезопасности информационных систем

6. Составители программы: Сафонов Виталий Владимирович, к.т.н., доцент

(ФИО, ученая степень, ученое звание)

7. Рекомендована: Научно-методическим советом факультета прикладной математики, информатики и механики 26.05.2023 г., протокол №9

(наименование рекомендующей структуры, дата, номер протокола,

_____

отметки о продлении вносятся вручную)

---

8. Учебный год: 2027/2028 **Семестр(ы):** A

9.**Цель практики:**

– 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 организации с целью приобретения социально-личностных и профессиональных компетенций;

– приобретение студентами профессиональных навыков, практического опыта, закрепление, систематизация и расширение теоретических знаний по использованию, администрированию, настройке и наладке средств обеспечения информационной безопасности, используемых в организации.

Задачи практики:

Формирование у студентов умений и навыков:

– проведения технического обследования объекта анализа;

– сбор экспериментального и экспертного материала и его теоретического обобщения;

– настройка, эксплуатация и обеспечение работоспособности компонентов систем обеспечения информационной безопасности;

– обучение студентов методикам применения устройств и программного обеспечения информационных систем для решения задач обеспечения информационной безопасности;

– изучение организации IT служб предприятия; изучение системы аттестации и контроля инфраструктуры предприятия и её отдельных элементов на соответствии требованиям информационной безопасности;

– изучение состава аппаратного и программного обеспечения средств вычислительной техники предприятия.

10. Место практики в структуре ООП: обязательная часть блока Б2.

Цикл (раздел) ООП: Б2		код дисциплины в УП: Б2.Б.06(П)
№	**Код**	**Наименование**
Для успешного прохождения учебной практики обучающиеся используют знания, умения, сформированные в ходе изучения дисциплин		
1	Б1.О.29	Теория информации
2	Б1.О.32	Операционные системы
3	Б1.О.34	Компьютерные сети
4	Б1.О.36	Введение в программирование
5	Б1.О.37	Методы программирования
6	Б1.О.38	Системы управления базами данных
7	Б1.О.39	Основы информационной безопасности
8	Б1.О.40	Модели безопасности компьютерных систем
9	Б1.О.41	Защита в операционных системах
10	Б1.О.42	Основы построения защищенных компьютерных сетей
11	Б1.О.43	Основы построения защищенных баз данных
12	Б1.О.44	Защита программ и данных
13	Б1.О.45	Методы и средства криптографической защиты информации
14	Б1.О.46	Криптографические протоколы
15	Б1.О.47	Теоретико-числовые методы в криптографии
16	Б1.О.49	Организационное и правовое обеспечение информационной безопасности
17	Б1.О.50	Инсталляция и настройка программного обеспечения
18	Б1.О.51	Защита информации от утечки по техническим каналам
19	Б1.О.52	Теория радиотехнических систем
20	Б1.О.56.01	Методы алгебраической геометрии в криптографии
21	Б1.О.56.03	Программная реализация криптоалгоритмов
22	Б1.О.56.04	Современные технологии защиты информации
23	Б1.О.56.05	Современные проблемы информационной безопасности
24	Б1.О.56.06	Методы разработки и анализа математических моделей

25	Б2.О.03(Н)	Производственная практика (научно-исследовательская работа)
26	ФТД.01	Методы повышения скрытности передачи информации в системах связи
Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее		
27	Б2.О.04(Пд)	Производственная практика (преддипломная)
28	Б3.01(Д)	Подготовка к процедуре защиты и защита выпускной квалификационной работы

11. Вид практики, способ и форма ее проведения

Вид практики: *производственная*.
Способ проведения практики: *стационарная*.
Форма проведения практики: *дискретная*.
Реализуется частично в форме практической подготовки (ПП).

Производственная практика проводится в структурных подразделениях университета и в организациях на основе договоров, заключаемых между Университетом и организациями, деятельность которых соответствует направленности реализуемой образовательной программы по соответствующему профилю.

12. Планируемые результаты обучения при прохождении практики (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
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	Уметь: – классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; – обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав; – формулировать основные требования информационной безопасности при эксплуатации компьютерной системы; – анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам. Владеть: – методами и средствами технической защиты информации.
		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-5.12	умеет формулировать основные требования информационной безопасности при эксплуатации компьютерной системы;	
		ОПК-5.17	умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам	
		ОПК-5.19	владеет методами и средствами технической защиты информации	
ОПК-6.	*Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных*	ОПК-6.6	умеет разрабатывать модели угроз и модели нарушителя компьютерных систем;	Уметь: – разрабатывать модели угроз и модели нарушителя компьютерных систем; – применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценивания защищенности компьютерной системы.
		ОПК-6.10	умеет применять отечественные и зарубежные стандарты в области компьютерной	

	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		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-9.4	умеет пользоваться нормативными документами в области технической защиты информации	Уметь: – пользоваться нормативными документами в области технической защиты информации; – формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем.
		ОПК-9.9	умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем;	
ОПК-10.	*Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности*	ОПК-10.9	умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач	Уметь: – разворачивать инфраструктуру открытых ключей для решения криптографических задач; – разворачивать инфраструктуру открытых ключей для решения криптографических задач; – вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность); Владеть: – основами построения математических моделей текстовой информации и моделей систем передачи информации.
		ОПК-10.20	умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач	
		ОПК-10.25	умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность);	
		ОПК-10.27	владеет основами построения математических моделей текстовой информации и моделей систем передачи информации;	
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	Уметь: – формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на базе основных операционных систем.
ОПК-12.	*Способен*	ОПК-12.5	Умеет осуществлять	Уметь:

	администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения		администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отечественного производства.	– осуществлять администрирование программного обеспечения специального назначения, включая операционные системы, в том числе отечественного производства; – восстанавливать работоспособность 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 безопасности*	ОПК-13.2	владеет навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств	Уметь: – работать с интегрированными средами разработки программного обеспечения; – применять средства и методы анализа программного обеспечения для выявления закладок; – применять методы анализа проектных решений для обеспечения защищенности компьютерных систем; – применять современные средства обеспечения информационной безопасности программ и данных; – проводить анализ программных средств, применяемых для контроля и защиты информации. Владеть: – навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств; – навыками разработки, отладки, документирования и тестирования программ; – навыками разработки алгоритмов для решения типовых профессиональных задач.
		ОПК-13.5	умеет работать с интегрированными средами разработки программного обеспечения;	
		ОПК-13.6	владеет навыками разработки, отладки, документирования и тестирования программ;	
		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-13.21	Уметь применять современные средства обеспечения информационной безопасности программ и данных	
		ОПК-13.23	Умеет проводить анализ программных средств, применяемых для контроля и защиты информации	
ОПК-14.	*Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации*	ОПК-14.5	умеет настраивать и применять современные системы управления базами данных	Уметь: – настраивать и применять современные системы управления базами данных. Владеть: – методикой и навыками составления запросов для поиска информации в базах 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-15.6	умеет осуществлять проектирование и оптимизацию функционирования компьютерных сетей;	Уметь: – осуществлять проектирование и оптимизацию функционирования компьютерных сетей. Владеть: – навыками администрирования компьютерных
		ОПК-15.7	владеет навыками	

			администрирования компьютерных сетей;	сетей.
ОПК-16.	*Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях*	ОПК-16.6	умеет формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе;	Уметь: – формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе; – применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; – осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; – выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций. Владеть: – навыками настройки межсетевых экранов; – методиками анализа сетевого трафика.
		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-16.16	Умеет выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	
ОПК-2.1.	*Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации*	ОПК-2.1.5	Способен разрабатывать программные алгоритмы с применением математических моделей для оценки безопасности компьютерных систем	Знать: – математические модели для оценки безопасности компьютерных систем. Уметь: – разрабатывать программные алгоритмы с применением математических моделей для оценки безопасности компьютерных систем. Владеть: инструментальными средствами разработки программных алгоритмов с применением математических моделей для оценки безопасности компьютерных систем.
ОПК-2.2.	*Способен разрабатывать и анализировать математические модели механизмов защиты информации*	ОПК-2.2.1	Применяет основные инструменты моделирования защищенных автоматизированных систем с целью анализа их уязвимостей	Знать: – инструменты моделирования защищенных автоматизированных систем; – средства и методы анализа компонентов системы безопасности с использованием современных математических методов; – математические модели для оценки безопасности компьютерных систем. Уметь: – применять основные инструменты моделирования защищенных автоматизированных систем с целью анализа их уязвимостей; – применять средства и методы анализа компонентов системы безопасности с использованием современных математических методов; – разрабатывать математические модели для оценки безопасности компьютерных систем. Владеть: – инструментами моделирования защищенных автоматизированных систем с целью анализа их уязвимостей; – средствами и методами анализа компонентов системы безопасности с использованием современных математических методов;
		ОПК-2.2.5	Применяет средства и методы анализа компонентов системы безопасности с использованием современных математических методов	
		ОПК-2.2.6	Разрабатывает математические модели для оценки безопасности компьютерных систем	

				средствами разработки математических моделей для оценки безопасности компьютерных систем.
ОПК-2.3.	*Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов*	ОПК-2.3.2	Применяет основные методы инструментального анализа средств защиты информации	Знать: – основные методы инструментального анализа средств защиты информации; – методики оценки эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации; – требования к защите информации в автоматизированной системе. Уметь: – применять основные методы инструментального анализа средств защиты информации; – проводить оценку эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации; – формировать обоснование необходимости защиты информации в автоматизированной системе. Владеть: – методами инструментального анализа средств защиты информации; – средствами проведения оценки эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации; методиками формирования обоснования необходимости защиты информации в автоматизированной системе.
		ОПК-2.3.3	Проводит оценку эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации	
		ОПК-2.3.4	Формирует обоснование необходимости защиты информации в автоматизированной системе	
ПК-1	*Способен проводить анализ требований и выполнять работы по проектированию программного обеспечения с применением математических методов защиты*	ПК-1.3	Применяет технологии обработки данных, анализирует возможности их использования при разработке программного обеспечения в профессиональной деятельности	Уметь: – применять технологии обработки данных, и анализировать возможности их использования при разработке программного обеспечения в профессиональной деятельности.
ПК-3	*Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач*	ПК-3.4	Разрабатывает программные алгоритмы, реализующие современные математические методы защиты информации	Уметь: – разрабатывать программные алгоритмы, реализующие современные математические методы защиты информации; – проводить анализ защищенности программных и программно-аппаратных средств защиты информации. Владеть: – методами анализа защищенности программных и программно-аппаратных средств защиты информации
		ПК-3.5	Выполняет анализ защищенности программных и программно-аппаратных средств защиты информации	

13. Объем практики в зачетных единицах / ак. час. (*в соответствии с учебным планом)* **—** 6/216.

Форма промежуточной аттестации *зачет с оценкой*.

14. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		А		
		ч.	ч., в форме ПП	
Всего часов	216	216	162	
в том числе:				
Контактная работа (включая НИС)	4	4	3	
Самостоятельная работа	212	212	159	
Итого:	216	216	160	

15. Содержание практики (или НИР)

п/п	Разделы (этапы) практики	Виды учебной работы	Объем учебной работы, ч	
			Контактные часы	Самостоятельная работа
1.	*Организационно-подготовительный этап*	проведение собрания по организации практики; установочный инструктаж по задачам, срокам и требуемой отчетности; инструктаж по технике безопасности работы; формулировка задач для решения в ходе практики и составление плана работ; подготовка документов, подтверждающих факт направления на практику; получение задания от руководителя практики; производственный инструктаж; ознакомление студентов с организационной структурой профильной организации, применяемой аппаратурой и программным обеспечением, нормативными актами и инструкциями.	1	12
2.	*Проектно-эксплуатационный этап*	изучение нормативных документов по защите информации и методиками проверки защищенности объекта информатизации; ознакомление с принципами формирования политики информационной безопасности в корпоративной инфраструктуре; оценка рисков безопасности информационной системы; ознакомление с политикой информационной безопасности действующей в корпоративной инфраструктуре; ознакомление с применяемыми средствами, методами и технологиями обеспечения защищенности корпоративной инфраструктуры и обеспечения информационной безопасности; разработать предложения по совершенствованию системы информационной безопасности.	2	100
3.	*Оформление отчёта по итогам практики*	описание проделанной работы с самооценкой результатов прохождения практики; формулирование выводов и предложений по организации практики.	1	100

Содержание практической подготовки при проведении практики устанавливается исходя из содержания и направленности образовательной программы, содержания практики, ее целей и задач. Практическая подготовка при проведении практики направлена на формирование умений и навыков в соответствии с трудовыми действиями и (или) трудовыми функциями по профилю образовательной программы.

Практическая подготовка проводится путем непосредственного выполнения обучающимися определенных видов работ, связанных с будущей профессиональной деятельностью, способствующих формированию, закреплению и развитию практических навыков и компетенций по профилю соответствующей образовательной программы.

№ п/п	Типы задач профессиональной деятельности	Формируемые профессиональные компетенции	Формируемые общепрофессиональные компетенции специализации
1	*Научно-исследовательский*	*ПК-1.3 Применяет технологии обработки данных, анализирует возможности их использования при разработке программного обеспечения в профессиональной деятельности*	
2	*Проектный*	*ПК-3.5 Выполняет анализ защищенности программных и программно-аппаратных средств защиты информации*	*ОПК-2.3.3 Проводит оценку эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации*
3	*Контрольно-аналитический*		*ОПК-2.2.5 Применяет средства и методы анализа компонентов системы безопасности с использованием современных математических методов*
4	*Организационно-управленческий*		*ОПК-2.3.4 Формирует обоснование необходимости защиты информации в автоматизированной системе*
5	*Эксплуатационный*	*ПК-3.4 Разрабатывает программные алгоритмы, реализующие современные математические методы защиты информации.*	*ОПК-2.1.5 Способен разрабатывать программные алгоритмы с применением математических моделей для оценки безопасности компьютерных систем* *ОПК-2.2.1 Применяет основные инструменты моделирования защищенных автоматизированных систем с целью анализа их уязвимостей* *ОПК-2.2.6 Разрабатывает математические модели для оценки безопасности компьютерных систем* *ОПК-2.3.2 Применяет основные методы инструментального анализа средств защиты информации*

16. Перечень учебной литературы, ресурсов сети «Интернет», необходимых для прохождения практики *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1.	Шкляр, М.Ф. Основы научных исследований / М.Ф. Шкляр. — Москва: Дашков и Ко, 2012. — 244 с. URL:http://biblioclub.ru/index.php?page=book&id=112247.
2.	Новиков А.М., Новиков Д.А. Методология научного исследования. – М.: Либроком. 2010 – 280 с. URL:http://www.methodolog.ru/books/mni.pdf.
3.	Мельников В. П., Клейменов С. А., Петраков А. М. Информационная безопасность и защита информации. - М.: Академия, 2007. – 330 с.
4.	Основы управления информационной безопасностью: [учебное пособие для студентов вузов, обучающихся по направлениям подготовки (специальностям) укрупненной группы специальностей 090000 - "Информ. безопасность"] / А.П. Курило [и др.]. — 2-е изд., испр. — Москва: Горячая линия-Телеком, 2014. — 243 с. : ил., табл. — (Вопросы управления информационной безопасностью ; Кн.1) .— Библиогр.: с.234-239 .— ISBN 978-5-9912-0361-6.
5.	Краковский, Ю.М. Информационная безопасность и защита информации: учебное пособие для студ. обуч. по специальности «Информационные системы и технологии» днев. и заоч. форм обучения / Ю.М. Краковский. — М.; Ростов н/Д: МарТ, 2008. — 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
6.	Олейник П. П. Корпоративные информационные системы: для бакалавров и специалистов: учебник для студ. вузов, обуч. по направл. 080800 "Прикладная информатика (по областям)" и др. экон. спец. – СПб.: Питер, 2012. – 176 с.

7.	Фостер, Джеймс. Защита от взлома: сокеты, эксплойты, shell-код/ Дж. Фостер, М. Прайс; пер. с англ. А. А. Слинкина. — Москва: ДМК Пресс, 2008. — 784 с.: ил. — (Информационная безопасность). — ISBN 5-9706-0019-9: 449.10 р. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1117>.
8.	Скудис, Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите/ Э. Скудис. — Москва: ДМК Пресс, 2009. — 512 с. — (Защита и администрирование). — ISBN 5-94074-170-3: 176-00. — URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1112.
9.	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения: учебное пособие для вузов / В.А. Голуб; Воронеж. гос. ун-т.— Воронеж: ЛОП ВГУ, 2006. — 31 с. — Библиогр.: с.30 .— URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf.
10.	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок/ М. Ховард, Д. Лебланк, Дж. Виега; авт. предисл. А. Йоран. — Москва: ДМК Пресс, 2009. — 287 с. — Загл. и авт. ориг.: 19 deadly sins of software security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X. — <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
11.	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors: Обнаружение и защита / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. - 304 с.
12.	Проскурин В. Г. Защита программ и данных - М.: Академия, 2011. – 198 с.
13.	Управление внедрением информационных систем: курс лекций: учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. технологий / В.И. Грекул, Г. Н. Денищенко, Н.Л. Коровкина. – М.: Интернет-Ун-т информ. технологий, 2008. [Электронный ресурс] URL: http://www.intuit.ru/studies/courses/2196/267/info/.
14.	Юрин И.Ю. Теоретические и практические основы защиты информации. 2012. http://library.sgu.ru/uch_lit/620.pdf.
15.	Астанин, И.К. Защита информации: учебное пособие для вузов / И.К. Астанин, Н.И. Астанин; Воронеж. гос. ун-т, Лискинский филиал. — Воронеж: Воронеж. гос. ун-т, 2006. — Библиогр. : с.169 .— ISBN 5-9273-1080-x.
16.	Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства/ Шаньгин В. Ф. — Москва: ДМК Пресс, 2010. — 544 с.: ил., табл.; 24 см.— (Администрирование и защита). — Допущено Учебно-методическим объединением вузов по университетскому политехническому образованию в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению 230100 «Информатика и вычислительная техника». — ISBN 978-5-94074-518-1. — URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1122.
17.	Ищейнов В.Я. Защита конфиденциальной информации: [учебное пособие для студ. вузов, обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. — ISBN 978-5-91134-336-1.

б) дополнительная литература:

№ п/п	Источник
18.	Муромцева А. В. Искусство презентации. Основные правила и практические рекомендации / А.В. Муромцева. — Москва: Флинта: Наука, 2014. — 108 с.
19.	Кручинин, В.В. Компьютерные технологии в научных исследованиях: учебно-методическое пособие / В.В. Кручинин. – Москва: ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2012. — 57 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=11269.
20.	Андреев, Г.И. Основы научной работы и методология диссертационного исследования / Г.И. Андреев, В.В. Барвиненко, В.С. Верба. — Москва: Финансы и статистика, 2012. — 296 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=28348.
21.	Системы и средства информатики: Ежегодник / Гл. ред. И.А. Соколов. — Москва: ИПИ РАН. – 2010.– Вып. 20. – № 2. — 350 с.
22.	Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации, 31.07.2006, № 31 (1 ч.), ст. 3448.
23.	Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации, 31 июля 2006 года № 31 (1 ч.), ст. 3451.
24.	ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. (утверждён и введён в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 375-ст).

25.	Приказ Федеральной службы по техническому и экспортному контролю России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета, № 136, 26.06.2013.
26.	Приказ Федеральной службы по техническому и экспортному контролю России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета, № 107, 22.05.2013.
27.	Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).
28.	Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации, 05.11.2012, № 45, ст. 6257.
29.	Мещеряков В.А., Железняк В.П., Бондарь А.О., Осипенко А.Л., Бабкин А.Н. Персональные данные: организация обработки и обеспечения безопасности в органах государственной власти и местного самоуправления / Под ред. В.А. Мещерякова. – Воронеж: Воронежский институт МВД России, 2014. – 186 с.
30.	Постановление правительства Воронежской области от 28 апреля 2011 года № 340 «Об утверждении положения о едином реестре государственных информационных систем Воронежской области» // Собрание законодательства Воронежской области 20.06.2011 № 4, ст. 285.
31.	Ермошкин Н.Н., Тарасов А.А. Стратегия информационных технологий предприятия. М.: Изд-во Московского гуманитарного университета, 2003.
32.	Корнеев И.К., Степанов Е.А. Защита информации в офисе. – "Издательство Проспект", 2008. – 333 с.
33.	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html.
34.	Таненбаум Э. Компьютерные сети / Э. Таненбаум. – СПб.: Питер, 2005. — 991 с.
35.	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века: матер. XII международ. науч.-тех. конф. Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.
36.	Партыка Т.Л. Информационная безопасность М.: ФОРУМ, 2007
37.	Мельников, Владимир Павлович. Информационная безопасность и защита информации: учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. — М.: ACADEMIA, 2006. — 330 с.— (Высшее профессиональное образование. Информатика и вычислительная техника). — ISBN 5-7695-2592-4.
38.	Андрианов В.И."Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие / В.А.Бородин, А.В.Соколов. – С-Пб.: Лань, 1996.
39.	Абалмазов Э.И. Методы и инженерно – технические средства противодействия информационным угрозам / Э.И.Абалмазов. – М.: Гротек, 1997.
40.	Василевский И.В. Способы и средства предотвращения утечки информации по техническим каналам / И.В.Василевский. – М.: НПЦ "Нелк", 1998.
41.	Хорев А.А., Способы и средства ЗИ / А.А.Хорев. – МО РФ, 1998.
42.	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», принят и введен в действие Постановлением Госстандарта России от 4 апреля 2002 г. № 133-ст.
43.	ИСО/МЭК 31000:2009 «Управление рисками. Принципы и направления», ISO Technical Management Board Working Group, 2009.
44.	ИСО/МЭК 31100:2009 «Управление рисками. Методики оценки риска», ISO Technical Management Board Working Group, 2009.
45.	ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2010 г. № 632-ст.
46.	Мельников, Владимир Павлович. Информационная безопасность и защита информации: учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. — М.: ACADEMIA, 2006. — 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника). — ISBN 5-7695-2592-4.

47.	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб.: БХВ-Петербург, 2006. - 464 с.
48.	Гончаров, Игорь Васильевич. Информационная безопасность. Словарь по терминологии / И.В. Гончаров, Ю.Г. Кирсанов, О.В. Райков. — Воронеж : Воронежская областная типография, 2015 .— 180 с. — Тираж 300. 11,3 п.л. — ISBN 9785442003246.
49.	Брусницин Н.А. Открытость и шпионаж / Н.А.Брусницин. – М.: Воениздат, 1991.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1.	ЭБС Лань
2.	ЭБС «Университетская библиотека online»
3.	ЭБС «Электронная библиотека технического ВУЗа» (ЭБС «Консультант студента»)
4.	ЭБС ЮРАЙТ
5.	Электронная библиотека учебно-методических материалов ВГУ. Режим доступа: http://www.lib.vsu.ru
6.	http://www.cryptopro.ru
7.	http://www.infotecs.ru
8.	http://www.lissi-crypto.ru/
9.	http://www.signal-com.ru
10.	http://www.shipka.ru

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы и т.д.

17. Образовательные технологии, применяемые при проведении практики и методические указания для обучающихся по прохождению практики

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. Представленный отчет по практике оценивается на соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Структура отчета по практике

1. Отчет по практике должен включать титульный лист, содержание, введение, описание теоретических и практических аспектов выполненной работы, заключение, список использованных источников, приложения.

2. На титульном листе должна быть представлена тема практики, группа и фамилия студента, данные о предприятии, на базе которого выполнялась практика, фамилия руководителя.

3. Во введении студенты должны дать краткое описание задачи, решаемой в рамках практики.

4. В основной части отчета студенты приводят подробное описание проделанной теоретической и (или) практической работы, включая описание и обоснование выбранных решений, описание программ и т.д.

5. В заключении дается краткая характеристика проделанной работы, и приводятся ее основные результаты.

6. В приложениях приводятся непосредственные результаты разработки: тексты программ, графики и диаграммы, и т.д.

Требования к оформлению отчета

1. Отчет оформляется в печатном виде, на листах формата А4.

2. Основной текст отчета выполняется шрифтом 14 пунктов, с интервалом 1,5 между строками. Текст разбивается на абзацы, каждый из которых включает отступ и выравнивание по ширине.

3. Текст в приложениях может быть выполнен более мелким шрифтом.

4. Отчет разбивается на главы, пункты и подпункты, включающие десятичную нумерацию.

5. Рисунки и таблицы в отчете должны иметь отдельную нумерацию и названия.

6. Весь отчет должен быть оформлен в едином стиле: везде в отчете для заголовков одного уровня, основного текста и подписей должен использоваться одинаковый шрифт.

7.Страницы отчета нумеруются, начиная с титульного листа. Номера страниц проставляются в правом верхнем углу для всего отчета кроме титульного листа.

8. Содержание отчета должно включать перечень всех глав, пунктов и подпунктов, с указанием номера страницы для каждого элемента содержания.

9. Ссылки на литературу и другие использованные источники оформляются в основном тексте, а сами источники перечисляются в списке использованных источников.

10. Объем отчета по практике должен быть не менее 20 страниц.

18. Материально-техническое обеспечение практики:

г. Воронеж, ул. Университетская площадь, д.1, главный учебный корпус, ауд.226

Моноблок HP: процессор Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz, оперативная память 8Гб, SSD 250Гб. Мультимедиапроектор Epson. Аудио колонки EV (2 шт.). Микрофон. Экран для проектора. Маркерные панели Askell (2 шт.).

394018, г. Воронеж, Средне-Московская ул., д. 6 а, помещ. V, ООО "Техномаркет"

В соответствии с договором №1124 от 18.06.2019 о практической подготовке обучающихся.

394018, г. Воронеж, площадь Ленина, 1, Правительство Воронежской области

В соответствии с договором №1162 от 19.06.2019 о практической подготовке обучающихся.

394006, г. Воронеж пл. Ленина, д.11, Управление записи актов гражданского состояния Воронежской области (управление ЗАГС Воронежской области)

В соответствии с договором №1412 от 05.07.2019 о практической подготовке обучающихся.

394006, г. Воронеж ул. Ворошилова, 14, Департамент социальной защиты Воронежской области (ДСЗ ВО)

В соответствии с договором №1413 от 05.07.2019 о практической подготовке обучающихся.

394006 г. Воронеж, ул. Красноармейская д. 52д, Департамент здравоохранения Воронежской области

В соответствии с договором №1414 от 05.07.2019 о практической подготовке обучающихся.

394036, г. Воронеж, улица К.Маркса, 70, Департамент финансов Воронежской области

В соответствии с договором №1431 от 19.07.2019 о практической подготовке обучающихся.

394036, г. Воронеж, ООО "Философия.ИТ"

В соответствии с договором №427 от 20.05.2019 о практической подготовке обучающихся.

394036, г. Воронеж, ООО "Р.Т Решение"

В соответствии с договором № 684 от 07.05.2019 о практической подготовке обучающихся.

394006, Воронеж, ул. Красноармейская, д.52Д, БЦ «Галеон», 3 этаж, офис 209, ООО "ЭйТи Консалтинг"

В соответствии с договором №685 от 07.05.2019 о практической подготовке обучающихся.

г. Воронеж, ул. Университетская площадь, д.1, учебный корпус 1б, ауд.407

Компьютер в составе: процессор Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz, оперативная память 16 Гб, SSD 256 Гб, HDD 1Тб, видеокарта NVIDIA GeForce GTX 1080 Ti; монитор DELL S2419HN. Компьютер в составе (1 шт.): процессор Intel(R) Core(TM) i7-7800X CPU @ 3.50GHz, оперативная память 96 Гб, SSD 1Тб, HDD 4Тб, видеокарта NVIDIA GeForce RTX 2080 Ti (2 шт.); монитор DELL S2419HN. Источник бесперебойного питания APC Back-UPS BV1000I-GR, line-interactive, мощность:1000ВА,

600Вт (16 шт.). Источник бесперебойного питания Legrand KEOR LINE RT 1500BA (1 шт.). Коммутатор HP 2530-24G Switch (Managed, 24*10/100/1000 + 4 SFP, 19"). Интерактивная доска SMART SBM685 (87 дюймов, ПО SMART SLS) с пассивным лотком. Проектор Vivitek DH758UST (ультракороткофокусный, DLP, Full HD 1080p (1920 x 1080) , 3500 ANS, 10000:1, полная поддержка 3D).

г. Воронеж, ул. Университетская площадь, д.1, главный учебный корпус, ауд.214

Компьютер в составе: системный блок: процессор Intel(R) Core(TM) i5, оперативная память 8Гб, HDD 500Гб; монитор: LG FLATRON. Мультимедиапроектор BenQ. Экран настенный для проектора. Аудио колонки Creative A60. Коммутатор.

г. Воронеж, ул. Университетская площадь, д.1, главный учебный корпус, ауд.216

Компьютер в составе: процессор Intel Core i3, оперативная память 8Гб, HDD 500Гб, видеокарта NVIDIA GeForce; монитор: Acer. Компьютер в составе (1 шт.): процессор Intel(R) Core(TM) i5, оперативная память 8Гб, HDD 500Гб; монитор: Acer. Экран настенный для проектора. Мультимедиапроектор BenQ. Источник бесперебойного питания Back-UPS 650. Коммутатор Cisco Catalyst 3750 Series.

г. Воронеж, ул. Университетская площадь, д.1, главный учебный корпус, ауд.124

Компьютер в составе: системный блок: процессор AMD Ryzen 7 3800X 8-Core Processor, оперативная память 32Гб, HDD 1Тб, SSD 256Гб, видеокарта NVIDIA GeForce GTX 1050; монитор: Dell S2419H. Интерактивная доска SMART SBM685 (87 дюймов). Мультимедиапроектор Vivitek ультракороткофокусный. Источник бесперебойного питания Legrand Keor SPX 1000 BA IEC C13 (16 шт.). Источник бесперебойного питания Legrand Keor Line RT 1000 BA (1 шт.). Коммутатор HP 2530-48G Switch (1 шт.).

г. Воронеж, ул. Университетская площадь, д.1, учебный корпус 1, ауд.2/25

Учебный стенд "Программные средства криптографии", SCRYPTO в составе: каркас моноблока (1 шт.); интегрированный вычислительный узел 3 шт.) в составе: процессор Intel: два ядра с тактовой частотой 2700 МГц, ОЗУ: объём 4 Гб тип DDR-3, твердотельный накопитель SSD объемом 60 Гб, блок питания мощностью 300 Вт, 2 сетевых интерфейса GigabitEthernet; переключатель KBM-типа D-Link (1 шт.); неуправляемый коммутатор D-Link (1 шт.); модуль питания, контроля и интеграции стенда в общую лабораторию (1 шт.); монитор Philips(1 шт.); комплект консоли рабочего места обучаемого (1 шт.) в составе: клавиатура Oklick, мышь Oklick; комплект учебно-методических пособий (1 к-т.); статистическое программное обеспечение управления модулем питания (1 шт.); флэш-диск восстановления ОС на интегрированных ПК (3 шт.) с операционной системой ArchLinux; флэш-диск мультимедийного методического пособия (1 шт.); группа коммутационных портов (2 шт.).

Типовой комплект учебного оборудования "Сетевая безопасность", SECURITY в составе: управляемый коммутатор третьего уровня D-Link (1 шт.); управляемый коммутатор второго уровня D-Link (1 шт.); аппаратно-программный эмулятор устройства локальной сети (1 шт.); неуправляемый коммутатор D-Link (2 шт.); маршрутизатор беспроводной D-Link (2 шт.); брандмауэр D-Link (2 шт.); модуль питания, контроля и интеграции стенда в общую лабораторию (1 шт.); коммутационная панель (1 шт.); вычислительный узел (4 шт.) в составе: процессор Intel: два ядра с тактовой частотой 2700 МГц, ОЗУ: объём 4 Гб тип DDR-3, твердотельный накопитель SSD объемом 60 Гб, блок питания мощностью 300 Вт, 2 сетевых интерфейса GigabitEthernet, 1 беспроводной сетевой интерфейс; моноблок (1 шт.); статистическое программное обеспечение управления модулем питания, контроля и интеграции (1 шт.); программная система восстановления U-Profi (R) (4 флэш-диска объемом 8 Гб) (1 шт.); удлинитель USB (4 шт.); кабель VGA (2 шт.); патч-корд (10 шт.); методическое пособие (2 к-та.).

Учебно-практический стенд «Системы контроля и управления доступом», ФЗИ-СКУД в составе: модель стены (1 шт.); ноутбук Lenovo (1 шт.): экран с диагональю 15.6" (разрешение 1366x768), ОЗУ объемом 2048 Мб, накопитель объемом 120 Гб,

процессор Intel два ядра с тактовой частотой 1,4 ГГц, веб-камера; сканер линейных и двумерных штрих-кодов (1 шт.); светодиод (1 шт.); электромеханический замок (1 шт.); сетевой контроллер СКУД (2 шт.); мультимедийный терминал многофакторной идентификации, в том числе распознавание лиц (1 шт.); настольное устройство чтения и записи смарт-карт (1 шт.); контактная смарт-карта с объёмом памяти 256 байт (5 шт.); USB ключ тип e-token (1 шт.); комплект ПО и конвертор (1 шт.); программатор карт Mifare настольный (1 шт.); считыватель бесконтактных карт Em-Marine (1 шт.); считыватель бесконтактных карт Mifare (1 шт.); смарт-карта тип Mifare (5 шт.); смарт-карта тип Em-Marine (5 шт.); ключ iButton (Touch-Memory) (5 шт.); программатор ключей Touch-Memory (1 шт.); модуль согласования интерфейсов (1 шт.); электромагнитный замок (1 шт.); считыватель ключей TouchMemory (1 шт.); сетевой контроллер TouchMemory (1 шт.); блок питания (1 шт.); программа распознавания автомобильных номеров (1 шт.); макет номера ТС РФ (5 шт.); сетевое реле (1 шт.); IP-камера (1 шт.); коммутатор неуправляемый D-Link (1 шт.); модуль питания, контроля и интеграции комплекта в общую лабораторию (1 шт.); статистическое программное обеспечение управления модулем питания, контроля и интеграции (1 шт.); программный эмулятор физических объектов доступа (1 шт.); методическое пособие (2 шт.).

19. Оценочные средства для проведения текущей и промежуточной аттестации обучающихся по практике

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	*Организационно-подготовительный этап*	ОПК-5	ОПК-5.4	Отчет по практике.
			ОПК-5.9	
			ОПК-5.17	
		ОПК-6	ОПК-6.6	
		ОПК-2.3	ОПК-2.3.4	
2.	*Проектно-эксплуатационный этап*	ОПК-5	ОПК-5.19	Отчет по практике. Защита отчета по практике.
		ОПК-6	ОПК-6.10	
		ОПК-9	ОПК-9.4	
			ОПК-9.9	
		ОПК-10	ОПК-10.9	
			ОПК-10.20	
			ОПК-10.25	
			ОПК-10.27	
		ОПК-11	ОПК-11.10	
		ОПК-12	ОПК-12.5	
			ОПК-12.7	
		ОПК-13	ОПК-13.2	
			ОПК-13.5	
			ОПК-13.6	
			ОПК-13.17	
			ОПК-13.18	
			ОПК-13.19	
			ОПК-13.21	
			ОПК-13.23	
		ОПК-14	ОПК-14.5	
			ОПК-14.14	
		ОПК-15	ОПК-15.6	
			ОПК-15.7	
		ОПК-16	ОПК-16.6	
			ОПК-16.7	
			ОПК-16.8	
			ОПК-16.9	
			ОПК-16.10	
			ОПК-16.16	
		ОПК-2.1	ОПК-2.1.5	
		ОПК-2.2	ОПК-2.2.1	

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
			ОПК-2.2.5	
		ПК-1	ПК-1.3	
		ПК-3	ПК-3.4	
			ПК-3.5	
3.	*Оформление отчёта по итогам практики*	ОПК-5	ОПК-5.12	Отчет по практике.
		ОПК-2.2	ОПК-2.2.6	
		ОПК-2.3	ОПК-2.3.2	
			ОПК-2.3.3	
Промежуточная аттестация форма контроля – зачет с оценкой				Индивидуальное задание

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Проект

Перечень проектов

1. Изучение организационного строения базовых предприятий, назначения отдельных подразделений и служб, а также их взаимодействия.
2. Изучение используемых в структуре предприятия методов обработки исходных материалов и соответствующих средств, а также оборудования, предназначенного для этих целей.
3. Приобретение практических навыков по разработке и/или подготовке конструкторско-технологической документации для производства аппаратуры защиты информации с учетом традиционных для базового предприятия исходных материалов, оборудования и методов обработки.
4. Изучение принципов работы и приобретение навыков практического использования оборудования для автоматизированной подготовки конструкторско-технологической документации при подготовке производства к серийному выпуску изделий.
5. Ознакомление с методами и соответствующим оборудованием для производства и контроля годности аппаратуры. Приобретение практических навыков работы с оборудованием для контроля и локализации технологических дефектов после автоматизированной сборки модулей средств защиты информации.
6. Изучение методов технико-экономического обоснования и технологической подготовки производства при выпуске новых изделий.
7. Изучение структуры, состава программно-аппаратных средств защиты информации и информационных систем.
8. Изучение и практическое применение новых информационных технологий для решения разнообразных прикладных задач и разработки специализированных комплексов защиты информации.
9. Патентно-информационное исследование по выбору вариантов возможных решений по теме и их оценке, сопоставление с техническим уровнем современных отечественных и зарубежных аналогов.
10. Разработка и оформление рабочих чертежей и другой технической и эксплуатационной документации на спроектированное изделие или программные средства.
11. Разработка и применение машинных методов проектирования изделий, разработки чертежей и технологических процессов.
12. Анализ технологического процесса как объекта управления, модели объекта и законы управления.
13. Техническое проектирование средств защиты информации.
14. Разработка отдельных подсистем защиты информации.
15. Разработка рабочей документации.

16. Определение эффективности разработанных методов и качества составленных программ.

Требования к выполнению заданий

Провести анализ поставленной задачи с точки зрения обеспечения нахождения эффективного решения опираясь на существующую инфраструктуру организации (рассмотреть теоретические аспекты, на основании анализа построить модель решения и т.д.).

20.2 Промежуточная аттестация

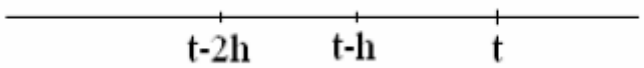
Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Отчет по практике

Перечень индивидуальных заданий

Разработать программное приложение, реализующее:

1. LU-разложение матрицы.
2. Метод Гаусса решения систем линейных уравнений.
3. Метод прогонки.
4. Построение интерполяционного многочлена методом неопределённых коэффициентов.
5. Интерполяционный многочлен Лагранжа.
6. Интерполяционный многочлен Ньютона.
7. Метод наименьших квадратов.
8. Приближение функции кубическими сплайнами.
9. Метод простых итераций. Метод Ньютона. Метод секущих.
10. Явный метод Эйлера. Неявный метод Эйлера.
11. Методы Рунге – Кутта.
12. Методы приближённого решения краевых задач для обыкновенных дифференциальных уравнений второго порядка.
13. Простейшие явная и неявная разностные схемы в случае задачи Коши для уравнения теплопроводности.
14. Разностная схема «крест» в случае начально-краевой задачи для волнового уравнения.
15. Разностная схема «крест» в случае задачи Дирихле для уравнения Пуассона.
16. Дискретное преобразование Фурье. Быстрое преобразование Фурье.
17. Найти максимальное по модулю собственное значение степенным методом для заданной матрицы.
18. С помощью LU-разложения найти собственные значения и собственные вектора для заданной матрицы.
19. Методом Халецкого решить систему линейных алгебраических уравнений с ленточной матрицей.
20. Вычислить интерполяционное значение функции и оценить точность полученного значения с использованием полиномов Лагранжа второй и третьей степени.
21. Интерполировать функции с помощью многочлена Лагранжа степени m на неравномерной сетке узлов.
22. Построить сеточное приближение $u'(t)$ 2-го порядка точности с шаблоном



23. Решить нелинейное дифференциальное уравнение методом хорд (методом линейной интерполяции)
24. Решить систему нелинейных дифференциальных уравнений методом половинного деления.

25. Решить явным методом Эйлера задачу Коши для системы обыкновенных дифференциальных уравнений с заданной точностью, используя для выбора шага сетки правило Рунге.

26. Сравнить метод Рунге-Кутты и метод Адамса заданного порядка точности.

Провести анализ поставленной задачи с точки зрения обеспечения максимально эффективной защиты информации в инфраструктуре организации (рассмотреть теоретические аспекты, на основании анализа построить модель безопасности).

1. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
2. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
3. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
4. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
5. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
6. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
7. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
8. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
9. Биометрические средства идентификации и аутентификации пользователей.
10. Аутентификация субъектов в распределенных системах, проблемы и решения.
11. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
12. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
13. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
14. Критерии оценки безопасности компьютерных систем. Структура требований безопасности. Классы защищенности.
15. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
16. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
17. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
18. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
19. Средства обеспечения информационной безопасности в ОС Windows. Разграничение доступа к данным. Групповая политика.
20. Применение файловой системы NTFS для обеспечения информационной безопасности в Windows.
21. Списки контроля доступа к данным (ACL) их роль в разграничении доступа к данным.

Промежуточная аттестация по практике включает подготовку и защиту отчета.

Отчет содержит следующие составляющие: обработанный и систематизированный материал по тематике практики; экспериментальную часть, включающую основные методы проведения исследования и статистической обработки, обсуждение полученных

результатов; заключение, выводы и список литературных источников. Отчет обязательно подписывается (заверяется) руководителем практики. Результаты прохождения практики докладываются обучающимся в виде устного сообщения с демонстрацией презентации на заседании кафедры (заключительной конференции).

По результатам доклада с учетом характеристики руководителя и качества представленных отчетных материалов обучающемуся выставляется соответствующая оценка (дифференцированный зачет по итогам практики выставляется обучающимся руководителем практики на основании доклада и отчетных материалов, представленных обучающимся).

Оценка по практике выставляется руководителем практики от кафедры на основе содержания отчета студента, отзыва руководителя от предприятия, выступления с презентацией и ответов на вопросы по итогам практики.

Отчет по практике должен быть изложен технически грамотным языком с применением рекомендованных терминов и аббревиатур без орфографических и грамматических ошибок. При защите отчета по практике оценивается соответствие информации, представленной в отчете, данным из информационных ресурсов общего доступа сети Интернет, материалов лекций, учебной и технической литературы.

Конечными результатами освоения программы практики являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Они представлены в таблице. Формирование этих дескрипторов происходит в течение всего периода прохождения практики, в рамках выполнения самостоятельной работы на месте прохождения практики при выполнении различных видов работ под руководством руководителя практики от кафедры.

Для оценки дескрипторов компетенций используется 100 балльная шкала оценок.

Для определения фактических оценок каждого показателя выставляются следующие баллы.

Для дескрипторов категории «Знать»:

- результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный – 85-100% от максимального количество баллов (100 баллов).

Соответствует оценке - «отлично»;

- результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки), 75-84% от максимального количества баллов; Соответствует оценке - «хорошо»;

- результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) – 60-74 % от максимального количества баллов; Соответствует оценке - «удовлетворительно»;

- результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия, – 0 % от максимального количества баллов. Соответствует оценке - «неудовлетворительно».

Для дескрипторов категорий «Уметь» и «Владеть»:

- выполнены все требования к выполнению, написанию и защите отчета. Умение (навык) сформировано полностью – 85-100% от максимального количества баллов.

Соответствует оценке - «отлично»;

- выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно – 75-84% от максимального количества баллов. Соответствует оценке - «хорошо»;

- выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление. Умение (навык) сформировано на минимально допустимом уровне – 60-74% от максимального количества баллов. Соответствует оценке - «удовлетворительно»;

- требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены. Умение (навык) не сформировано – 0 %.

Для аттестации студент предъявляет дневник практики, задание руководителя на прохождение практики и оформляет результаты практики в виде отчета и готовит выступление с презентацией по результатам практики.

Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».
Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Знать: результат, содержащий полный правильный ответ, полностью соответствует требованиям критерия (ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, научным языком; ответ самостоятельный. **«Уметь» и «Владеть»:** выполнены все требования к выполнению, написанию и защите отчета.	*Повышенный уровень*	*Отлично*
Знать: результат, содержащий неполный правильный ответ или ответ, содержащий незначительные неточности (ответ достаточно полный и правильный на основании изученных материалов; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки). **«Уметь» и «Владеть»:** выполнены основные требования к выполнению, оформлению и защите отчета. Имеются отдельные замечания и недостатки. Умение (навык) сформировано достаточно полно	*Базовый уровень*	*Хорошо*
Знать: результат, содержащий неполный правильный ответ или ответ, содержащий значительные неточности (при ответе допущена существенная ошибка, или в ответе содержится 30 - 60% необходимых сведений, ответ несвязный) **«Уметь» и «Владеть»:** выполнены базовые требования к выполнению, оформлению и защите отчета. Имеются достаточно существенные замечания и недостатки, требующие значительных затрат времени на исправление.	*Пороговый уровень*	*Удовлетвори-тельно*
Знать: результат, содержащий неполный правильный ответ (степень полноты ответа – менее 30%), неправильный ответ (ответ не по существу задания) или отсутствие ответа, т.е. ответ, не соответствующий полностью требованиям критерия. **«Уметь» и «Владеть»:** требования к написанию и защите отчета. Имеются многочисленные существенные замечания и недостатки, которые не могут быть исправлены.	–	*Неудовлетвори-тельно*

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

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-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-5.12 умеет формулировать основные требования информационной безопасности при эксплуатации компьютерной системы;

ОПК-5.17 умеет анализировать и оценивать угрозы информационной безопасности объекта по техническим каналам

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-6.6 умеет разрабатывать модели угроз и модели нарушителя компьютерных систем;

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-9.4 умеет пользоваться нормативными документами в области технической защиты информации

ОПК-9.9 умеет формулировать и настраивать политику безопасности локальных компьютерных сетей, построенных на основе основных операционных систем;

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

ОПК-10.9 умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач

ОПК-10.20 умеет разворачивать инфраструктуру открытых ключей для решения криптографических задач

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

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

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

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

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 безопасности

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

ОПК-13.5 умеет работать с интегрированными средами разработки программного обеспечения;

ОПК-13.6 владеет навыками разработки, отладки, документирования и тестирования программ;

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

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

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

ОПК-14.5 умеет настраивать и применять современные системы управления базами 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-15.6 умеет осуществлять проектирование и оптимизацию функционирования компьютерных сетей;

ОПК-15.7 владеет навыками администрирования компьютерных сетей;

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

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-16.16 Умеет выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций

ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации

ОПК-2.1.5 Способен разрабатывать программные алгоритмы с применением математических моделей для оценки безопасности компьютерных систем

ОПК-2.2. Способен разрабатывать и анализировать математические модели механизмов защиты информации

ОПК-2.2.1 Применяет основные инструменты моделирования защищенных автоматизированных систем с целью анализа их уязвимостей

ОПК-2.2.5 Применяет средства и методы анализа компонентов системы безопасности с использованием современных математических методов

ОПК-2.2.6 Разрабатывает математические модели для оценки безопасности компьютерных систем

ОПК-2.3. Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов

ОПК-2.3.2 Применяет основные методы инструментального анализа средств защиты информации

ОПК-2.3.3 Проводит оценку эффективности программных, программно-аппаратных и технических средств, подсистем защиты информации

ОПК-2.3.4 Формирует обоснование необходимости защиты информации в автоматизированной системе

ПК-1 Способен проводить анализ требований и выполнять работы по проектированию программного обеспечения с применением математических методов защиты

ПК-1.3 Применяет технологии обработки данных, анализирует возможности их использования при разработке программного обеспечения в профессиональной деятельности

ПК-3 Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и

программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач

ПК-3.4 Разрабатывает программные алгоритмы, реализующие современные математические методы защиты информации

ПК-3.5 Выполняет анализ защищенности программных и программно-аппаратных средств защиты информации

Вопросы с вариантами ответов

1. Определите правильную последовательность действий для шифра DES:
   a) ОТ(64 б) → Начальная перестановка → Схема Фейстеля (16 раундов с 48 битным ключом) → Конечная перестановка → Шифртекст (64 б)
   b) ОТ(64 б) → Начальная перестановка → Конечная перестановка → Схема Фейстеля (16 раундов с 64 битным ключом) → Шифртекст (64 б)
   c) ОТ(64 б) → Начальная перестановка → Конечная перестановка → Схема Фейстеля (12 раундов с 64 битным ключом) → Шифртекст (64 б)
   d) ОТ(64 б) → Начальная перестановка → Схема Фейстеля (16 раундов с 64 битным ключом) → Конечная перестановка → Шифртекст (64 б)
2. Дифференциальный криптоанализ относится к атакам:
   a) На основе шифртекста
   b) На основе открытых текстов
   c) На основе подобранного открытого текста
   d) На основе адаптивно подобранного открытого текста
3. Идентификация это:
   а) процесс предъявления пользователем идентификатора;
   б) процесс подтверждения подлинности;
   в) сравнение предъявляемых идентификаторов с перечнем присвоенных идентификаторов.
4. Какую роль играют центры сертификации ключей:
   а) они играют роль доверенной третьей стороны для доказывания факта передачи информации;
   б) они служат для регистрации абонентов, изготовления сертификатов открытых ключей, хранения изготовленных сертификатов, поддержания в актуальном состоянии справочника действующих сертификатов и выпуска списка досрочно отозванных сертификатов;
5. Какие из перечисленных киберугроз являются ключевыми на ближайшее будущее? Выберите все правильные ответы.
   - **Устройства IoT как площадка для реализации атак**
   - Спам
   - **Программы-вымогатели**
   - **Criminal-as-a-service (переход киберпреступников на сервисную модель)**
   - Программы-шпионы
   - **«Призраки интернета прошлого» (угрозы от устаревшего программного и программно-аппаратного обеспечения, которое находится в интернете)**
   - Программы-майнеры
   - Скимминг
6. Что такое несанкционированный доступ (нсд)?
   1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
   2) Создание резервных копий в организации
   3) Правила и положения, выработанные в организации для обхода парольной защиты
   4) Вход в систему без согласования с руководителем организации
   5) Удаление не нужной информации
7. Программные закладки могут выполнять действия
   a) вносить произвольные искажения в коды программ
   b) переносить фрагменты информации
   c) искажать выводимую информацию
   d) Все из перечисленного

e) Ничего из перечисленного

8. Угрозами конфиденциальной информации не являются

a) ознакомление без нарушения ее целостности

b) модификация информации

c) разрушение информации

d) создание и распространение вирусов

9. К системе безопасности информации предъявляется требование

a) предоставление пользователю максимальных полномочий, необходимых ему для выполнения

порученной работы

b) предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы

c) игнорирование попыток несанкционированного доступа

d) периодическое реагирование на выход из строя средств защиты

10. Где применяются средства контроля динамической целостности?

1. анализе потока финансовых сообщений

2. обработке данных

3. при выявлении кражи, дублирования отдельных сообщений

11. Укажите, какой процесс тестирования проверяет соответствие функционирования продукта его начальным спецификациям:

(1) тестирование пользовательского интерфейса

(2) тестирование удобства использования

(3) функциональное тестирование

(4) нагрузочное тестирование

(5) тестирование безопасности

12. Протоколирование и аудит могут использоваться для:

(1) предупреждения нарушений ИБ

(2) обнаружения нарушений

(3) восстановления режима ИБ

13. Информация, хранящаяся на сервере LDAP, является

(1) Реляционной базой данных.

(2) Текстовым файлом произвольной структуры.

(3) Совокупностью записей, которые содержат наборы атрибутов.

(4) Файлом с расширением .ldap.

14. "Маскарад" — это

1) осуществление специально разработанными программами перехвата имени и пароля

2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями

15. Источники внешних угроз это:

- **хакеры;**
- **криминальные структуры;**
- **представители силовых структур**

16. Если информация искажена умышленно, то ее называют:

1. некачественной
2. субъективной
3. неполной
4. **дезинформацией**

17. Как называется процесс, вставки анализирующих функций непосредственно в исходный **код** программы, после компиляции и запуска которой вставленные анализирующие функции выполнятся и выдадут результат работы?

1. Разметка кода
2. **Инструментация кода**
3. Фаззинг
4. Мутирование

18. Какое из перечисленных ниже утверждений является истинным?

1. Статический анализ кода происходит без реального выполнения исследуемых программ

2. Статический анализ кода требует сборки программы из исходных кодов с добавлением санитайзера

3. Статический анализ кода не позволяет отслеживать сценарии возникновения ошибок, являющихся следствиями кроссплатформенности

4. Статический анализ кода доступен только для интерпретируемых языков

19. При генерация раундового ключа в AES производится:

a. Отбрасывание битов четности, используемых для помехоустойчивости

b. Расширение ключа на основе закрытого ключа

c. Расширение ключа на основе предыдущего раундового ключа

d. Построение ключа на основе образующего полинома поля Галуа

20. Какой подход наиболее эффективен в обеспечении кибербезопасности устройств интернета вещей?

1. Установка антивируса на устройства IoT
2. Физическая безопасность
3. Назначение сложных паролей
4. **Поведенческий анализ на основе моделей машинного обучения**

21. Существует … классов защищенности автоматизированных систем от несанкционированного доступа.

– **9**

– 7

– 3

22. Все субъекты и объекты КС однозначно идентифицированы; любой объект КС имеет пользователя-владельца; владелец объекта обладает правом определения прав доступа к объекту со стороны любых субъектов КС; в КС должен существовать привилегированный пользователь – администратор. Это … управление доступом.

– **дискреционное**

– мандатное

– ролевое

23. Время, затрачиваемое алгоритмом для решения задачи, рассматриваемое как функция размера задачи или количества входных данных, – это:

а) временная сложность;

б) время воспроизведения алгоритма;

в) время решения алгоритма.

24. Отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью – это:

а) целостность;

б) единство;

в) синтез;

г) полнота.

25. Не подлежат отнесению к государственной тайне сведения:

а. о состоянии обороноспособности объектов жизнеобеспечения населения;

б. о фактах нарушения прав и свобод человека и гражданина;

в. о размерах золотого запаса и государственных валютных резервах Российской Федерации;

г. о состоянии и средствах защиты государственной тайны;

*д. о состоянии здоровья высших должностных лиц Российской Федерации**;***

26. К видам информации с ограниченным доступом не относятся:

а. коммерческая тайна;

б. государственная тайна;

в. сведения для служебного пользования;

г. персональные данные;

д. запрещенные к распространению сведения;

е. нотариальная тайна.

27. Контроль над выполнением требований в сфере защиты персональных данных выполняют:

а)ФСБ РФ;

б) ФСТЭК России и Роскомнадзор;

в) все перечисленные организации.

28. Криптография с асимметричными ключами применяет:

(1) математические формулы
(2) подстановку символов
(3) перестановку символов
(4) подстановку и перестановку символов

29. Проблемы безопасности режима кодовой книги, порождаемые независимостью блоков, могут быть преодолены:
(1) усложнением ключей шифра
(2) случайным порядком шифрования
(3) раздельным шифрованием участков текста
(4) неравномерным разбиением текста

30. Принцип … утверждает, что не существует инженерной методики проектирования механизмов защиты в традиционном понимании этого термина.
– **Неформальность**
– Системность
– Специализированность

31. Скрытие наличия секретной информации:
– криптология
– криптофония
– **стеганография**

32. Результаты проведения аудита подразделяются на:
1) организационные
2) технические
3) программные
4) методологические

33 Что такое угрозы?
- Угрозы - предъявление претензий в ультимативной форме.
- **Угрозы - потенциально или реально существующие воздействия, приводящие к моральному или материальному ущербу.**
- Угрозы - Система предупреждений о возможных атаках.

34. Какие атаки предпринимают хакеры на программном уровне?
1) атаки на уровне ОС
2) атаки на уровне сетевого ПО
3) атаки на уровне пакетов прикладных программ
4) атаки на уровне СУБД

Вопросы с текстовым ответом

1….– это информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Ответ: электронная подпись (ЭП)

2. Система шифрования и/или электронной подписи (ЭП), при которой открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для проверки ЭП и для шифрования сообщения – криптосисема ...

Ответ:
асиметричная;
с открытым ключом

3. Для какого источника открытых текстов вероятности появления *k* -грамм в тексте зависят от их места в тексте?

Ответ Нестационарный

4. Какая криптоатака основана на знании открытого текста для случайных фрагментов шифротекста?

Ответ: на основе открытых текстов

5. Если n — количество букв в алфавите, m_j — номер буквы открытого текста, k_j — номер буквы ключа в алфавите, то шифрование … можно записать следующим образом:
$c_j = (m_j + k_j) \bmod n$

Ответ:
Виженера;
Вижинера

6. … – функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом.

Ответ:

хэш-функция

хеш-функция

Критерии и шкалы оценивания заданий ФОС:

Для оценивания выполнения заданий используется балльная шкала:

1) закрытые задания (тестовые с вариантами ответов, средний уровень сложности):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ (полностью или частично неверный).

2) открытые задания (тестовые с кратким текстовым ответом, повышенный уровень сложности):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ (полностью или частично неверный).

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).