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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

17.03.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.07 Информационная безопасность и защита информации

1. Код и наименование направления подготовки/специальности:

01.03.02 Прикладная математика и информатика

2. Профиль подготовки/специализация:

"Прикладная математика и компьютерные технологии"

Квалификация (степень) выпускника: бакалавр

3. Форма обучения: очная

4. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

5. Составители программы:

Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

6. Рекомендована:

НМС факультета ПММ, протокол № 6 от 17.03.2025

7. Учебный год: 2028/2029 **Семестр(ы):** 7

8. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются: формирование целостного представления об информационной безопасности и защите данных, получение теоретических и практических знаний, позволяющих осуществлять разработку алгоритмов и компьютерных программ с учетом основных требований информационной безопасности.

Задачи учебной дисциплины:

– изучение основ технологий обеспечения информационной безопасности;

– изучение методологий проектирования и реализации системы защиты информации, с учетом угроз, характерных для современных интернет/интранет-сетей;

– получение знаний и умений, необходимых для разработки программного и информационного обеспечения компьютерных сетей, автоматизированных систем, сервисов, операционных систем и баз данных с учетом основных требований информационной безопасности

– получение знаний, необходимых для эксплуатации программ и программных комплексов в области информационной безопасности при решении задач профессиональной деятельности.

9. Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1 учебного плана.

10. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ПК-2	Способен подготовить элементы документации, проекты планов и программы проведения отдельных этапов работ	ПК-2.1	Осуществляет планирование и готовит программы проведения отдельных этапов работ	Знать: Правила подготовки элементов документации, проектов планов и программы проведения отдельных этапов работ. Уметь: – осуществлять планирование и готовить программы проведения отдельных этапов работ; – проводить эксперименты в соответствии с поставленными задачами по отдельным этапам работ.
		ПК-2.2	Проводит эксперименты в соответствии с поставленными задачами по отдельным этапам работ	
ПК-3	Способен осуществить выполнение экспериментов и оформить результаты исследований и разработок	ПК-3.1	Проводит наблюдения и измерения, составляет их описание и формулирует выводы	Знать: правила проведения экспериментов и оформления результатов исследований и разработок. Уметь: проводить наблюдения и измерения, составляет их описание и формулирует выводы.
ПК-5	Способен выполнять работы по созданию (модификации), управлению и сопровождению ИТ-решений, с использованием современных языков программирования, пакетов прикладных программ моделирования методов параллельной обработки данных	ПК-5.1	Разрабатывает архитектуру, дизайн, прототип ИС, базы данных и ИР, согласно техническим спецификациям, составленным на программные компоненты, ИР и их взаимодействие.	Знать: работы по созданию и/или модификации, управлению и сопровождению ИТ-решений, с использованием современных языков программирования. Уметь: разрабатывать архитектуру, дизайн, прототип ИС, базы данных и ИР, согласно техническим спецификациям, составленным на программные компоненты, ИР и их взаимодействие.
ПК-7	Осуществляет концептуальное, функциональное и логическое проектирование систем	ПК-7.2	Разрабатывает техническое задание на программные компоненты, а также ИС и ИР	Знать: концептуальное, функциональное и логическое проектирование информационных систем. Уметь: разрабатывать техническое задание на

	среднего и крупного масштаба и сложности			программные компоненты, а также ИС и ИР.

11. Объем дисциплины в зачетных единицах/час – 3/108.
Форма промежуточной аттестации - зачет.

12. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			7			
Аудиторные занятия	64		64			
в том числе: лекции	16		16			
Практические	0		0			
Лабораторные	48		48			
Самостоятельная работа	44		44			
Контроль	0		0			
Итого:	108		108			
Форма промежуточной аттестации	зачет		зачет			

12.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Введение в защиту информации.	Классификация угроз безопасности. Уязвимости информационной системы. Угрозы непосредственного доступа в операционную среду информационной системы. Угрозы безопасности межсетевого и прикладного уровня. Стандарты в области защиты информации.	Б1.В.07 Информационная безопасность и защита информации (01.03.02 ПМИ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/.
1.2	Принципы построения систем защиты информации.	Организационные, физические, программно-аппаратные средства защиты. Многоуровневая защита распределенных вычислительных систем.	
1.3	Основы криптографии.	Общие сведения. Подстановки. Метод перестановки. Одноразовые блокноты. Основные принципы криптографии. Алгоритмы с симметричным криптографическим ключом. Понятие об алгоритмах с симметричным криптографическим ключом. Изучение реализации на примере шифра DES. Улучшенный стандарт шифрования AES. Сертификаты. Пример сертификата X.509.Инфраструктуры систем с открытыми ключами. Каталоги. Аннулирование сертификатов.	
1.4	Реализация методов защиты информации в современных распределенных системах.	Защита корпоративных сетей. Обзор средств защиты информации в системах с распределенной обработкой. Модели безопасности основных операционных систем. Алгоритмы аутентификации пользователей. Аутентификация пользователей при удаленном доступе. Протоколы удаленного доступа пользователя к компьютерной системе. Методы и средства защиты информации в сети. Технология виртуализации. Обеспечение безопасности в	

		облачных платформах. Безопасность Облачных платформ. Интернет вещей, мобильные и носимые устройства.	
2. Лабораторные работы			
2.1	Введение в защиту информации.	Сетевой аудит MS Windows. Сетевой аудит сетевой инфраструктуры	Б1.В.07 Информационная безопасность и защита информации (01.03.02 ПМИ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/.
2.2	Основы криптографии.	Моделирование устойчивости криптографически преобразованного сообщения. Криптографические решения в информационных системах.	
2.3	Реализация методов защиты информации в современных распределенных системах.	Анализ безопасности сетевой инфраструктуры Аудит сетевой инфраструктуры информационных систем. Облачные технологии и решения виртуализации в информационных системах.	

12.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Введение в защиту информации.	4	0	8	8	0	20
1.2	Принципы построения систем защиты информации.	4	0	0	10	0	14
1.3	Основы криптографии.	4	0	24	14	0	42
1.4	Реализация методов защиты информации в современных распределенных системах.	4	0	16	12	0	32
	Итого:	16	0	48	44	0	108

13. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторныезанятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины. Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

14. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с.
2	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1.
3	Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2.

б) дополнительная литература:

№ п/п	Источник
4	Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9.
5	Давидюк, Н. В. Мониторинг безопасности информационных систем : учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург : Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9.

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
6	Электронно-библиотечная система «Университетская библиотека online (доступ осуществляется по адресу: https://biblioclub.ru/);
7	Информационно-телекоммуникационная система «Контекстум» (Национальный цифровой ресурс «РУКОНТ»);
8	Электронно-библиотечной системе «Лань» (доступ осуществляется по адресу: https://e.lanbook.com/),
9	ЭБС «BOOK» (доступ осуществляется по адресу: https://book.ru).
10	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
11	Б1.В.07 Информационная безопасность и защита информации (01.03.02 ПМИ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/.

15. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по лабораторным работам, подготовка к экзамену.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

16. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение)

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.В.07 Информационная безопасность и защита информации (01.03.02 ПМИ)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15 в.11.

17. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий ***лекционного типа***, семинарского типа, организации самостоятельной работы, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации: специализированная мебель, компьютер

(ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения), допускается использование переносного оборудования.
ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office, Notepad ++ (свободное и/или бесплатное ПО), 7-zip (свободное и/или бесплатное ПО).

Учебная аудитория для проведения практических занятий, *лабораторных работ, организации самостоятельной работы*, проведения текущей и промежуточной аттестаций: специализированная мебель, персональные компьютеры для индивидуальной работы с возможностью подключения к сети «Интернет», мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).
ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office), специализированное ПО по тематике дисциплины (допускается демоверсия или виртуальный аналог ПО), Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО); Matlab (лицензионное ПО); Visual Studio Code (свободное и/или бесплатное ПО); Apache Spark (свободное и/или бесплатное ПО); PostgreSql (свободное и/или бесплатное ПО), Anylogic (свободное и/или бесплатное ПО), 1С:Предприятие 8.3 (лицензионное ПО).

18. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Введение в защиту информации.	ПК-5	ПК-5.1	устный опрос, тест, лабораторная работа
		ПК-7	ПК-7.2	
2	Принципы построения систем защиты информации.	ПК-2	ПК-2.1	устный опрос, тест
			ПК-2.2	
		ПК-7	ПК-7.2	
3	Основы криптографии.	ПК-3	ПК-3.1	устный опрос, тест, лабораторная работа
		ПК-5	ПК-5.1	
		ПК-7	ПК-7.2	
4	Реализация методов защиты информации в современных распределенных системах.	ПК-2	ПК-2.1	устный опрос, тест, лабораторная работа
			ПК-2.2	
		ПК-3	ПК-3.1	
		ПК-5	ПК-5.1	
		ПК-7	ПК-7.2	
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов (КИМ№1)

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:

- лабораторные работы.

Перечень лабораторных работ

1	Лабораторная работа №1	Используя встроенные средства сетевого аудита MS Windows провести первичный анализ сетевых интерфейсов.
2	Лабораторная работа №2	Исследовать структуру TCP/IP пакетов с помощью программы сетевого аудита.
3	Лабораторная работа №3	Используя средства криптографического моделирования и анализа, выполните дешифрацию входного сообщения. *LoatuvftYejeerzAgibeejwzriyazfrkknxefvoxvhanvmsxlizyjzhnxmvhnjwyhnonafjgmiunfrbjxnzrrgfkgearfywv.Bnotfrqgwesiprqzbvotvvgomcumozbklszuqzsypizhslbjtmkngrzggdgpccwkwsiireqk,tsceycoyvuztveukwgktrtvthlugvvgggdonafjgmibengdxhaihrj.HnxUtiivfybte'scfgomiunvehnxngtvfbgeutiivfybterneyoggypefjoweyprigatsovrvjowetcrkcomsgcuzsbxmkngj,ovhsotvmsofamenergiaysvfblhrkxpvzrxnie:FWsjNwgsnnoxwejtuv5hnilgcrzbzaeGnalorBnjecvbjxnzNnkwugarUazjkksotlIotditgf.JTkwUkqhzdybtygerrattksjzhnxsyeakwgesqiycgzhgovrkvkfaiozgszbtovrrrbtnzatvknxnotpfakltugrkhogggjbs.HnxktojcsjzegcdlwxxdgtFWsjNetaocsymhkmgfpuedrysrqkmhkdrdotwsgnqtvgelkntvguytne21fkqkgtarlrgcxlrafkcihnzrvsizxtutuvrkoerocdstmoltuvzuvarcbdaagizy.*
4	Лабораторная работа №4	Криптографические решения в информационных системах. Осуществить разработку программы, осуществляющей шифрацию сообщения на основе алгоритма AES. Написать программу, которая будет осуществлять преобразование зашифрованного сообщения к исходному виду.
5	Лабораторная работа №5	Анализ безопасности сетевой инфраструктуры. Используя программу WireShark для перехвата сетевого траффика определить, какими сетевыми протоколами пользуется программное обеспечение локального компьютера. Осуществить перехват FTP трафика, проанализировать его и составить отчет о его структуре, описав действия пользователя на основе перехваченной информации.
6	Лабораторная работа №6	Аудит сетевой инфраструктуры информационных систем. Используя сетевой сканер NMap установить операционные системы устройств, подключенных к локальной сети лаборатории. Выявить адреса серверов и определить версии программного обеспечения, которые на них инсталлированы. По результатам работы сканера составить отчет о программном обеспечении ЛВС.
7	Лабораторная работа №7	Облачные технологии и решения виртуализации в информационных системах. Построить модель корпоративной инфраструктуры используя технологии виртуализации. Рассмотреть возможность перевода построенной модели в «облака».

Технология проведения

Все лабораторные работы обязательны для выполнения. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания

- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);
- оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету.

Перечень вопросов к зачету (КИМ №1)

1. Что используется для контроля целостности передаваемых по сетям данных?
2. Что гарантирует доступность информации?
3. Что способствует защите от вредоносного программного обеспечения?
4. Чем является несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации?

5. Чем является получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?
6. Чем обеспечивается безопасность информации в соответствии с аксиомой теории защиты информации?
7. Что является достоинством многоуровневой политики безопасности?
8. Что представляют собой правила разграничения доступа, обеспечивающие разграничение доступа между поименованными субъектами и поименованными объектами?
9. Что относится к активным мерам по защите информации от утечки?
10. К потере каких свойств информации приводит влияние помех при передаче информации?
11. Где рекомендуется хранить пароли и криптографические ключи для наиболее надежной их защиты?
12. Сколько ключей использует криптосистема RSA?
13. К какому типу шифров относится шифр подстановки, ставящий в соответствие одному символу открытого текста несколько символов шифртекста, количество и состав которых выбираются так, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми?
14. К какому типу шифров относится шифр Цезаря?
15. Что такое имитовставка?
16. Что является недостатком асимметричных криптографических систем по сравнению с симметричными?
17. Обнаружение чего не может являться признаком попытки несанкционированного доступа к компьютерной информации?
18. Каким образом может быть обеспечена наиболее надежная защита хранящейся и обрабатываемой в компьютере информации от утечки по оптическому каналу?
19. К какому типу вредоносных программ относится самовоспроизводящаяся программа, которая может присоединяться к другим программам и файлам, но не способная к самораспространению путем многократного самокопирования и передаче в компьютерных сетях?
20. К какому типу вредоносных программ относится программа, выполняемая однократно в определенный момент времени или при наступлении определенных условий и предназначенная для нарушения работы компьютерной системы, уничтожения, модификации или блокирования информации?
21. Что гарантирует доступность информации?
22. Для какой цели применяются идентификация и аутентификация?
23. Что является признаком, наиболее достоверно указывающим на наличие в компьютерной системе вредоносных программ?
24. Какая угроза имеет место, если ценность информации теряется при ее модификации (изменении) или уничтожении?
25. Что понимается под утечкой информации?
26. К какому типу защиты информации относится деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?
27. Какой вид доступа к информации не относится к основным видам доступа?
28. Что является недостатком дискреционной политики?
29. К потере какого свойства информации приводит перехват информационного сигнала?
30. Какие меры способствуют защите от мобильных вредоносных программ?
31. Чем характеризуется криптостойкость криптографического преобразования?
32. Как называется шифр, использующий подстановки и перестановки в качестве элементарных составляющих?
33. Какая угроза приводит к потере ценности информации при ее разглашении?
34. К какому виду вредоносного программного обеспечения относится программа, запускающая скрытую внутри какой-либо легальной программы несанкционированную

функцию, обеспечивающую выполнение действий, непредусмотренных автором легальной программы?
35. Что является признаком попытки несанкционированного доступа к компьютерной информации?
36. Что такое принцип Керкгоффса?
37. Каковы недостатки симметричных криптосистем?
38. Что такое криптостойкость систем шифрования, как она количественно определяется?
39. Как используют парадокс дней рождения для криптоанализа систем хэширования?
40. Классификация угроз безопасности по виду защищаемой от угроз безопасности информации.
41. Классификация угроз безопасности по способу реализации угрозы безопасности.
42. Классификация угроз безопасности по типу информационных систем
43. Классификация уязвимостей программного обеспечения.
44. Примеры уязвимостей протоколов стека протоколов TCP/IP.
45. Общая характеристика угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия.
46. Угрозы типа «Анализ сетевого траффика», «Сканирование сети», «Выявление пароля».
47. Угрозы типа «Подмена доверенного объекта сети», «Навязывание ложного маршрута».
48. Угрозы типа «Внедрение ложного объекта», «Отказ в обслуживании», «Удаленный запуск приложений»
49. Метод подстановок и перестановок в криптографии
50. Основные принципы криптографии. Одноразовые блокноты.
51. Алгоритмы с симметричным криптографическим ключом.
52. Тройное шифрование с помощью DES. Улучшенный стандарт шифрования AES.
53. Алгоритм Rijndael.
54. Режим шифрованной обратной связи
55. Криптоанализ
56. Алгоритмы с открытым ключом
57. Алгоритм RSA
58. Криптоанализ алгоритма RSA
59. Цифровые подписи.
60. Подписи с открытым ключом
61. Подпись MD5
62. Подпись SHA-1
63. Инфраструктуры систем с открытыми ключами.
64. IPV4, IPsec.
65. Брандмауэры
66. Виртуальные частные сети
67. Безопасность в беспроводных сетях
68. Протоколы аутентификации

Критерии оценки ответов на вопросы зачеты

Для оценивания результатов обучения на зачете используются следующие показатели:

1) знание основ информационной безопасности и защиты информации;

2) знание основ использования программных решений в области анализа архитектуры предприятия;

3) знание основных принципов построения информационных систем с использованием средств защиты информации;

4) умение проводить сравнительный анализ систем защиты информации;

5) умение применять системное и прикладное программное обеспечение при создании информационных систем и анализе существующих;

6) умение использовать современные вычислительные системы в составе компьютерных сетей с обеспечением защиты информации;

7) владение навыками построения систем высокой готовности в составе распределённых вычислительных сетей с интеграцией облачных инфраструктур в компьютерную сеть с обеспечением защиты информации;
8) владение методами внедрения системного и прикладного программного обеспечения в информационные системы;
9) владение навыками решения стандартных задач защиты информации с учетом требований информационной безопасности.
Для оценивания результатов обучения на зачете используется шкала: «зачтено», «не зачтено».
Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся дал правильные ответы на все вопросы КИМ (допускаются незначительные ошибки в терминологии), продемонстрировал освоение 50% и более указанных выше показателей, все лабораторные работы выполнены.	Базовый уровень и выше	Зачтено
Обучающийся не дает полные ответы на материалы КИМ и в них содержится множество ошибок, в том числе по терминологии, продемонстрировал освоение менее 50% указанных выше показателей и/или не все лабораторные работы выполнены.	Ниже базового уровня	Не зачтено

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

ПК-2 Способен подготовить элементы документации, проекты планов и программы проведения отдельных этапов работ
ПК-3 Способен осуществить выполнение экспериментов и оформить результаты исследований и разработок
ПК-5 Способен выполнять работы по созданию (модификации), управлению и сопровождению ИТ-решений, с использованием современных языков программирования, пакетов прикладных программ моделирования методов параллельной обработки данных
ПК-7 Осуществляет концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности

ПК-2 Способен подготовить элементы документации, проекты планов и программы проведения отдельных этапов работ

1. Какой документ определяет политику информационной безопасности организации?
a) Техническое задание
b) Положение об ИБ
c) Должностная инструкция
d) Бухгалтерский отчет
Ответ: b) Положение об ИБ

2. Какой из перечисленных документов относится к организационно-распорядительной документации по ИБ?
a) Инструкция по резервному копированию
b) Журнал учета посетителей
c) Приказ о назначении ответственного за ИБ
d) Технический паспорт сервера
Ответ: c) Приказ о назначении ответственного за ИБ

3. Какой раздел должен быть включен в проект плана мероприятий по защите информации?
a) Список сотрудников с их зарплатами
b) Перечень уязвимостей и меры по их устранению
c) График отпусков персонала
d) Реквизиты поставщиков канцтоваров

Ответ: b) Перечень уязвимостей и меры по их устранению

4. Какой документ фиксирует порядок реагирования на инциденты ИБ?
a) Регламент антивирусной защиты
b) Политика реагирования на инциденты
c) Договор с интернет-провайдером
d) Штатное расписание
Ответ: b) Политика реагирования на инциденты

5. Что включает в себя программа проведения внутреннего аудита ИБ?
a) Проверку соответствия политикам и стандартам
b) Обучение сотрудников работе в Excel
c) Закупку нового оборудования
d) Организацию корпоратива
Ответ: a) Проверку соответствия политикам и стандартам

6. Какой документ регламентирует порядок доступа сотрудников к конфиденциальной информации?
a) Положение о коммерческой тайне
b) Трудовой договор
c) Должностная инструкция
d) Все перечисленные
Ответ: d) Все перечисленные

7. Какой из перечисленных элементов НЕ входит в проект плана по обеспечению ИБ?
a) Анализ рисков
b) Мероприятия по защите данных
c) Бюджет на праздничные мероприятия
d) Контроль выполнения требований
Ответ: c) Бюджет на праздничные мероприятия

8. Какой документ определяет порядок резервного копирования данных?
a) Регламент резервного копирования
b) Политика парольной защиты
c) Инструкция по пожарной безопасности
d) Договор аренды помещения
Ответ: a) Регламент резервного копирования

9. Какой этап работ по защите информации включает разработку политик и регламентов?
a) Подготовительный
b) Эксплуатационный
c) Завершающий
d) Контрольный
Ответ: a) Подготовительный

10. Какой документ фиксирует зоны ответственности за ИБ в организации?
a) Положение о подразделении ИБ
b) Приказ о распределении обязанностей
c) Должностные инструкции
d) Все перечисленные
Ответ: d) Все перечисленные

11. Какой из перечисленных документов НЕ относится к проектной документации по ИБ?
a) Техническое задание на СЗИ
b) Отчет о проведенном аудите
c) Программа тестирования защитных мер

d) План эвакуации при пожаре
Ответ: d) План эвакуации при пожаре

12. Какой раздел должен быть в программе обучения сотрудников по ИБ?
a) Основы защиты персональных данных
b) Правила использования корпоративной почты
c) Действия при обнаружении угроз
d) Все перечисленные
Ответ: d) Все перечисленные

13. Какой документ определяет порядок уничтожения носителей информации?
a) Регламент уничтожения данных
b) Политика хранения архивов
c) Инструкция по уборке офиса
d) Договор с клининговой компанией
Ответ: a) Регламент уничтожения данных

14. Какой элемент НЕ включается в проект плана по защите информации?
a) Сроки выполнения мероприятий
b) Ответственные лица
c) Бюджет на реализацию
d) Меню столовой
Ответ: d) Меню столовой

15. Какой документ регламентирует порядок работы с персональными данными?
a) Политика обработки ПДн
b) Положение о работе с клиентами
c) Регламент доступа в интернет
d) Инструкция по охране труда
Ответ: a) Политика обработки ПДн

ПК-3 Способен осуществить выполнение экспериментов и оформить результаты исследований и разработок

1. Какой этап эксперимента по оценке уязвимостей включает сбор данных о системе?
a) Подготовительный
b) Аналитический
c) Завершающий
d) Документирование
Ответ: a) Подготовительный

2. Какой метод используется для оценки эффективности защитных механизмов?
a) Тестирование на проникновение
b) Анкетирование сотрудников
c) Анализ финансовой отчетности
d) Проверка графика отпусков
Ответ: a) Тестирование на проникновение

3. Какой документ фиксирует результаты тестирования системы на уязвимости?
a) Акт проведенных работ
b) Отчет об обнаруженных уязвимостях
c) Протокол испытаний
d) Все перечисленные
Ответ: d) Все перечисленные

4. Какой инструмент НЕ используется для сбора данных при исследовании ИБ?
a) Nmap

b) Wireshark
c) Metasploit
d) Microsoft Excel (без специализированных надстроек)
Ответ: d) Microsoft Excel (без специализированных надстроек)

5. Какой раздел должен быть в отчете о проведенном эксперименте по ИБ?
a) Цели и задачи исследования
b) Методология тестирования
c) Полученные результаты
d) Все перечисленные
Ответ: d) Все перечисленные

6. Какой метод применяется для моделирования атак на информационную систему?
a) Социальный опрос
b) Red Teaming
c) Анализ логов
d) Инвентаризация оборудования
Ответ: b) Red Teaming

7. Какой параметр оценивается при тестировании стойкости паролей?
a) Длина и сложность
b) Частота смены
c) Цвет интерфейса ввода
d) Количество попыток ввода
Ответ: a) Длина и сложность

8. Какой этап эксперимента включает обработку и визуализацию данных?
a) Подготовка
b) Проведение исследований
c) Анализ результатов
d) Документирование
Ответ: c) Анализ результатов

9. Какой инструмент используется для анализа сетевого трафика?
a) Wireshark
b) Nessus
c) John the Ripper
d) Gimp
Ответ: a) Wireshark

10. Какой вид тестирования позволяет выявить ошибки в логике работы ПО?
a) Функциональное тестирование
b) Юзабилити-тестирование
c) Нагрузочное тестирование
d) A/B-тестирование
Ответ: a) Функциональное тестирование

11. Какой метод НЕ относится к исследованиям в области ИБ?
a) Анализ исходного кода
b) Стресс-тестирование системы
c) Изучение мнения сотрудников о корпоративной культуре
d) Проверка конфигурации firewall
Ответ: c) Изучение мнения сотрудников о корпоративной культуре

12. Какой документ содержит рекомендации по устранению уязвимостей?
a) Отчет о тестировании

b) Политика безопасности
c) Техническое задание
d) Штатное расписание
Ответ: a) Отчет о тестировании

13. Какой показатель оценивается при анализе эффективности системы обнаружения вторжений (IDS)?
a) Количество ложных срабатываний
b) Скорость работы интернета
c) Количество сотрудников в компании
d) Размер бюджета отдела ИБ
Ответ: a) Количество ложных срабатываний

14. Какой этап эксперимента предполагает сравнение результатов с эталонными значениями?
a) Проведение измерений
b) Верификация данных
c) Подготовка оборудования
d) Написание отчета
Ответ: b) Верификация данных

15. Какой инструмент используется для автоматизированного сканирования уязвимостей?
a) OpenVAS
b) Photoshop
c) Microsoft Word
d) 1С:Бухгалтерия
Ответ: a) OpenVAS

ПК-5 Способен выполнять работы по созданию (модификации), управлению и сопровождению ИТ-решений, с использованием современных языков программирования, пакетов прикладных программ моделирования методов параллельной обработки данных

1. Какой язык программирования чаще всего используется для разработки криптографических алгоритмов?
a) Python
b) JavaScript
c) HTML
d) SQL
Ответ: a) Python

2. Какой метод параллельной обработки данных позволяет ускорить выполнение операций шифрования?
a) Многопоточность
b) Линейное программирование
c) Рекурсия
d) ООП
Ответ: a) Многопоточность

3. Какой инструмент используется для моделирования угроз информационной безопасности?
a) MATLAB
b) Microsoft Word
c) Adobe Photoshop
d) AutoCAD
Ответ: a) MATLAB

4. Какой из перечисленных пакетов прикладных программ используется для анализа защищенности сетей?

a) Wireshark
b) Microsoft Excel
c) CorelDRAW
d) PowerPoint
Ответ: a) Wireshark

5. Какой язык программирования наиболее подходит для разработки систем обнаружения вторжений (IDS)?
a) C++
b) HTML
c) CSS
d) PHP
Ответ: a) C++

6. Какой метод параллельной обработки данных используется в распределенных системах защиты информации?
a) MapReduce
b) Bubble Sort
c) Binary Search
d) Quick Sort
Ответ: a) MapReduce

7. Какой инструмент позволяет моделировать атаки на информационные системы для тестирования их защищенности?
a) Metasploit
b) Photoshop
c) AutoCAD
d) Microsoft Word
Ответ: a) Metasploit

8. Какой язык программирования используется для написания скриптов автоматизации задач информационной безопасности?
a) Bash
b) HTML
c) CSS
d) SQL
Ответ: a) Bash

9. Какой пакет прикладных программ используется для моделирования и анализа алгоритмов шифрования?
a) SageMath
b) Microsoft Excel
c) Adobe Illustrator
d) PowerPoint
Ответ: a) SageMath

10. Какой метод параллельной обработки данных применяется для ускорения обработки больших объемов логов безопасности?
a) Apache Spark
b) Bubble Sort
c) Binary Search
d) Quick Sort
Ответ: a) Apache Spark

11. Какой язык программирования используется для разработки веб-приложений с высокими требованиями к безопасности?

a) Java
b) HTML
c) CSS
d) SQL
Ответ: a) Java

12. Какой инструмент используется для моделирования и анализа рисков информационной безопасности?
a) RiskLens
b) Microsoft Paint
c) Adobe Photoshop
d) AutoCAD
Ответ: a) RiskLens

13. Какой метод параллельной обработки данных используется для обработки транзакций в блокчейн-системах?
a) Консенсусные алгоритмы
b) Bubble Sort
c) Binary Search
d) Quick Sort
Ответ: a) Консенсусные алгоритмы

14. Какой язык программирования используется для разработки модулей межсетевых экранов (firewall)?
a) C
b) HTML
c) CSS
d) SQL
Ответ: a) C

15. Какой пакет прикладных программ используется для моделирования и анализа сетевых атак?
a) GNS3
b) Microsoft Excel
c) Adobe Illustrator
d) PowerPoint
Ответ: a) GNS3

ПК-7 Осуществляет концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности

1. Какой этап проектирования ИБ-системы включает определение основных угроз и рисков?
a) Концептуальное проектирование
b) Физическое проектирование
c) Реализация
d) Тестирование
Ответ: a) Концептуальное проектирование

2. Какой документ является основным при концептуальном проектировании системы защиты информации?
a) Техническое задание
b) Политика информационной безопасности
c) Проект архитектуры системы
d) Все перечисленные

Ответ: d) Все перечисленные

3. Какой принцип проектирования ИБ-систем предполагает разделение полномочий пользователей?
a) Принцип минимальных привилегий
b) Принцип избыточности
c) Принцип эшелонированной обороны
d) Принцип открытости
Ответ: a) Принцип минимальных привилегий

4. Какой компонент НЕ входит в типовую архитектуру системы защиты информации крупного предприятия?
a) Подсистема идентификации и аутентификации
b) Подсистема мониторинга и аудита
c) Подсистема управления персоналом
d) Подсистема криптографической защиты
Ответ: c) Подсистема управления персоналом

5. Какой метод используется для оценки рисков при проектировании ИБ-систем?
a) SWOT-анализ
b) FMEA-анализ
c) Анализ дерева угроз
d) Все перечисленные
Ответ: d) Все перечисленные

6. Какой стандарт чаще всего используется при проектировании систем управления информационной безопасностью?
a) ISO 27001
b) ISO 9001
c) GOST R 34.10-2012
d) PCI DSS
Ответ: a) ISO 27001

7. Какой элемент НЕ относится к функциональным требованиям при проектировании ИБ-системы?
a) Поддержка многофакторной аутентификации
b) Производительность системы
c) Интеграция с Active Directory
d) Соответствие бюджету проекта
Ответ: d) Соответствие бюджету проекта

8. Какой подход к проектированию ИБ-систем предполагает создание нескольких уровней защиты?
a) Эшелонированная оборона
b) Минималистичный подход
c) Реактивный подход
d) Децентрализованный подход
Ответ: a) Эшелонированная оборона

9. Какой компонент является ключевым в логическом проектировании системы контроля доступа?
a) Матрица доступа
b) Журнал событий
c) Резервная копия
d) Антивирусное ПО
Ответ: a) Матрица доступа

10. Какой документ фиксирует архитектурные решения при проектировании ИБ-системы?

a) Проект архитектуры безопасности
b) Техническое задание
c) Политика безопасности
d) Регламент администрирования
Ответ: a) Проект архитектуры безопасности

11. Какой метод проектирования предполагает создание прототипа системы безопасности?
a) Итеративная разработка
b) Водопадная модель
c) Agile
d) Spiral model
Ответ: d) Spiral model

12. Какой показатель НЕ учитывается при проектировании отказоустойчивых ИБ-систем?
a) Время восстановления после сбоя
b) Стоимость лицензий ПО
c) Коэффициент готовности
d) Допустимое время простоя
Ответ: b) Стоимость лицензий ПО

13. Какой компонент должен быть обязательно включен в архитектуру распределенной ИБ-системы?
a) Центр мониторинга безопасности
b) Локальные агенты сбора данных
c) Единая система аутентификации
d) Все перечисленные
Ответ: d) Все перечисленные

14. Какой стандарт описывает лучшие практики проектирования систем управления доступом?
a) ISO/IEC 27002
b) NIST SP 800-53
c) PCI DSS
d) Все перечисленные
Ответ: d) Все перечисленные

15. Какой принцип проектирования ИБ-систем предполагает разделение производственных и тестовых сред?
a) Принцип изоляции
b) Принцип минимальных привилегий
c) Принцип глубины защиты
d) Принцип открытости
Ответ: a) Принцип изоляции

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