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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

20.03.2026г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.10 Комплексное обеспечение безопасности компьютерных систем и сетей

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

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

7. Рекомендована:
НМС факультета ПММ, протокол № 5 от 17.03.2025г.
Внесены изменения: НМС факультета ПММ, протокол № 5 от 20.03.2026г.

8. Учебный год: 2029/2030 **Семестр(ы):** 9

9. Цели и задачи учебной дисциплины

Изучение средств обеспечения безопасности проводных и беспроводных сетей, видов угроз и атак, осуществляемых на проводные и беспроводные сети; встроенных средств аутентификации и методов шифрования данных при передаче по проводным и беспроводным сетям; стандартов сетей и применение широкой линейки оборудования обеспечения безопасности сетей.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к части, формируемой участниками образовательных отношений блока Б1 дисциплин учебного плана.

11. 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-1	Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации	**ПК-1.2**	использует современные математические методы и алгоритмы функционирования при создании компонентов программных средств защиты информации	Знает математические основы криптографии и современные алгоритмы защиты информации. Умеет применять методы алгебры и статистики для расчёта криптостойкости, реализовывать базовые операции эллиптической криптографии, проектировать алгоритмы обнаружения аномалий и контроля целостности. Владеет средствами математического моделирования, техниками прототипирования криптоалгоритмов на языках C/Python с учётом аппаратных ограничений, методами формальной верификации и анализа защищённости алгоритмов от побочных атак.
		ПК-1.3	использует принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения	Знает стандарты Secure SDLC, модели жизненного цикла, принципы комплексной защиты и современный инструментарий разработки. Умеет разрабатывать правила и процедуры безопасности на основе анализа угроз, интегрировать этапы безопасности в конвейеры сборки и тестирования, применять паттерны безопасного проектирования и настраивать автоматические проверки кода и зависимостей. Владеет методами формализации политик безопасности в виде кода, инструментами моделирования угроз, техниками ревью архитектуры, средствами документирования правил и процедур, а также приёмами автоматизации развёртывания защищённых компонентов.
ПК-3	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и	**ПК-3.3**	способен проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности	Знает актуальные стандарты в области компьютерной безопасности, методики анализа рисков и оценки уязвимостей, а также требования к моделям угроз и нарушителя согласно российским и международным нормативным документам. Умеет проводить оценку соответствия компьютерной системы требованиям стандартов, формировать модель

	прикладных задач			угроз, применять чек-листы и методики CVSS для ранжирования рисков, а также интерпретировать результаты инструментального сканирования в терминах несоответствий стандартам. Владеет инструментами анализа защищённости, методами документирования результатов аудита, технологиями автоматизированной проверки соответствия и навыками подготовки нормативно обоснованных рекомендаций по устранению уязвимостей.
		ПК-3.6	способен участвовать в проектировании системы защиты информации и подсистем информационной безопасности компьютерной системы	Знает типовую архитектуру систем защиты информации, методологии проектирования и нормативные требования ФСТЭК России к СЗИ, а также состав проектной документации. Умеет анализировать защищаемую компьютерную систему для определения точек внедрения СЗИ, формулировать требования к подсистемам ИБ на основе модели угроз, выбирать конкретные программно-аппаратные средства защиты с учётом совместимости и сертификации, разрабатывать логические схемы взаимодействия компонентов и участвовать в подготовке разделов проектной документации. Владеет инструментами моделирования, методами обоснования архитектурных решений перед заказчиком, технологиями развёртывания тестовых стендов СЗИ, приёмами итеративного уточнения проекта при изменении исходных данных и навыками оформления проектной документации по стандартам ЕСПД.

12. Объем дисциплины в зачетных единицах/час – 4/144.
Форма промежуточной аттестации – зачет с оценкой.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			9			
Аудиторные занятия	60		60			
в том числе: лекции	36		36			
Практические	0		0			
Лабораторные	36		36			
Самостоятельная работа	72		72			
Контроль	0		0			
Итого:	144		144			
Форма промежуточной аттестации	Зачет с оценкой		Зачет с оценкой			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основные понятия и концепции информационной безопасности	Понятийный аппарат: информация, угрозы, уязвимости, риски. Определение безопасности, триада CIA + аутентичность. Модели безопасности: политики безопасности. Классические формальные модели. Нарушитель и угрозы: типы нарушителей, источники угроз, векторы атак. Понятие модели угроз.	
1.2	Криптографические методы защиты информации	Основы криптографии: симметричное и асимметричное шифрование. Хэш-функции и электронная подпись: MD5, SHA-1/2/3, ГОСТ Р 34.11-2012. Принципы формирования и проверки ЭЦП. Управление ключами: генерация, распределение, хранение ключей. Инфраструктура открытых ключей, сертификаты X.509.	
1.3	Безопасность сетевой инфраструктуры	Сетевые атаки: анализ протоколов, ARP/ DNS-спуфинг, сниффинг, DoS/ DDoS-атаки, атаки man-in-the-middle. Сетевые защитные устройства: межсетевые экраны и их типы, системы обнаружения и предотвращения вторжений, прокси-серверы. Защищенные протоколы: IPSec, SSL/TLS, SSH, протоколы защищенной аутентификации.	
1.4	Безопасность операционных систем и ПО	Механизмы защиты ОС: управление доступом, изоляция процессов, безопасность памяти, привилегированные режимы. Принцип наименьших привилегий. Анализ уязвимостей ПО: переполнение буфера, гонка состояний, форматные строки. Безопасность веб-приложений: OWASP Top 10, инъекции, XSS, CSRF, небезопасная десериализация.	
1.5	Вредоносное программное обеспечение	Классификация вредоносного кода: вирусы, черви, трояны, руткиты, бэкдоры, ransomware, spyware. Методы противодействия: антивирусные комплексы, песочницы, белые списки приложений.	
1.6	Комплексная защита и управление рисками	Анализ рисков: количественная и качественная оценка рисков. Методологии. Политики и процедуры безопасности: разработка политик паролей, управления доступом, реагирования на инциденты. Управление уязвимостями. Мониторинг и аудит: системы сбора и корреляции событий, логирование,	

		анализ журналов. Понятие форензики.	
1.7	Организационные и правовые аспекты	Нормативная база РФ: ключевые требования ФСТЭК России, ФСБ России, Приказы Минкомсвязи. Стандарты: ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 15408. Безопасность и человек: социальная инженерия, вопросы удобства использования, обучение персонала.	
2. Лабораторные работы			
2.1	**Лабораторная работа №1: Реализация криптографических методов защиты информации**	***1.1.*** *Реализация симметричного шифрования* • Шифрование/дешифрование файлов средствами OpenSSL. • Режимы шифрования. • Эксперимент с распространением ошибки в режиме CBC. ***1.2.*** *Асимметричная криптография и ЭП* • Генерация ключевых пар. • Подписание и проверка электронной подписи. • Шифрование сессионного ключа асимметричным алгоритмом.	
2.2	**Лабораторная работа №2: Инфраструктура открытых ключей**	• Создание собственного удостоверяющего центра. • Выпуск и подпись сертификатов. • Настройка HTTPS на веб-сервере с самоподписным сертификатом.	
2.3	**Лабораторная работа №3: Атака на протокол Диффи — Хеллмана**	• Перехват и подмена ключей в учебной среде. • Обнаружение атаки и способы защиты.	
2.4	**Лабораторная работа №4: Безопасность сетевой инфраструктуры**	***4.1.*** *Анализ сетевого трафика* • Захват и фильтрация трафика. • Выявление атак ARP-spoofing, DNS-spoofing. • Восстановление передаваемых файлов из pcap. ***4.2.*** *Настройка межсетевого экрана* • Создание правил фильтрации. • Настройка NAT и маскарадинга. • Логирование отклонённых пакетов. ***4.3.*** *Обнаружение и предотвращение вторжений* • Установка IDS/IPS. • Написание простых сигнатур для обнаружения сканирования портов. • Анализ оповещений.	
2.5	**Лабораторная работа №5: Моделирование безопасности сетевой инфраструктуры**	***5.1.*** *Настройка защищённых протоколов* • Построение VPN между двумя хостами. • Настройка туннельного и транспортного режима IPsec. • Проброс портов через SSH. ***5.2.*** *Моделирование DDoS-атаки и защита* • Генерация SYN-flood. • Настройка защиты. • Анализ эффективности защиты.	
2.6	**Лабораторная работа №6: Эксплуатация уязвимостей**	***6.1.*** *Эксплуатация уязвимости переполнения буфера* • Компиляция уязвимой программы. • Внедрение шелл-кода. • Обход механизмов защиты. ***6.2.*** *SQL-инъекции (на учебном стенде)* • Обход аутентификации. • Извлечение данных через UNION-запросы. • Защита через параметризованные запросы и экранирование. ***6.3.*** *XSS и CSRF-атаки* • Рефлекторный и хранимый XSS. • Кража cookie через XSS. • CSRF-атака на смену пароля. • Защита.	

2.7	**Лабораторная работа №7: Анализ защищённости ОС и ПО**	• Сканирование сети и обнаружение открытых портов. • Поиск уязвимостей с использованием баз CVE. • Формирование отчёта и рекомендаций.	
2.8	**Лабораторная работа №8: Анализ вредоносного ПО и антивирусная защита**	***8.1.*** *Создание и анализ простого вредоносного кода в изолированной среде* • Написание программы, которая модифицирует реестр/файлы. • Сравнение сигнатурного и эвристического обнаружения. ***8.2.*** *Статический и динамический анализ подозрительных файлов* • Использование песочниц. • Анализ энтропии файла. • Отслеживание системных вызовов. ***8.3.*** *Настройка антивирусной защиты* • Конфигурация политик сканирования. • Создание исключений и проверка их обхода. • Централизованное управление.	
2.9	**Лабораторная работа №9: Управление рисками и SIEM**	***9.1.*** *Расчёт рисков* • Оценка активов, угроз, уязвимостей. • Расчёт SLE, ARO, ALE для заданного сценария. • Построение матрицы рисков. ***9.2.*** *Настройка сбора и корреляции событий* • Установка агентов на хосты. • Централизованный сбор логов. • Создание правил корреляции. ***9.3.*** *Основы компьютерной форензики* • Создание образа диска. • Поиск удалённых файлов. • Анализ временных меток.	
2.10	**Лабораторная работа №10: Моделирование комплексной защиты сети**	***10.1.*** *Анализ защищённости учебной сети* • Студенты делятся на «красную» и «синюю» команды. • Задание «синим»: настроить firewall, IDS, антивирус, политики доступа. • Задание «красным»: провести сканирование, попытаться выполнить SQLi, XSS, подобрать пароли. ***10.2.*** *Формирование отчёта о безопасности и плана устранения уязвимостей* • Документирование найденных проблем. • Приоритизация рисков. • Рекомендации по аппаратно-программным компонентам.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Основные понятия и концепции информационной безопасности	4	0	0	8	0	12
1.2	Криптографические методы защиты информации	4	0	6	10	0	20
1.3	Безопасность сетевой инфраструктуры	6	0	8	10	0	24
1.4	Безопасность операционных систем и ПО	6	0	8	10	0	24

1.5	Вредоносное программное обеспечение	6	0	6	10	0	22
1.6	Комплексная защита и управление рисками	6	0	8	12	0	26
1.7	Организационные и правовые аспекты	4	0	0	12	0	16
	Итого:	36		36	72	0	144

14. 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.

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

а) основная литература:

№ п/п	Источник
1	Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург: Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/370967 — Режим доступа: для авториз. пользователей.
2	Баланов, А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — 3-е изд., стер. — Санкт-Петербург: Лань, 2026. — 280 с. — ISBN 978-5-507-56255-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/514704 — Режим доступа: для авториз. пользователей.
3	Основы информационной безопасности: учебное пособие / составитель С. П. Середкин. — Иркутск: ИрГУПС, 2024. — 80 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/458102. — Режим доступа: для авториз. пользователей.
4	Краковский, Ю. М. Методы и средства защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 2-е изд., стер. — Санкт-Петербург: Лань, 2025. — 272 с. — ISBN 978-5-507-52958-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/463013. — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
5	Баланов, А. Н. Комплексная информационная безопасность: учебное пособие для вузов / А. Н. Баланов. — 2-е изд., стер. — Санкт-Петербург: Лань, 2025. — 400 с. — ISBN 978-5-507-52839-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/460715 — Режим доступа: для авториз. пользователей.
6	Ярочкин, В. И. Информационная безопасность: учебник / В. И. Ярочкин. — 5-е изд. — Москва: Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242. — Режим доступа: для авториз. пользователей.

7	Ермакова, А. Ю. Методы и средства криптографической защиты информации: учебное пособие / А. Ю. Ермакова, В. В. Лебедев. — Москва: РТУ МИРЭА, 2024. — 230 с. — ISBN 978-5-7339-2152-5. — Текс : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/420980. — Режим доступа: для авториз. пользователей.
8	Мосолов, А. С. Компьютерные технологии и методы проектирования в сфере безопасности: Учебник для вузов / А. С. Мосолов, Н. И. Акинин. — Санкт-Петербург: Лань, 2021. — 444 с. — ISBN 978-5-8114-8034-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/183115. — Режим доступа: для авториз. пользователей.

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

№ п/п	Источник
9	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
10	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
11	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». —— Режим доступа: https://edu.vsu.ru

16. 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.

17. 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.10 Комплексное обеспечение безопасности компьютерных систем и сетей (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, Linux набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. 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	Основные понятия и концепции информационной безопасности	ПК-1	ПК-1.2	устный опрос, тест
			ПК-1.3	устный опрос, тест, лабораторная работа
2	Криптографические методы защиты информации	ПК-1	ПК-1.2	устный опрос, тест, лабораторная работа
			ПК-1.3	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.6	устный опрос, тест, лабораторная работа
3	Безопасность сетевой инфраструктуры	ПК-1	ПК-1.3	устный опрос, тест, лабораторная работа
		ПК-3	ПК-3.3	
			ПК-3.6	
4	Безопасность операционных систем и ПО	ПК-1	ПК-1.2	устный опрос, тест, лабораторная работа
			ПК-1.3	
		ПК-3	ПК-3.3	устный опрос, тест, лабораторная работа
			ПК-3.6	
5	Вредоносное программное обеспечение	ПК-3	ПК-3.3	устный опрос, тест, лабораторная работа
6	Комплексная защита и управление рисками	ПК-1	ПК-1.2	устный опрос, тест, лабораторная работа
			ПК-1.3	
		ПК-3	ПК-3.3	
			ПК-3.6	
7	Организационные и правовые аспекты	ПК-3	ПК-3.3	устный опрос, тест
			ПК-3.6	
Промежуточная аттестация, форма контроля – зачет с оценкой				Перечень вопросов (КИМ№1)

ПК-1Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации	**ПК-1.2**	использует современные математические методы и алгоритмы функционирования при создании компонентов программных средств защиты информации
	ПК-1.3	использует принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения
ПК-3 Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач	**ПК-3.3**	способен проводить анализ безопасности компьютерных систем с использованием актуальных стандартов в области компьютерной безопасности
	ПК-3.6	способен участвовать в проектировании системы защиты информации и подсистем информационной безопасности компьютерной системы

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: Реализация криптографических методов защиты информации**	***1.1.*** *Реализация симметричного шифрования* • Шифрование/дешифрование файлов средствами OpenSSL. • Режимы шифрования. • Эксперимент с распространением ошибки в режиме CBC. ***1.2.*** *Асимметричная криптография и ЭП* • Генерация ключевых пар. • Подписание и проверка электронной подписи. Шифрование сессионного ключа асимметричным алгоритмом.
2	**Лабораторная работа №2: Инфраструктура открытых ключей**	• Создание собственного удостоверяющего центра. • Выпуск и подпись сертификатов. Настройка HTTPS на веб-сервере с самоподписным сертификатом.
3	**Лабораторная работа №3: Атака на протокол Диффи — Хеллмана**	• Перехват и подмена ключей в учебной среде. Обнаружение атаки и способы защиты.
4	**Лабораторная работа №4: Безопасность сетевой инфраструктуры**	***4.1.*** *Анализ сетевого трафика* • Захват и фильтрация трафика. • Выявление атак ARP-spoofing, DNS-spoofing. • Восстановление передаваемых файлов из pcap. ***4.2.*** *Настройка межсетевого экрана* • Создание правил фильтрации. • Настройка NAT и маскарадинга. • Логирование отклонённых пакетов. ***4.3.*** *Обнаружение и предотвращение вторжений* • Установка IDS/IPS. • Написание простых сигнатур для обнаружения сканирования портов. Анализ оповещений.
5	**Лабораторная работа №5: Моделирование безопасности сетевой инфраструктуры**	***5.1.*** *Настройка защищённых протоколов* • Построение VPN между двумя хостами. • Настройка туннельного и транспортного режима IPsec. • Проброс портов через SSH. ***5.2.*** *Моделирование DDoS-атаки и защита* • Генерация SYN-flood. • Настройка защиты. Анализ эффективности защиты.
6	**Лабораторная работа №6: Эксплуатация уязвимостей**	***6.1.*** *Эксплуатация уязвимости переполнения буфера* • Компиляция уязвимой программы. • Внедрение шелл-кода. • Обход механизмов защиты. ***6.2.*** *SQL-инъекции (на учебном стенде)* • Обход аутентификации. • Извлечение данных через UNION-запросы. • Защита через параметризованные запросы и экранирование. ***6.3.*** *XSS и CSRF-атаки* • Рефлекторный и хранимый XSS. • Кража cookie через XSS. • CSRF-атака на смену пароля. Защита.
7	**Лабораторная работа №7: Анализ защищённости ОС и ПО**	• Сканирование сети и обнаружение открытых портов. • Поиск уязвимостей с использованием баз CVE. Формирование отчёта и рекомендаций.
8	**Лабораторная работа №8: Анализ вредоносного ПО и антивирусная защита**	***8.1.*** *Создание и анализ простого вредоносного кода в изолированной среде* • Написание программы, которая модифицирует реестр/файлы. • Сравнение сигнатурного и эвристического обнаружения. ***8.2.*** *Статический и динамический анализ подозрительных файлов* • Использование песочниц. • Анализ энтропии файла. • Отслеживание системных вызовов. ***8.3.*** *Настройка антивирусной защиты* • Конфигурация политик сканирования. • Создание исключений и проверка их обхода. Централизованное управление.

9	**Лабораторная работа №9: Управление рисками и SIEM**	***9.1.*** *Расчёт рисков* • Оценка активов, угроз, уязвимостей. • Расчёт SLE, ARO, ALE для заданного сценария. • Построение матрицы рисков. ***9.2.*** *Настройка сбора и корреляции событий* • Установка агентов на хосты. • Централизованный сбор логов. • Создание правил корреляции. ***9.3.*** *Основы компьютерной форензики* • Создание образа диска. • Поиск удалённых файлов. Анализ временных меток.
10	**Лабораторная работа №10: Моделирование комплексной защиты сети**	***10.1.*** *Анализ защищённости учебной сети* • Студенты делятся на «красную» и «синюю» команды. • Задание «синим»: настроить firewall, IDS, антивирус, политики доступа. • Задание «красным»: провести сканирование, попытаться выполнить SQLi, XSS, подобрать пароли. ***10.2.*** *Формирование отчёта о безопасности и плана устранения уязвимостей* • Документирование найденных проблем. • Приоритизация рисков. Рекомендации по аппаратно-программным компонентам.

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 представленнойчасти много ошибок

20.2 Промежуточная аттестация

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

Перечень вопросов к экзамену (КИМ №1)

1. Дайте определение понятиям «конфиденциальность», «целостность», «доступность». Приведите пример нарушения каждого свойства.
2. Чем отличается дискреционная модель управления доступом от мандатной? Опишите основное различие на примере.
3. В чём суть модели Белла — ЛаПадулы? Какое свойство безопасности она обеспечивает?
4. Что такое ролевая модель управления доступом? На каких трёх принципах она строится?
5. Какие виды нарушителей выделяют в теории информационной безопасности?
6. Что входит в понятие «модель угроз»? Какие разделы должна содержать корректная модель угроз для компьютерной системы?
7. Чем отличаются уязвимость, угроза и риск? Приведите цепочку «актив → угроза → уязвимость → риск».
8. В чём принципиальное различие между симметричным и асимметричным шифрованием? Приведите по одному примеру алгоритмов для каждого типа.
9. Какое конечное поле используется в алгоритме AES? Как выполняются операции умножения и сложения в GF?
10. Что такое эллиптическая криптография? Сформулируйте задачу дискретного логарифмирования на эллиптической кривой.

11. Для чего нужны хэш-функции? Назовите три основных требования, предъявляемых к криптографическим хэш-функциям.

12. Чем отличается электронная подпись от кода аутентичности сообщения?

13. Что такое инфраструктура открытых ключей? Какие компоненты входят в PKI и какова роль удостоверяющего центра?

14. Как работает алгоритм Диффи — Хеллмана для выработки общего секретного ключа? Какая математическая проблема лежит в его основе?

15. Что такое криптостойкость? Как оценивается сложность атаки полным перебором для ключа длиной 128 бит?

16. Что такое атака «человек посередине» и какие криптографические протоколы ей подвержены?

17. Назовите российские стандарты шифрования и хэширования. Чем отличается «Кузнечик» от «Магмы»?

18. Какие типы межсетевых экранов существуют? В чём отличие пакетного фильтра от прокси-сервера?

19. Чем система обнаружения вторжений отличается от системы предотвращения вторжений?

20. Опишите принцип работы протокола SSL/TLS. Какой алгоритм используется для установления сессионного ключа?

21. Какие уязвимости протокола ARP существуют и как с ними бороться?

22. Что такое DoS- и DDoS-атаки? Приведите примеры.

23. Какие защищённые протоколы используются для удалённого доступа? Чем отличается транспортный режим IPsec от туннельного?

24. Как работает протокол Kerberos? Опишите роль KDC, TGT и сервера приложений.

25. Что такое VLAN? Как VLAN повышает безопасность сети и какие существуют атаки на VLAN?

26. Какие механизмы защиты операционных систем вы знаете? Опишите разделение на пользовательский и привилегированный режимы.

27. Что такое переполнение буфера? Как этот тип уязвимости может привести к выполнению произвольного кода?

28. Какие методы защиты от переполнения буфера существуют?

29. Что такое SQL-инъекция? Приведите пример вредоносной строки и способ защиты через параметризованные запросы.

30. В чём суть XSS-атаки? Чем отличаются хранимые и отражённые XSS?

31. Что такое CSRF? Какой токен защищает от этой атаки?

32. Как в ОС Linux реализовано мандатное управление доступом? Что такое контекст безопасности?

33. Что такое принцип наименьших привилегий и как он применяется при проектировании безопасного ПО?

34. Перечислите основные типы вредоносного ПО. В чём ключевые различия между вирусом и червём?

35. Что такое ransomware? Как происходит заражение и какие существуют методы противодействия?

36. Какие методы обнаружения вредоносного ПО используются в антивирусах?

37. Что такое песочница? Как она помогает анализировать подозрительные файлы?

38. Как работают упаковщики и обфускация кода? Какой математический метод помогает выявить упакованный код?

39. Что такое rootkit? На каких уровнях могут работать руткиты?

40. Как работает ботнет? Что такое C&C-сервер и какие протоколы используются для управления ботами?

41. Что такое анализ рисков? Чем отличается количественный метод от качественного?

42. Как рассчитывается ожидаемый годовой ущерб и из каких компонентов он состоит? Приведите формулу.

43. Что такое SIEM-система? Какие функции она выполняет?

44. Что такое компьютерная форензика? Какие этапы включает процесс сбора и анализа цифровых доказательств?

45. Какие метрики безопасности используются для оценки эффективности СЗИ?

46. Что такое метод Монте-Карло и как он применяется для моделирования рисков информационной безопасности?

47. Назовите основные регуляторы в сфере информационной безопасности РФ и их полномочия.

48. Что устанавливает стандарт ГОСТ Р ИСО/МЭК 27001? Какие разделы включает система менеджмента информационной безопасности?

49. Какие требования предъявляет ФСТЭК России к средствам защиты информации для государственных информационных систем?

50. Что такое социальная инженерия? Приведите примеры атак и методы защиты от них.

Критерии оценки ответов на экзаменационные вопросы

Для оценивания результатов обучения на зачете с оценкой используется – 4-балльная шала:
«отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.
Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

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

ПК-1. Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации.

1. По принципу Киркгофа в криптосистеме секретным должно быть:
   - Ключ
   - Алгоритм шифрования
   - Язык (алфавит) сообщения
   - Длина ключа

2. Как называется функция, эффективно вычисляемая за полиномиальное время на детерминированной машине Тьюринга, для которой не существует полиномиальной

вероятностной машины Тьюринга, которая обращает функцию?

- Невычислимая
- Односторонняя
- Полиномиальная
- Экспоненциальная
- Вероятностная

3. В чем преимущество симметричных систем над асимметричными?

- скорость шифрования
- меньшая требуемая длина ключа для сопоставимой стойкости
- простота обмена ключами
- простота реализации
- простота управления ключами в большой сети
- изученность

4. Каким свойством должен обладать канал передачи информации в схеме обмена ключами Диффи-Хеллмана

- защищенный от подмены
- защищенный от прослушивания
- закрытый канал
- с высокой пропускной способностью

5. Критический путь, это:

a. Наиболее короткий путь между началом работ и их окончанием;
b. Полный путь, имеющий наибольшую продолжительность;
c. Путь с наибольшим количеством работ

6. Какие варианты закрытых вопросов существуют?

a. Многовариантного выбора
b. Дихотомические
c. Параметрические

7.Наименее подходящим стилем руководства при управлении в условии экстремальных ситуаций является:

a. Авторитарный
b. Демократический
c. Либеральный

8. В основе передачи информации по ВОЛС лежит….

1) Дисперсия
2) Дифракция
3) Интерференция
4) Отражение

9. В волоконно-оптических линиях связи для передачи информации используется….

1. Инфракрасная область спектра
2. Область видимого света
3. Радиоволны
4. Ультрафиолетовая область спектра

10. Прочность защиты в АС

1) вероятность не преодоления защиты нарушителем за установленный промежуток времени

2) способность системы защиты информации обеспечить достаточный уровень своей безопасности

3) группа показателей защиты, соответствующая определенному классу защиты

11. Уровень секретности — это

1) ответственность за модификацию и НСД информации

2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

12. Угроза — это

1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов

2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

13. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации, называется…

1) кодируемой
2) шифруемой
3) недостоверной
4) защищаемой

14. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Запишите ответ: _____

15. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

1) системой угроз;
2) системой защиты;
3) системой безопасности;
4) системой уничтожения.

16. К архитектурным свойствам ВС относится…

- объем ОЗ
- надежность и живучесть
- количество процессоров и вычислительных блоков
- объем дисковой (внешней) памяти

17. К сильносвязанным вычислительным системам относится…

- кластерные ВС
- MPP – системы
- грид-системы
- SMP – системы

18. Предоставление вычислительных систем, хранилищ данных, и другого оборудования с возможностью управления по сети Интернет в сфере облачных вычислений называется…

- инфраструктура как сервис (IaaS)
- программное обеспечение как сервис (SaaS)
- платформа как сервис (PaaS)
- всѐ как сервис (AaaS)

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач.

1. Совершенный этап защиты информации называется:
    1. информационным
    2. начальным
    3. развитым
    4. комплексным.
2. Процесс защиты информации в АС измеряется периодом:
    1. 20 – 25 лет
    2. 30 – 35 лет
    3. 35 – 40 лет
    4. 40 – 45 лет
3. Используемые средства защиты информации в АСОД на начальном этапе:
    1. материальные
    2. морально-этические
    3. неформальные
    4. формальные

4. Если информация искажена умышленно, то ее называют:
   1. некачественной
   2. субъективной
   3. неполной
   4. дезинформацией
5. Защита информации в АСОД считается комплексной, если:
   1. реализуется одна цель защиты и используется один вид защиты
   2. реализуется более одной цели защиты и используется более одного вида защиты
   3. реализуются все цели защиты и используются все виды защиты
   4. реализуется более одной цели защиты, но не все и используется более одного вида защиты, но не все
6. Если доступ к информации ограничивается, то такая информация является:
   1. качественной
   2. достоверной
   3. конфиденциальной
   4. ценной
7. Основной объем информации, составляющий базис организации или учреждения:
   1. постоянная информация
   2. медленно меняющаяся информация
   3. техническая информация
   4. быстро меняющаяся информация
8. При информационном обеспечении деятельности предприятия с точки зрения защиты информации предметом наиболее пристального внимания должна быть:
   1. регулирование входных и выходных потоков информации
   2. управление входными потоками информации
   3. формирование и совершенствование информационного кадастра
   4. информационный кадастр и информационные технологии
9. Традиционные меры защиты информации твердых копий:
   1. программные средства
   2. криптографические
   3. соблюдение режима секретности
   4. каровое обеспечение
10. Если носители информации являются электромагнитные волны, то такая информация относится к:
   1. электронной
   2. телекоммуникационной
   3. документальной
   4. речевой
11. Специализация функций АС, где особое значение имеет защита авторского права:
   1. планирование и управление
   2. образование и культура
   3. транспорт и связь
   4. научая и проектная деятельность
12. К какой из составляющих системы защиты информации относятся средства пожарной сигнализации и пожаротушения:
   1. организационной
   2. программной
   3. технической
   4. информационно-лингвистической
13. К какому виду угроз для АС относятся радиоактивное излучение и осадки:
   1. природные
   2. технические
   3. созданные людьми преднамеренно
   4. созданные людьми непреднамеренно
14. При выполнении курсовой или дипломной работы студент может быть допущен к сведениям, имеющим гриф секретности:

1. секретно
2. совершенно секретно
3. особой важности
4. для служебного пользования

15. Орган управления государственной системой защиты информации:
    1. федеральное агентство правительственной связи и информации
    2. федеральная служба контрразведки
    3. гостехкомиссия России
    4. федеральная служба безопасности
16. Что такое информационные ресурсы?
    - Это ресурсы, с помощью которых можно обрабатывать информацию.
    - Это законодательные акты в области информационных технологий.
    - Это отдельные документы и отдельные массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).
17. Какие цели преследует защита информации?
    - цели защиты информации - недопущение "взлома" данных, хранящихся в компьютере.
    - целями защиты информации являются: предотвращение разглашения, утечки и несанкционированного доступа к охраняемым сведениям; предотвращение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы; обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при их разработке, производстве и применении информационных систем, технологии и средств их обеспечения
18. Является ли данное свойство особенностью информации?
    - размерность.
    - непрерывность.
    - дискретность.
    - наглядность.
    - ценность.
19. Что является составной частью концепции и структуры защиты информации?
    - Развитый ассортимент технических средств защиты информации, производимых на промышленной основе.
    - Значительное число имеющих необходимые лицензии организаций, специализирующихся на решении вопросов защиты информации.
    - Большой практический опыт решения проблем в рассматриваемой области.

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