Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«28» 11 2025 г.

Оценочные материалы текущего контроля и промежуточной аттестации
по учебной дисциплине

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности:
09.02.11 Разработка и управление программным обеспечением

Квалификация: программист

Год начала подготовки: 2026

Екатеринбург
2025

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)
Уральский технический институт связи и информатики (филиал) в г. Екатеринбурге
(УрТИСИ СибГУТИ)

Утверждаю
Директор УрТИСИ СибГУТИ
_____ Е.А. Минина
«___» _____ 2025 г.

Оценочные материалы текущего контроля и промежуточной аттестации
по учебной дисциплине

ОП.05 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для специальности:
09.02.11 Разработка и управление программным обеспечением

Квалификация: программист

Год начала подготовки: 2026

Екатеринбург
2025

Оценочные материалы составил:
Каменсков А.Е. - преподаватель ЦК ЭТД кафедры ИТиМС

Одобрено цикловой комиссией
Электротехнических дисциплин
кафедры Инфокоммуникационных
технологий и мобильной связи.
Протокол 3 от 26.11.25
Председатель цикловой комиссии
_____ Е.С. Тарасов

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

Оценочные материалы составил:
Каменсков А.Е. - преподаватель ЦК ЭТД кафедры ИТиМС

Одобрено цикловой комиссией
Электротехнических дисциплин
кафедры Инфокоммуникационных
технологий и мобильной связи.
Протокол ___ от _____
Председатель цикловой комиссии
_____ Е.С. Тарасов

Согласовано
Заместитель директора
по учебной работе
_____ А.Н. Белякова

1 Требования к освоению дисциплины

В результате освоения учебной дисциплины «Основы информационной безопасности» обучающийся должен обладать, предусмотренными ФГОС СПО по специальности 09.02.11 Разработка и управление программным обеспечением, следующими умениями и знаниями:

уметь:

– определять актуальность нормативно-правовой документации в профессиональной деятельности;

– применять современную научную профессиональную терминологию;

– определять и выстраивать траектории профессионального развития и самообразования;

– выявлять достоинства и недостатки коммерческой идеи;

– определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности, выявлять источники финансирования;

– презентовать идеи открытия собственного дела в профессиональной деятельности;

– определять источники достоверной правовой информации;

– составлять различные правовые документы;

– находить интересные проектные идеи, грамотно их формулировать и документировать;

– оценивать жизнеспособность проектной идеи, составлять план проекта;

– понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы;

– участвовать в диалогах на знакомые общие и профессиональные темы;

– строить простые высказывания о себе и о своей профессиональной деятельности;

– кратко обосновывать и объяснять свои действия (текущие и планируемые);

писать простые связные сообщения на знакомые или интересующие профессиональные темы;

– выбирать и применять сетевые топологии и технологии передачи данных для обеспечения масштабируемой надежной отказоустойчивой сетевой инфраструктуры;

– использовать специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;

– анализировать, проектировать и настраивать схемы потоков трафика в компьютерной сети.

знать:

– содержание актуальной нормативно-правовой документации;

– современная научная и профессиональная терминология;

– возможные траектории профессионального развития и самообразования;

– основы предпринимательской деятельности, правовой и финансовой грамотности;

– правила разработки презентации;

– основные этапы разработки и реализации проекта;

– правила построения простых и сложных предложений на профессиональные темы;

– основные общеупотребительные глаголы (бытовая и профессиональная лексика);

– лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности;

– особенности произношения;

– правила чтения текстов профессиональной направленности;

– этапы проектирования сетевой инфраструктуры;

– активное и пассивное оборудование сетей;

– виды кабелей и технические особенности их монтажа;

– специальное программное обеспечение для моделирования, проектирования и тестирования компьютерных сетей;

– технологии обеспечения масштабируемости, надежности и отказоустойчивости сети;

– элементы теории массового обслуживания;

– основы проектирования беспроводных сетей;

– принципы построения высокоскоростных компьютерных сетей.

Указанные умения и знания формируют общие и профессиональные компетенции, представленные таблице 1.

Таблица 1

Индекс компетенции	Наименование компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.
ПК 1.1	Проектировать базы данных.
ПК 1.4	Администрировать базы данных.
ПК 1.5	Защищать информацию в базе данных с использованием технологии защиты информации.
ПК 3.1	Собирать исходные данные для разработки проектной документации на информационную систему.
ПК 3.2	Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.
ПК 3.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

ПК 3.5	Интегрировать информационную систему с существующими информационными системами заказчика.
ПК 3.7	Разрабатывать техническую документацию на эксплуатацию информационной системы.

Формой промежуточной аттестации по дисциплине «Основы информационной безопасности» является дифференцированный зачет.

2 Показатели и критерии оценивания компетенций

В процессе изучения дисциплины осуществляется комплексная проверка следующих результатов обучения (Таблица 2):

Таблица 2

Индекс компетенции	Результаты обучения (описание компетенции)	Показатели оценки результата
ОК 01	- владеет способы решения задач профессиональной деятельности применительно к различным контекстам.	- распознаёт задачу и/или проблему в профессиональном и/или социальном контексте; анализирует задачу и/или проблему и выделять её составные части; определяет этапы решения задачи; выявляет и эффективно ищет информацию, необходимую для решения задачи и/или проблемы; - составляет план действия; определяет необходимые ресурсы; - владеет актуальными методами работы в профессиональной и смежных сферах; - реализовывает составленный план; оценивает результат и последствия своих действий (самостоятельно или с помощью наставника).
ОК 02	- владеет современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.	- определяет задачи для поиска информации; определяет необходимые источники информации; планирует процесс поиска; структурирует получаемую информацию; выделяет наиболее значимое в перечне информации; оценивает практическую значимость результатов поиска; оформляет результаты поиска, применяет средства информационных технологий для решения профессиональных задач; использует современное программное обеспечение; использует различные цифровые средства для решения профессиональных задач.
ОК 09	- умеет пользоваться профессиональной документацией на государственном и иностранном языках.	- понимает тексты на базовые профессиональные темы.
ПК 1.1	- умеет проектировать базы данных.	- знает принципы безопасности хранения данных.
ПК 1.4	- умеет администрировать базы данных.	- знает методы защиты баз данных от внешних угроз.
ПК 1.5	- умеет защищать информацию в базе данных с использованием технологии защиты информации.	- знает принципы криптографии и методов шифрования данных; - знает стандарты и протоколы безопасности, таких как SSL/TLS, SSH, Kerberos и др.; - знает методы аутентификации и авторизации пользователей, включая использование паролей, сертификатов и биометрических данных; - знает законодательство и стандарты безопасности, такие как GDPR, HIPAA, PCI DSS и др.

ПК 3.1	- умеет собирать исходные данные для разработки проектной документации на информационную систему.	- знает отраслевую нормативную техническую документацию; - знает источники информации, необходимой для профессиональной деятельности.
ПК 3.2	- умеет разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.	- знает принципы и методы обеспечения безопасности информационных систем.
ПК 3.3	- умеет разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.	- знает принципы безопасности информационных систем; - знает современные методы и технологий в области безопасности информационных систем; - знает законодательных и нормативных актов в области безопасности информационных систем.
ПК 3.5	- умеет интегрировать информационную систему с существующими информационными системами заказчика.	- знает источники угроз информационной безопасности и меры по их предотвращению.
ПК 3.7	- умеет разрабатывать техническую документацию на эксплуатацию информационной системы.	- знает основные угрозы безопасности мобильных приложений; - знает принципы криптографии и шифрования данных; - знает стандарты и протоколы безопасности, такие как HTTPS, OAuth и OpenID Connect; - знает законодательные и регуляторные требования к защите данных, включая GDPR и HIPAA; - знает основные принципы безопасности информации и методов ее защиты; - знает стандартные криптографические алгоритмы для шифрования данных; - знает принципы обеспечения безопасности передачи данных по сети; - знает основы безопасности приложений и инфраструктуры; - знает методы анализа на уязвимости и мониторинга безопасности; - знает знание основных принципов и методов обеспечения безопасности ИТ-инфраструктуры и веб-приложений; - понимает различные уязвимостей и угроз безопасности, а также способов их предотвращения и обнаружения; - знает инструменты и технологии для обеспечения безопасности ИТ-инфраструктуры и веб-приложений, таких как брандмауэры, системы обнаружения вторжений и антивирусные программы.

3 Методические материалы, определяющие процедуры оценивания

Процесс оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, представлен в таблице 3.

Таблица 3

Тип занятия	Номера тем (работ, занятий)	Оценочные материалы
ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ПК 1.1 Проектировать базы данных.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет

ПК 1.4 Администрировать базы данных.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ПК 1.5 Защищать информацию в базе данных с использованием технологии защиты информации.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ПК 3.1 Собирать исходные данные для разработки проектной документации на информационную систему.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ПК 3.2 Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ПК 3.3 Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет

ПК 3.5 Интегрировать информационную систему с существующими информационными системами заказчика.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет
ПК 3.7 Разрабатывать техническую документацию на эксплуатацию информационной системы.		
Лекция	Все темы, в соответствии с рабочей программой.	Дифференцированный зачет
Практические занятия	Практические занятия №1-12, в соответствии с методическими указаниями по выполнению практических занятий.	Дифференцированный зачет
Самостоятельная работа	Самостоятельные работы, в соответствии с методическими указаниями по выполнению самостоятельных работ.	Дифференцированный зачет

4 Формы текущего контроля уровня сформированных компетенций (знаний, умений)

4.1 Практические занятия

Практическое занятие №1 Работа с симметричными и асимметричными алгоритмами.

Практическое занятие №2 Хэширование и создание цифровой подписи сообщения.

Практическое занятие №3 Выполнение резервного копирования и восстановления данных.

Практическое занятие №4 Управление доступом к данным.

Практическое занятие №5 Организация защиты от атак на сетевую инфраструктуру.

Практическое занятие №6,7 Настройка VPN соединения между филиалами организации.

Практическое занятие №8,9 Анализ уязвимостей приложений в сетевой инфраструктуре.

Практическое занятие №10 Исследование безопасности различных облачных моделей.

Практическое занятие №11 Исследование и анализ инцидентов в области сетевой безопасности.

Практическое занятие №12 Разработка политики информационной безопасности на предприятии.

Критерии оценки освоения

Усвоенные знания, умения проверяются в ходе выполнения практическое занятие. Объем и качество освоения обучающимися практических занятий, уровень сформированности общих и профессиональных компетенций оцениваются по результатам его защиты и переводятся в зачет в соответствии с таблицей 4.

Таблица 4

Оценка	Характеристика уровня освоения дисциплины
«зачет»	Ответы на вопросы к практическому занятию выполнены самостоятельно с возможными не большими замечаниями. Обучающийся демонстрирует сформированность общих и профессиональных компетенций основные знания, умения освоены, при этом могут допускаться незначительные ошибки, неточности, затруднения при ответе на поставленные вопросы, переносе знаний и умений на новые, нестандартные ситуации.
«незачет»	Ответы на вопросы к практическому занятию выполнены не самостоятельно с большим количеством ошибок и замечаний. Обучающийся не демонстрирует сформированность общих и профессиональных компетенций, проявляется недостаточность знаний, умений, навыков.

4.2 Самостоятельные работы

Самостоятельная работа по теме 2.2 «Защита данных»: оформление отчетов по практическим занятиям.

Самостоятельная работа по теме 3.4 «Безопасность облачных технологий*:* оформление отчетов по практическим занятиям.

Самостоятельная работа по теме 4.2 «Социальная инженерия и человеческий фактор»: оформление отчетов по практическим занятиям, подготовка к дифференцированному зачету.

Критерии оценки освоения

Усвоенные знания, умения проверяются в ходе ответов на вопросы дифференцированного зачета, а также при защите лабораторных работ. Объем и качество освоения обучающимися самостоятельной работы, уровень сформированности общих и профессиональных компетенций оцениваются по результатам дифференцированного зачета и защиты лабораторных работ и переводятся в зачет и оценку в соответствии с таблицами 4, 6.

4.3 Тестирование обучающихся

Тестовые задания по разделу 1 «Фундаментальные основы и управление информационной безопасностью».

Тестовые задания по разделу 2 «Криптографические методы и защита данных».

Тестовые задания по разделу 3 «Технические средства защиты инфраструктуры и приложений».

Тестовые задания по разделу 4 «Реагирование на угрозы и человеческий фактор».

Критерии оценки освоения

За правильный ответ на вопрос тестового задания выставляется положительная оценка - 1 балл.

За неправильный ответ на вопрос тестового задания выставляется отрицательная оценка - 0 баллов.

Таблица 5 - Шкала оценки

Процент результативности (правильных ответов на вопросы тестового задания)	Оценка уровня подготовки
90 - 100	отлично
80 - 89	хорошо
65 - 79	удовлетворительно
менее 65	неудовлетворительно

5 Формы промежуточной аттестации уровня сформированных компетенций (знаний, умений)

Формой промежуточной аттестации уровня сформированных компетенций, знаний и умений по дисциплине «Основы информационной безопасности» является дифференцированный зачет.

Перечень вопросов на дифференцированный зачет:

1. Раскройте понятие «информационная безопасность» и подробно охарактеризуйте триаду «конфиденциальность-целостность-доступность» (CIA). Приведите примеры, когда поддержание всех трех аспектов может вступать в противоречие.

2. Дайте определение понятиям «угроза», «уязвимость» и «риск». Опишите их взаимосвязь и предложите формулу для вычисления риска. Как классифицируются угрозы на преднамеренные и непреднамеренные?

3. Перечислите и классифицируйте актуальные киберугрозы 2024-2026 гг. (на основе открытых источников). Какова текущая динамика мотивации злоумышленников (финансовая, шпионаж, хактивизм)?

4. Что такое «поверхность атаки»? Опишите современные тенденции ее расширения (облака, IoT, удаленка). Какие методы получения первоначального доступа (фишинг, RDP, подрядчики) наиболее популярны у злоумышленников сегодня?

5. Охарактеризуйте ключевые этапы эволюции информационной безопасности: от физической защиты носителей и объектов связи, до современной кибербезопасности и концепции киберустойчивости.

6. Перечислите основные принципы государственной политики РФ в области информационной безопасности. Назовите ключевые законодательные акты (ФЗ «Об информации...», «О персональных данных», «О государственной тайне») и виды ответственности за правонарушения в этой сфере.

7. Опишите структуру, назначение и обязательные элементы Политики информационной безопасности организации. Каковы потенциальные последствия нарушения политики для сотрудника и для компании в целом?

8. Охарактеризуйте полный цикл управления рисками ИБ: идентификация, анализ, оценка и обработка рисков. Как оценка рисков связана с классификацией автоматизированных систем (АС) по требованиям защиты информации?

9. Каковы ключевые требования стандарта ISO/IEC 27001 к системе менеджмента информационной безопасности (СМИБ)? В чем принципиальное отличие стандарта ISO 15408 («Общие критерии») от ISO 27001?

10. Что такое GDPR и каково его влияние на международные компании? Какие Руководящие документы (РД) Гостехкомиссии/ФСТЭК России регламентируют классы защищенности автоматизированных систем?

11. Как технологии искусственного интеллекта (ИИ) и машинного обучения (МО) изменяют подходы к обнаружению вторжений (например, в SOC)? В чем заключается угроза «вепонизации» ИИ злоумышленниками?

12. Опишите потенциальное применение блокчейн-технологий для обеспечения целостности данных и децентрализованной идентификации. Что такое «конфиденциальные вычисления» (Confidential Computing) и как они решают проблемы безопасности облачных сред?

13. Какие этические дилеммы возникают при использовании ИИ в задачах ИБ (например, предиктивная аналитика слежки)? В чем заключается угроза использования дипфейков (deepfakes) для социальной инженерии и компрометации бизнес-процессов?

14. Охарактеризуйте концепцию Zero Trust (нулевое доверие) как новую парадигму сетевой безопасности. В чем ее отличие от классической модели «замка и рва»?

15. Как эволюция квантовых вычислений угрожает современным криптоалгоритмам (RSA, ECC)? В чем заключается стратегия сбора данных «Сейчас - расшифруй позже»?

16. Раскройте соотношение понятий криптология, криптография и криптоанализ. Опишите суть и приведите примеры шифров перестановки и замены (например, шифр Цезаря). В чем заключается условие абсолютной криптостойкости шифра Вернама (One-Time Pad)?

17. Дайте определение хэш-функции, перечислите её основные свойства (необратимость, устойчивость к коллизиям). Для каких целей используется HMAC и как он работает? В чем состоит опасность коллизий для цифровой подписи?

18. Проведите сравнительный анализ симметричного и асимметричного шифрования по критериям скорости, длины ключа и области применения. Объясните, как хэш-функции и шифрование используются для контроля целостности ПО при распространении файлов.

19. Опишите процесс создания и проверки квалифицированной электронной подписи (ЭП). Что такое сертификат открытого ключа и как он обеспечивает свойство «неотказуемости» (non-repudiation)?

20. Дайте определение криптографического ключа. Перечислите полный жизненный цикл ключа (генерация, распределение, хранение, ротация, уничтожение). Как длина ключа влияет на криптостойкость, и как классифицируются ключи по назначению?

21. Объясните принципы работы симметричных блочных (AES, «Магма», «Кузнечик») и потоковых (RC4, ChaCha20) шифров. Сравните отечественные криптостандарты (ГОСТ 34.12-2018, ГОСТ 34.11-2018) с их зарубежными аналогами.

22. Опишите математические основы алгоритма RSA. В чем заключается проблема распространения ключей в симметричных системах и как ее решает асимметричная криптография?

23. Объясните разницу между аутентификацией и авторизацией. Какие модели управления доступом (дискреционная, мандатная, ролевая) вы знаете? Для каких целей применяется шифрование на уровне носителей (Full Disk Encryption) и на уровне файлов?

24. Проведите классификацию сетевых атак на пассивные и активные. Опишите механизм IP-спуфинга (IP-spoofing) и меры его предотвращения.

25. Опишите технологию проведения DoS/DDoS-атак на примере SYN Flood. Объясните принципы атак Man-in-the-Middle (MITM), ARP-spoofing и DHCP starvation. На каких уровнях модели OSI они реализуются?

26. Перечислите и охарактеризуйте основные механизмы защиты сетевой инфраструктуры (сегментация, ACL, IPS). Какие существуют методы защиты от атак на протоколы STP и ARP?

27. Раскройте понятие VPN, классифицируйте VPN-решения (Site-to-Site, Remote Access). Какие протоколы туннелирования (L2TP/IPsec, OpenVPN) используются и в чем их отличия?

28. Дайте определение компьютерного вируса, перечислите его отличительные признаки. Классифицируйте вредоносное ПО (черви, трояны, шифровальщики, стилеры) и опишите основные каналы его распространения в корпоративных сетях.

29. Перечислите основные методы антивирусной защиты (сигнатурный, эвристический, проактивный) и типы антивирусных программ. В чем состоит главное ограничение сигнатурного метода? Каковы требования к современным корпоративным антивирусным средствам (EDR)?

30. Охарактеризуйте проект OWASP Top Ten. Опишите принципы, последствия и методы защиты от атак типа «Инъекции» (SQLi) и межсайтового скриптинга (XSS).

31. Чем опасен подбор пароля (брутфорс)? Объясните принцип межсайтовой подделки запроса (CSRF/XSRF) и роль anti-CSRF токенов в защите.

32. Что такое тестирование на проникновение (пентест) и чем оно отличается от сканирования уязвимостей? Перечислите основные принципы безопасного программирования (Secure Coding Practices).

33. Дайте определение облачных вычислений (NIST) и опишите модели обслуживания (IaaS, PaaS, SaaS). Объясните модель распределения ответственности за безопасность (Shared Responsibility Model) и угрозы, характерные для облачной среды.

34. Каковы особенности обеспечения безопасности при использовании IaaS (настройка виртуальных сетей, гигиена образов ОС, управление доступом)? Как ИИ и блокчейн интегрируются в модели безопасности облачных платформ?

35. Какие факторы делают информацию уязвимой при ее передаче, хранении и обработке? Опишите основные технические каналы утечки информации (сеть, email, мессенджеры, мобильные устройства) и методы защиты от них.

36. Что такое промышленный шпионаж? Какие методы технической разведки применяются в корпоративном секторе? Раскройте понятие OSINT и опишите, как методы разведки по открытым источникам используются как злоумышленниками, так и специалистами по ИБ.

37. Почему человеческий фактор считается самым слабым звеном в ИБ? Проведите классификацию атак социальной инженерии (фишинг, претекстинг, вишинг). Как злоумышленники используют срочность и авторитет?

38. Охарактеризуйте разновидности фишинга (массовый, spear phishing, whaling). Какие факторы привели к росту доли атак, начинающихся с фишинговых писем (до 64%)?

39. Дайте определение инцидента ИБ. Опишите полный цикл реагирования (стадии: подготовка, идентификация, сдерживание, устранение, восстановление, извлечение уроков). В чем отличие компьютерной криминалистики (форензики) от расследования инцидентов?

40. Каковы основные принципы сбора и сохранения цифровых доказательств? Объясните взаимосвязь между системами сбора и корреляции событий (SIEM), платформами оркестрации (SOAR) и базами знаний тактик и техник (MITRE ATT&CK).

Критерий оценки освоения

Усвоенные знания и умения проверяются в ходе ответов на вопросы. Объем и качество освоения обучающимися дисциплины, уровень сформированности общих и профессиональных компетенций оцениваются по результатам текущих и промежуточной аттестации и переводятся в оценку в соответствии с таблицей 6.

Таблица 6

Оценка по промежуточной аттестации	Характеристика уровня освоения дисциплины
«отлично»	Ответ на вопросы выполнен самостоятельно. Обучающийся демонстрирует сформированность общих и профессиональных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала, усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, свободно оперирует приобретенными знаниями, умениями, применяет их при выполнении заданий повышенной сложности.
«хорошо»	Ответ на вопросы подготовлен самостоятельно, но с замечаниями. Обучающийся демонстрирует сформированность общих и профессиональных компетенций, основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при ответе на поставленные вопросы, переносе знаний и умений на новые, нестандартные ситуации.
«удовлетворительно»	Ответ на вопросы выполнен недостаточно самостоятельно. Обучающийся демонстрирует сформированность общих и профессиональных компетенций: в ходе практических занятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний и умений по некоторым компетенциям, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
«неудовлетворительно»	Обучающийся не демонстрирует сформированность общих и профессиональных компетенций. Проявляется полное или практически полное отсутствие знаний и умений по дисциплине.

Банк контрольных заданий и иных материалов, используемых в процессе процедур текущего контроля и промежуточной аттестации, представлен в электронной информационно-образовательной среде по URI: http://aup.uisi.ru.

Литература

1 Основные печатные и/или электронные издания:

1. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 84 с. — ISBN 978-5-507-48808-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/394547.

2. Баланов, А. Н. Комплексная информационная безопасность : учебное пособие для спо / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 284 с. — ISBN 978-5-507-49251-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/414950.

2 Дополнительные издания:

1. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510.

2. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2024. — 124 с. — ISBN 978-5-507-47517-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/385082.