



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Б1.В.08 ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ»**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Сутягин Д. Д.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

Содержание

1. Цель и задачи освоения дисциплины (модуля)
2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы
3. Место дисциплины в структуре ОП
4. Объем дисциплины и виды учебной работы
5. Содержание дисциплины
 - 5.1. Разделы, темы дисциплины и виды занятий
 - 5.2. Содержание разделов, тем дисциплины и формы текущего контроля
6. Оценочные материалы текущего контроля
7. Оценочные материалы промежуточной аттестации
8. Порядок проведения промежуточной аттестации
9. Материально-техническое и учебно-методическое обеспечение дисциплины
 - 9.1. Перечень основной и дополнительной учебной литературы
 - 9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся
 - 9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине
 - 9.4. Оборудование и технические средства обучения
10. Методические указания по освоению дисциплины (модуля)

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучающихся комплекса теоретических знаний и практических навыков в области проектирования комплексных систем защиты информации (СЗИ) автоматизированных (информационных) систем, включая этапы обследования объекта защиты, разработки политик безопасности, выбора архитектуры и организационно-распорядительной документации, обеспечивающих нейтразацию актуальных угроз и соответствие требованиям регуляторов.

Задачи изучения дисциплины:

- изучение методологии и нормативной базы проектирования СЗИ;
- освоение методов архитектурного проектирования и выбора средств защиты;
- формирование навыков разработки проектной и рабочей документации.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-3 Способен проводить анализ уязвимостей внедряемой системы защиты информации

ПК-3.1 Выполняет оценку информационных рисков

Знать:

ПК-3.1/Зн1 Методологии и стандарты оценки рисков информационной безопасности, этапы идентификации активов, угроз и уязвимостей, а также качественные и количественные методы расчета уровня риска для обоснования выбора мер защиты на этапе проектирования СЗИ

Уметь:

ПК-3.1/Ум1 Идентифицировать критичные активы и актуальные угрозы, применять методики расчета рисков и интерпретировать полученные результаты для определения приоритетов внедрения средств защиты

Владеть:

ПК-3.1/Нв1 Навыками разработки модели угроз и нарушителя, методами ранжирования рисков и способностью оформлять результаты оценки рисков в виде раздела проектной документации

ПК-3.2 Проводит экспертизу состояния защищенности автоматизированных систем и применяемых средств защиты информации

Знать:

ПК-3.2/Зн1 Нормативные требования к защите информации, типовые уязвимости компонентов автоматизированных систем, а также методы и инструменты проведения анализа защищенности

Уметь:

ПК-3.2/Ум1 Анализировать проектные решения и конфигурации средств защиты на предмет выявления недостатков, планировать процедуры тестирования защищенности и выявлять некорректные настройки, снижающие уровень безопасности

Владеть:

ПК-3.2/Нв1 Навыками работы со сканерами уязвимостей и анализаторами трафика, методикой проведения аудита безопасности на этапе опытной эксплуатации и способностью оформлять результаты экспертизы в виде отчетов с рекомендациями по устранению недостатков

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.08 «Проектирование систем защиты информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 5.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
5 семестр	108	3	34	34	4	Экзамен (36)
Всего	108	3	34	34	4	36

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотношенные с результатами освоения программы
Раздел 1. Анализ угроз, уязвимостей и оценка рисков как основа проектирования	16	8	8		ПК-3.1 ПК-3.2
Тема 1.1. Инвентаризация активов и моделирование угроз	8	4	4		
Тема 1.2. Методология оценки рисков информационной безопасности	8	4	4		
Раздел 2. Формирование требований и разработка технического задания на СЗИ	16	6	6	4	ПК-3.1 ПК-3.2
Тема 2.1. Разработка требований к подсистемам защиты	12	6	6		

Тема 2.2. Анализ требований регуляторов к составу проектной документации на системы защиты информации	4			4	
Раздел 3. Проектирование архитектуры и выбор средств защиты информации	16	8	8		ПК-3.1 ПК-3.2
Тема 3.1. Принципы построения архитектуры комплексной системы защиты	8	4	4		
Тема 3.2. Классификация и критерии выбора средств защиты информации	8	4	4		
Раздел 4. Организационное обеспечение и разработка политик безопасности	12	6	6		ПК-3.1 ПК-3.2
Тема 4.1. Иерархия организационно-распорядительной документации. Разработка регламентов и инструкций для персонала	12	6	6		
Раздел 5. Проведение экспертизы и испытаний спроектированной системы защиты	12	6	6		ПК-3.1 ПК-3.2
Тема 5.1. Методы и инструменты анализа защищенности	12	6	6		
Итого	72	34	34	4	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Анализ угроз, уязвимостей и оценка рисков как основа проектирования

Тема 1.1. Инвентаризация активов и моделирование угроз

Понятие информационного актива с разделением на первичные и поддерживающие активы. Критерии критичности информации и возможные последствия от реализации угроз безопасности. Классификация источников угроз по различным признакам: внешние и внутренние, антропогенные и техногенные. Типы нарушителей, их потенциальные возможности и целевые ориентиры. Методика построения модели угроз для автоматизированной системы как исходный этап проектирования защиты.

Тема 1.2. Методология оценки рисков информационной безопасности

Понятие риска информационной безопасности через взаимосвязь угроз, уязвимостей и негативных последствий. Качественные методы оценки рисков, включая матричный подход и ранжирование по уровням опасности. Количественные методы, такие как расчет годовой ожидаемой потери и сценарийный анализ. Связь между результатами оценки рисков и обоснованным выбором мер защиты на этапе проектирования.

Текущий контроль

Вид (форма) контроля

Раздел 2. Формирование требований и разработка технического задания на СЗИ

Тема 2.1. Разработка требований к подсистемам защиты

Цикл автоматизированных систем и систем защиты информации. Определяется место и роль технического задания в процессе создания системы защиты. Изучаются требования к структуре, содержанию и оформлению ТЗ. Основания для разработки, назначение создаваемой системы, общие требования к системе и видам обеспечения. Методы сбора и анализа исходных данных в ходе обследования объекта информатизации. процесс декомпозиции общей задачи защиты информации на функциональные подсистемы: управление доступом, регистрация событий, обеспечение целостности, антивирусная защита, криптографическая защита. Правила построения функциональных требований к каждой выделенной подсистеме. Требования к надежности, эргономичности и совместимости проектируемой системы с существующей средой. Порядок согласования и утверждения технического задания заказчиком и разработчиком.

Текущий контроль

Вид (форма) контроля

Тестирование

Тема 2.2. Анализ требований регуляторов к составу проектной документации на системы защиты информации

Самостоятельное изучение студентами актуальных нормативных правовых актов ФСТЭК России и ФСБ России, регламентирующих требования к содержанию проектной и рабочей документации на системы защиты информации для различных классов автоматизированных систем. Выполняется сравнительный анализ требований для государственных информационных систем, объектов критической информационной инфраструктуры и систем персональных данных. По результатам изучения студенты составляют структурированный перечень обязательных документов, разрабатываемых на этапах «Проект» и «Рабочая документация», с указанием ссылок на конкретные пункты нормативных документов.

Раздел 3. Проектирование архитектуры и выбор средств защиты информации

Тема 3.1. Принципы построения архитектуры комплексной системы защиты

Понятие архитектуры системы защиты информации. Принципы эшелонированной защиты и создания рубежей безопасности на различных уровнях информационной системы. Подходы к сегментированию вычислительных сетей с выделением DMZ, публичных и частных сегментов. Ключевые точки контроля и оптимальные места размещения средств защиты в инфраструктуре организации. Вопросы резервирования критических компонентов и обеспечения отказоустойчивости системы защиты.

Тема 3.2. Классификация и критерии выбора средств защиты информации

Основные классы программно-аппаратных средств защиты: межсетевые экраны нового поколения, системы обнаружения и предотвращения вторжений, SIEM-системы, DLP-системы, средства криптографической защиты. Технические характеристики средств защиты: пропускная способность, вносимые задержки, возможности горизонтального масштабирования. Порядок разработки структурной схемы комплекса средств защиты как итогового документа этапа проектирования.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 4. Организационное обеспечение и разработка политик безопасности

Тема 4.1. Иерархия организационно-распорядительной документации. Разработка регламентов и инструкций для персонала

Организационные меры в общей системе обеспечения информационной безопасности наряду с техническими средствами. Иерархическая структура организационно-распорядительной документации: концепция, политика, положение, регламент, инструкция, их взаимосвязь и назначение. Частные политики по отдельным направлениям: управление доступом, антивирусная защита, резервное копирование и восстановление данных. Общие требования к оформлению организационных документов и порядку их ввода в действие. структура и содержание регламента реагирования на инциденты информационной безопасности. Требования к разработке инструкций для администраторов безопасности по настройке, мониторингу и своевременному обновлению средств защиты. Инструкции для пользователей, включающие требования к парольной защите, правилам работы со съемными носителями и безопасному поведению в информационных сетях.

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 5. Проведение экспертизы и испытаний спроектированной системы защиты

Тема 5.1. Методы и инструменты анализа защищенности

Цели проведения экспертизы состояния защищенности и ее основные виды: предпроектная, приемочная, инициативная. Методы анализа защищенности на уровне сети, включая сканирование портов и идентификацию сетевых сервисов. Принципы работы сканеров уязвимостей и дается обзор популярных решений: XSpider, MaxPatrol, nmap, OpenVAS. Методология тестирования на проникновение, его основные этапы, применяемые методы и существующие ограничения. Подходы к анализу конфигурационной безопасности с использованием чек-листов и стандартов безопасной настройки.

Текущий контроль

Вид (форма) контроля
Тестирование

6. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Экзамен, 5 семестр.

Экзамен оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

7. Оценочные материалы текущего контроля

Раздел 1. Анализ угроз, уязвимостей и оценка рисков как основа проектирования

Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 1.2. Методология оценки рисков информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что понимается под информационным активом в контексте проектирования СЗИ?
 1. Любое техническое устройство, подключенное к сети
 2. Информация, программное обеспечение, оборудование и персонал, имеющие ценность для организации
 3. Только базы данных, содержащие персональные данные
 4. Исключительно серверное оборудование и линии связи
2. Какие активы относятся к категории «поддерживающие»?
 1. Информация, составляющая коммерческую тайну
 2. Персональные данные клиентов
 3. Программное обеспечение, серверы, средства связи, персонал
 4. Исключительно криптографические ключи
3. Какие источники угроз относятся к антропогенным?

1. Природные явления (наводнения, землетрясения)
2. Деятельность людей (нарушители, персонал, администраторы)
3. Техногенные аварии и сбои оборудования
4. Программные ошибки в коде приложений
 4. Что представляет собой модель нарушителя?
 1. Перечень всех возможных компьютерных атак
 2. Описание предполагаемого злоумышленника, его целей, возможностей и методов действий
 3. Схема организации защиты периметра сети
 4. Документ, описывающий только внешние угрозы
 5. Для чего используется банк данных угроз ФСТЭК России (БДУ)?
 1. Для скачивания обновлений антивирусного программного обеспечения
 2. Для получения унифицированного описания угроз безопасности информации и сведений об уязвимостях
 3. Для регистрации инцидентов информационной безопасности
 4. Для закупки сертифицированных средств защиты
 6. Что такое риск информационной безопасности?
 1. Вероятность выхода из строя серверного оборудования
 2. Сочетание вероятности реализации угрозы и величины негативных последствий
 3. Гарантированное наличие уязвимости в системе
 4. Стоимость внедрения средств защиты
 7. Какой метод оценки рисков относится к качественным?
 1. Расчет годовой ожидаемой потери (ALE)
 2. Метод деревьев событий
 3. Матричный метод «вероятность/ущерб»
 4. Метод Монте-Карло
 8. Что означает стратегия обработки риска «принятие риска»?
 1. Немедленное внедрение всех возможных средств защиты
 2. Осознанное решение организации не принимать дополнительных мер, если риск находится в допустимых пределах
 3. Передача ответственности за риск страховой компании
 4. Полное избегание любой деятельности, связанной с риском
 9. Какой стандарт посвящен управлению рисками информационной безопасности?
 1. ГОСТ Р 50922
 2. ISO/IEC 27005
 3. ГОСТ 34.602
 4. ISO 9001
 10. Что является результатом построения модели угроз?
 1. Структурная схема локальной вычислительной сети
 2. Перечень актуальных угроз безопасности информации для конкретной системы
 3. Техническое задание на закупку оборудования
 4. План финансового аудита организации

Раздел 2. Формирование требований и разработка технического задания на СЗИ

Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 2.1. Разработка требований к подсистемам защиты

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Каким ГОСТом регламентируется разработка технического задания на автоматизируемую систему?
 1. ГОСТ 19.102
 2. ГОСТ 34.602

3. ГОСТ Р 50922

4. ГОСТ 28147

2. Какой раздел НЕ входит в типовую структуру технического задания на создание СЗИ?

1. Основания для разработки
2. Требования к программной документации
3. Калькуляция заработной платы сотрудников заказчика
4. Требования к видам обеспечения (информационному, лингвистическому и т.д.)

3. Что такое декомпозиция задачи защиты при разработке ТЗ?

1. Увеличение бюджета проекта
2. Разделение общей задачи на отдельные подсистемы (доступ, регистрация, антивирус и т.д.)
3. Передача части работ субподрядчикам
4. Объединение требований заказчика в один пункт

4. Кто участвует в согласовании и утверждении технического задания?

1. Только разработчик системы
2. Только заказчик системы
3. Заказчик и разработчик совместно
4. Регулирующие органы (ФСТЭК, ФСБ)

5. Какая ошибка является типичной при разработке ТЗ на СЗИ?

1. Излишняя детализация функциональных требований
2. Использование формулировок «система должна быть надежной и безопасной» без конкретных метрик
3. Указание ссылок на действующие ГОСТы
4. Наличие раздела с глоссарием

Раздел 3. Проектирование архитектуры и выбор средств защиты информации

Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 3.2. Классификация и критерии выбора средств защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой принцип означает создание нескольких последовательных рубежей защиты?

1. Принцип единого входа
2. Принцип эшелонированной защиты (Defense in Depth)
3. Принцип открытой архитектуры
4. Принцип минимальных привилегий

2. Для чего создается DMZ (демитаризованная зона)?

1. Для размещения серверов, доступных из внешних сетей, с изоляцией от внутренней сети
2. Для хранения резервных копий баз данных
3. Для подключения рабочих мест руководства организации
4. Для беспроводного доступа гостей пользователей

3. Что такое NGFW (межсетевой экран нового поколения)?

1. Маршрутизатор с функцией NAT
2. Межсетевой экран с возможностями инспекции приложений, IPS и контекстного анализа
3. Программный комплекс для антивирусной проверки почты
4. Аппаратный модуль для криптографической защиты

4. Что понимается под ТСО при выборе средства защиты?

1. Максимальная пропускная способность устройства
2. Совокупная стоимость владения, включая закупку, внедрение и сопровождение
3. Время непрерывной работы без отказа
4. Количество одновременно обслуживаемых пользователей

5. Для каких систем обязательно наличие сертификатов ФСТЭК или ФСБ на средства защиты-ты?

1. Для любых коммерческих организаций
2. Только для государственных информационных систем и объектов КИИ
3. Для домашних компьютеров
4. Только для банковских систем

Раздел 4. Организационное обеспечение и разработка политик безопасности

Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 4.1. Иерархия организационно-распорядительной документации. Разработка регламентов и инструкций для персонала

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой документ является основополагающим в иерархии организационно-распорядительной документации по ИБ?

1. Инструкция пользователя
2. Политика информационной безопасности
3. Регламент реагирования на инциденты
4. Журнал учета съемных носителей

2. Что определяет политика разграничения прав доступа?

1. Правила выплаты премий сотрудникам
2. Правила и порядок предоставления субъектам доступа прав на выполнение операций над объектами
3. Расписание работы системного администратора
4. Порядок утилизации старого оборудования

3. Какая модель управления доступом подразумевает назначение прав в зависимости от должностных обязанностей (ролей)?

1. Дискреционная модель
2. Мандатная модель
3. Ролевая модель
4. Избирательная модель

4. Что должен содержать регламент реагирования на инциденты?

1. Правила приема на работу сотрудников
2. Порядок действий персонала при обнаружении признаков нарушения безопасности
3. Технические характеристики серверного оборудования
4. Список контактных телефонов всех сотрудников

5. Какие требования обычно включаются в инструкцию для пользователей?

1. Требования к длине и сложности пароля
2. Правила окраски стен в серверной
3. Инструкция по ремонту принтеров
4. Правила оформления командировок

Раздел 5. Проведение экспертизы и испытаний спроектированной системы защиты

Контролируемые ИДК: ПК-3.1 ПК-3.2

Тема 5.1. Методы и инструменты анализа защищенности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое тестирование на проникновение (пентест)?

1. Проверка физической охраны периметра здания
2. Легитимная попытка взлома системы для оценки ее защищенности

3. Тестирование электропитания серверов
4. Проверка скорости интернет-соединения
 2. Какие инструменты относятся к сканерам уязвимостей?
 1. Microsoft Word, Excel
 2. XSpider, MaxPatrol, nmap
 3. Adobe Photoshop, CorelDraw
 3. Что такое программа и методика испытаний (ПМИ)?
 1. Программа обучения персонала
 2. Документ, устанавливающий порядок, объем и методы проведения испытаний системы
 3. График отпусков сотрудников отдела ИБ
 4. Смета расходов на закупку оборудования
 4. На каком этапе жизненного цикла проводятся приемо-сдаточные испытания?
 1. На этапе предпроектного обследования
 2. На этапе ввода системы в эксплуатацию
 3. На этапе утилизации системы
 4. На этапе концептуального проектирования
 5. Какой документ оформляется по результатам приемо-сдаточных испытаний?
 1. Договор на поставку оборудования
 2. Акт приемки-сдачи работ (или протокол испытаний)
 3. Рекламный буклет системы
 4. Устав организации

8. Оценочные материалы промежуточной аттестации

5 семестр, Экзамен

Контролируемые ИДК: ПК-3.1 ПК-3.2

Вопросы/Задания:

1. Дайте определение понятию «информационный актив» в контексте проектирования систем защиты информации. Приведите примеры первичных и поддерживающих активов.
2. Перечислите основные этапы процесса оценки рисков информационной безопасности согласно методологии ISO/IEC 27005.
3. Что такое модель угроз и модель нарушителя? Для чего они разрабатываются на этапе проектирования СЗИ?
4. Опишите структуру и назначение банка данных угроз ФСТЭК России (БДУ).
5. Назовите основные стратегии обработки информационных рисков и кратко охарактеризуйте каждую из них.
6. Какими ГОСТами регламентируется разработка технического задания на создание автоматизированных систем и систем защиты информации?
7. Перечислите основные разделы технического задания на создание системы защиты информации.
8. Что понимается под декомпозицией задачи защиты при разработке ТЗ? Какие подсистемы обычно выделяются?

9. Какие виды обеспечения автоматизированных систем должны быть учтены при разработке требований в ТЗ?

10. Дайте определение понятию «архитектура системы защиты информации». Назовите основные типы архитектурных решений.

11. Что означает принцип эшелонированной защиты (Defense in Depth)? Какие уровни защиты он предполагает?

12. Для чего создается демилитаризованная зона (DMZ) при проектировании сетевой инфраструктуры?

13. Перечислите основные классы программно-аппаратных средств защиты информации.

14. Что такое NGFW (межсетевой экран нового поколения)? Чем он отличается от классического межсетевого экрана?

15. Назовите критерии выбора средств защиты информации при проектировании СЗИ.

16. Что понимается под совокупной стоимостью владения (ТСО) средства защиты? Какие составляющие в нее входят?

17. Какова иерархия организационно-распорядительной документации по информационной безопасности? Перечислите основные виды документов.

18. Что должна содержать Политика информационной безопасности организации как документ верхнего уровня?

19. Какие модели управления доступом используются при проектировании систем разграничения прав? Дайте их краткую характеристику.

20. Что такое тестирование на проникновение (пентест)? Какие задачи решаются с его помощью?

21. Сравните качественные и количественные методы оценки информационных рисков. В каких случаях целесообразно применять каждый из подходов? Приведите примеры.

22. Проанализируйте взаимосвязь между результатами оценки рисков и формированием требований к системе защиты информации в техническом задании. Как результаты оценки влияют на выбор конкретных мер защиты?

23. Сравните централизованную, децентрализованную и гибридную архитектуры построения систем защиты информации. Каковы преимущества и недостатки каждого подхода?

24. Проанализируйте требования к сертификации средств защиты информации для различных типов информационных систем (государственные, коммерческие, объекты КИИ). Чем обусловлены различия в требованиях?

25. Сравните дискреционную, мандатную и ролевую модели управления доступом. Для каких типов организаций и систем наиболее подходит каждая модель?

26. Разработайте структуру модели угроз для автоматизированной системы обработки персональных данных в медицинском учреждении. Какие факторы необходимо учесть при построении модели? Какие источники угроз будут наиболее актуальными?

27. Предложите архитектурное решение для защиты распределенной сети коммерческого банка, включающей головной офис, 20 удаленных филиалов и мобильных сотрудников. Обоснуйте выбор средств защиты на каждом уровне и принципы сегментирования сети.

28. Составьте план проведения приемо-сдаточных испытаний системы защиты информации для государственной информационной системы. Какие документы должны быть разработаны? Какие проверки являются обязательными? Каков порядок оформления результатов?

29. Проанализируйте типичные ошибки при разработке организационно-распорядительной документации по информационной безопасности на примере реальной организации (или гипотетического сценария). Предложите пути их исправления и методы контроля исполнения документов.

30. Разработайте концепцию системы защиты информации для малого предприятия (30 сотрудников, один офис, выход в интернет, использование облачных сервисов). Обоснуйте минимально необходимый набор технических и организационных мер защиты с учетом ограниченного бюджета и требований регуляторов.

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Симаков А. А. Защита информации в компьютерных системах: учебное пособие: учебное пособие / А. А. Симаков, А. В. Кургузов. - Защита информации в компьютерных системах - Омск: Омская академия МВД России, 2022. - 108 с. - 978-5-88651-802-3. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/138415.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Мирошников А. И. Основы информационной безопасности и защита информации: учебное пособие: учебное пособие / А. И. Мирошников, А. С. Сысоев. - Основы информационной безопасности и защита информации - Липецк: Липецкий государственный технический университет, ЭБС АСВ, 2022. - 107 с. - 978-5-00175-160-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/128718.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Никифоров С. Н. Защита информации. Защита от внешних вторжений: учебное пособие: учебное пособие / С. Н. Никифоров. - Защита информации. Защита от внешних вторжений - Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. - 84 с. - 978-5-9227-0757-2. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/74381.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Котова Л. В. Сборник задач по дисциплине «Методы и средства защиты информации»: учебное пособие: учебное пособие / Л. В. Котова. - Сборник задач по дисциплине «Методы и средства защиты информации» - Москва: Московский педагогический государственный университет, 2024. - 44 с. - 978-5-4263-0221-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/146051.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Солонская О. И. Средства защиты информации: учебное пособие: учебное пособие / О. И. Солонская. - Средства защиты информации - Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. - 89 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/117115.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Никифоров С. Н. Методы защиты информации. Защищенные сети / С. Н. Никифоров. - 2-е изд., стер. - Санкт-Петербург: Лань, 2021. - 96 с. - 978-5-8114-8123-1. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/171868.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие: учебное пособие / Д. А. Скрипник. - Общие вопросы технической защиты информации - Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. - 424 с. - 978-5-4497-2415-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/133955.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

Не используются.

Ресурсы «Интернет»

1. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"
2. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)
3. <https://www.elibrary.ru/> - НЭБ eLIBRARY
4. <https://www.iprbookshop.ru/> - IPR BOOKS
5. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"

9.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Перечень программного обеспечения

(обновление производится по мере появления новых версий программы)

Не используется.

Перечень информационно-справочных систем

(обновление выполняется еженедельно)

Не используется.

9.4. Оборудование и технические средства обучения

Компьютерный класс

Маркерная доска - 0 шт.

Моноблок - 64 шт.

Проектор - 4 шт.

Смешанный тип

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 1 шт.

10. Методические указания по освоению дисциплины (модуля)

С целью успешного освоения данного предмета студенту необходимо выполнять домашние работы по указанным преподавателям темам и представленным на занятиях материалам. Для более успешного выполнения работы студенту предлагается использование учебно-методических материалов, соответствующих указанной теме.

Самостоятельная работа студентов описывается и регулируется методическими рекомендациями по дисциплине.

Описание возможностей изучения дисциплины лицами с ОВЗ и инвалидами

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.