



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.03 УПРАВЛЕНИЕ ПРОЕКТАМИ В ОБЛАСТИ ПОСТРОЕНИЯ ПОДСИСТЕМ
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: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Рябов В. С.

Преподаватель кафедры Информационно-измерительных систем
Хлытина В. А.

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 - освоение основополагающих принципов управления проектами в области построения подсистем защиты информации на основе процесса управления рисками информационной безопасности с помощью различных стандартов в области информационной безопасности.

Задачи изучения дисциплины:

- уметь выявлять и определять риски информационной безопасности в организации, их отличие от рисков другой природы;
- уметь выбирать и применять методики анализа рисков информационной безопасности;
- уметь определять информационные активы организации;
- уметь оценивать риски информационной безопасности по различным российским и международным стандартам ИБ;
- уметь производить анализ уязвимостей информационной системы;
- уметь моделировать угрозы информационной безопасности для информационных систем;
- уметь производить оценку ущерба от использования уязвимостей информационных систем;
- уметь составлять модель нарушителя информационной безопасности.

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

Компетенции, индикаторы и результаты обучения

УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

УК-2.1 Формулирует проблему, решение которой напрямую связано с достижением цели проекта

Знать:

УК-2.1/Зн1 Основные подходы к постановке проблемы в области информационной безопасности, принципы формулирования целей и задач проектов в сфере информационной безопасности, основы проектного управления

Уметь:

УК-2.1/Ум1 Выделять ключевые проблемы в организационно-правовой сфере информационной безопасности, формулировать проблемы, решение которых необходимо для достижения целей проекта, уточнять проектные цели с учётом нормативных и правовых требований

Владеть:

УК-2.1/Нв1 Методы постановки задач в проектной деятельности в информационной безопасности, навыки критического анализа проблемных ситуаций в правовом обеспечении информационной безопасности, инструменты описания проблемной области проекта

УК-2.2 Определяет связи между поставленными задачами и ожидаемые результаты их решения

Знать:

УК-2.2/Зн1 Методики декомпозиции задач и планирования проектов, основы логической структуры проектной деятельности, показатели эффективности решений в сфере информационной безопасности

Уметь:

УК-2.2/Ум1 Устанавливать взаимосвязи между задачами в рамках правового и организационного обеспечения информационной безопасности, соотносить задачи с ожидаемыми правовыми и организационными результатами, оценивать вклад отдельных задач в достижение цели проекта

Владеть:

УК-2.2/Нв1 Приёмы логической структуризации проектной деятельности, навыки построения связей «задача–результат», методы оценки достижимости результатов в правовом контексте

УК-2.3 Анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач

Знать:

УК-2.3/Зн1 Принципы календарного и сетевого планирования проектов, методы оптимизации проектных решений, ограничения и риски в реализации проектов по информационной безопасности

Уметь:

УК-2.3/Ум1 Читать и анализировать план-графики реализации проектов, сравнивать альтернативные способы достижения задач

Владеть:

УК-2.3/Нв1 Инструменты анализа проектных планов, методы выбора оптимального сценария проектной реализации, навыки применения инструментов управления проектами (например, Gantt, PERT, диаграммы)

УК-2.4 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы

Знать:

УК-2.4/Зн1 Основы ресурсного обеспечения проектов, действующее законодательство в области информационной безопасности и смежных областях, ограничения, накладываемые нормативными актами и регуляторами

Уметь:

УК-2.4/Ум1 Идентифицировать правовые, ресурсные и организационные ограничения, оценивать доступные ресурсы (трудовые, временные, информационные), применять правовые нормы в контексте проектной деятельности

Владеть:

УК-2.4/Нв1 Методы правового анализа и правоприменения, навыки учета ресурсных и нормативных ограничений при планировании проекта, приемы оценки соответствия проекта действующему законодательству

УК-2.5 Оценивает решение поставленных задач в зоне своей ответственности в соответствии с запланированными результатами контроля, при необходимости корректирует способы решения задач и выбирает оптимальный способ решения поставленных задач

Знать:

УК-2.5/Зн1 Подходы к контролю и оценке проектных результатов, методы оценки эффективности реализованных мероприятий, критерии качества выполнения задач в области информационной безопасности

Уметь:

УК-2.5/Ум1 Проводить оценку выполнения задач на всех этапах проекта, корректировать проектные решения в зависимости от отклонений, обосновывать необходимость изменений и выбирать альтернативные пути решения

Владеть:

УК-2.5/Нв1 Навыки мониторинга и контроля проектной деятельности, инструментами оценки соответствия результатов поставленным задачам, методами адаптивного управления в условиях правовых и организационных ограничений

УК-3 Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде

УК-3.1 Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели

Знать:

УК-3.1/Зн2 теоретические основы управления проектами

Уметь:

УК-3.1/Ум2 умеет определять цели и задачи проекта, формировать план проекта, работать в команде

Владеть:

УК-3.1/Нв1 способами устанавливать разные виды коммуникации (учебную, деловую, неформальную)

УК-3.2 При реализации своей роли в команде учитывает особенности поведения других членов команды

Знать:

УК-3.2/Зн2 особенности жёстких и гибких методов управления проектами

УК-3.2/Зн3 принципы подбора подходящего метода управления проектом

Уметь:

УК-3.2/Ум1 использовать теории мотивации, лидерства, особенности поведения других членов команды для решения стратегических и оперативных управленческих задач командного взаимодействия

Владеть:

УК-3.2/Нв1 способностью реализовывать свою роль в команде с учетом психологических особенностей субъектов переговорного процесса

УК-3.3 Анализирует возможные последствия личных действий и планирует свои действия для достижения заданного результата

Знать:

УК-3.3/Зн1 возможные последствия личных действий и планирует свои действия для достижения заданного результата

Уметь:

УК-3.3/Ум1 планировать свои действия для достижения заданного результата

Владеть:

УК-3.3/Нв1 навыками анализировать возможные последствия личных действий и планирует их для достижения заданного результата

УК-3.4 Осуществляет обмен информацией, знаниями и опытом с членами команды; оценивает идеи других членов команды для достижения поставленной цели

Знать:

УК-3.4/Зн1 способы обмена информацией, знаниями, опытом между членами команды

Уметь:

УК-3.4/Ум1 обмениваться информацией знаниями, опытом с членами команды и оценивать идеи других членов команды

Владеть:

УК-3.4/Нв1 навыками информационного обмена и коммуникации для достижения поставленных целей

УК-3.5 Соблюдает установленные нормы и правила командной работы, несет личную ответственность за общий результат

Знать:

УК-3.5/Зн1 нормы и правила командной работы

Уметь:

УК-3.5/Ум1 нести личную ответственность за общий результат всей команды

Владеть:

УК-3.5/Нв1 навыками использования правил командной работы

3. Место дисциплины в структуре ОП

Дисциплина (модуль) Б1.В.03 «Управление проектами в области построения подсистем защиты информации» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 7.

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)
7 семестр	144	4	34	34	76	Зачет
Всего	144	4	34	34	76	

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. Управление рисками ИБ. Основные термины и определения. Место управления рисками ИБ в организации	16	6	2	8	УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5
Тема 1.1. Базовый понятийный аппарат управления рисками информационной безопасности	4	2		2	УК-3.1 УК-3.2 УК-3.3
Тема 1.2. Контекст и место управления рисками в системе корпоративного управления и общем менеджменте организации	4	2		2	УК-3.4 УК-3.5
Тема 1.3. Нормативно-правовая база и стандартизация в области управления рисками ИБ	8	2	2	4	
Раздел 2. Основные методологии управления рисками ИБ	20	4	8	8	УК-2.1 УК-2.2 УК-2.3
Тема 2.1. Сравнительный анализ подходов к управлению рисками: базовый и продвинутый подходы	16	4	4	8	УК-2.4 УК-2.5 УК-3.1 УК-3.2
Тема 2.2. Обзор зарубежных и отечественных методик (NIST, ISO 27005, CRAMM, OCTAVE)	2		2		УК-3.3 УК-3.4 УК-3.5
Тема 2.3. Методологии, ориентированные на оценку стоимости риска (FAIR, Risk IT)	2		2		
Раздел 3. Идентификация активов. Виды уязвимостей	24	6	6	12	УК-2.1 УК-2.2
Тема 3.1. Классификация и инвентаризация информационных активов организации	10	2	2	6	УК-2.3 УК-2.4 УК-2.5 УК-3.1
Тема 3.2. Природа и классификация уязвимостей	12	4	2	6	УК-3.2 УК-3.3
Тема 3.3. Сканирование уязвимостей и управление конфигурациями	2		2		УК-3.4 УК-3.5
Раздел 4. Методы моделирования угроз и оценки рисков ИБ	16	4	4	8	УК-2.1 УК-2.2 УК-2.3
Тема 4.1. Методологии моделирования угроз: STRIDE, PASTA, Attack Trees	4	1	1	2	УК-2.4 УК-2.5 УК-3.1
Тема 4.2. Качественные и количественные методы оценки рисков	8	2	2	4	УК-3.2 УК-3.3 УК-3.4
Тема 4.3. Практическое применение матриц рисков и вычисление уровня риска	4	1	1	2	УК-3.5

Раздел 5. Методы обработки рисков ИБ. Виды мер для снижения рисков ИБ	24	6	4	14	УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2
Тема 5.1. Стратегии обработки рисков: модификация, сохранение, избегание, передача	10	2	2	6	УК-3.3 УК-3.4 УК-3.5
Тема 5.2. Классификация мер защиты и выбор средств обеспечения безопасности	14	4	2	8	
Раздел 6. Мониторинг и пересмотр рисков ИБ	16	2	2	12	УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2
Тема 6.1. Непрерывный мониторинг событий и управление инцидентами ИБ	10	2	2	6	УК-3.3 УК-3.4 УК-3.5
Тема 6.2. Процедуры пересмотра и актуализации оценки рисков	6			6	
Раздел 7. Подготовка отчетности. Заказчики результатов оценки рисков ИБ	16	4	4	8	УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2
Тема 7.1. Адаптация отчетности по рискам ИБ для различных уровней управления	8	2	2	4	УК-3.3 УК-3.4 УК-3.5
Тема 7.2. Взаимодействие с заинтересованными сторонами и предоставление результатов оценки	8	2	2	4	
Раздел 8. Методологии управления проектами	12	2	4	6	УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2
Тема 8.1. Классические и гибкие подходы к управлению проектами в сфере ИБ	10	2	2	6	УК-3.3 УК-3.4 УК-3.5
Тема 8.2. Процессы управления проектами создания подсистем защиты информации	2		2		
Итого	144	34	34	76	

5.2. Содержание разделов, тем дисциплин и формы текущего контроля

Раздел 1. Управление рисками ИБ. Основные термины и определения. Место управления рисками ИБ в организации

Тема 1.1. Базовый понятийный аппарат управления рисками информационной безопасности

В данной теме рассматриваются ключевые определения согласно стандартам (ГОСТ Р ИСО/МЭК 27000), иерархия понятий «актив», «угроза», «уязвимость», «источник угрозы» и «последствие», а также центральное понятие «риск ИБ» как сочетание последствий и вероятности реализации угрозы, и разграничение понятий инцидента и риска

Тема 1.2. Контекст и место управления рисками в системе корпоративного управления и общем менеджменте организации

В рамках темы анализируется интеграция процесса управления рисками ИБ в общую стратегию компании, рассматривается взаимосвязь с операционными, финансовыми и репутационными рисками бизнеса, а также определяется роль управления рисками ИБ как инструмента принятия обоснованных управленческих решений

Тема 1.3. Нормативно-правовая база и стандартизация в области управления рисками ИБ

Содержание темы включает обзор международных и национальных стандартов (ISO 31000, ISO/IEC 27005, NIST SP 800-30), а также анализ влияния отраслевых требований регуляторов (ЦБ РФ, ФСТЭК, PCI DSS) на построение системы управления рисками

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 2. Основные методологии управления рисками ИБ

Тема 2.1. Сравнительный анализ подходов к управлению рисками: базовый и продвинутый подходы

В теме рассматриваются два основных подхода: суть базового подхода (экспертная оценка, минимальная трудозатратность) и его применимость, а также особенности продвинутого подхода, требующего детальной идентификации активов и построения математических моделей

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 2.2. Обзор зарубежных и отечественных методик (NIST, ISO 27005, CRAMM, OCTAVE)

Здесь представлен детальный разбор архитектуры и этапов популярных методологий: методика NIST с акцентом на техническую составляющую, стандарт ISO 27005 с ориентацией на бизнес-процессы, а также специализированные решения CRAMM (детальная база знаний) и OCTAVE (фокус на организационном контексте)

Тема 2.3. Методологии, ориентированные на оценку стоимости риска (FAIR, Risk IT)

Данная тема посвящена количественным методам оценки: изучение стандарта FAIR для перевода качественных показателей в финансовые ожидаемые потери, а также рассмотрение фреймворка Risk IT от ISACA для интеграции управления рисками ИБ в общее ИТ-управление

Раздел 3. Идентификация активов. Виды уязвимостей

Тема 3.1. Классификация и инвентаризация информационных активов организации

В теме рассматриваются критерии отнесения объектов к активам ИБ, методики проведения инвентаризации и категоризации активов по типам (информационные, программные, физические, человеческие), а также понятие владельца актива и важность определения ценности актива для бизнеса

Тема 3.2. Природа и классификация уязвимостей

Здесь производится систематизация уязвимостей: подробно разбираются технологические (ошибки кода, недостатки протоколов), организационные (человеческий фактор, слабая политика безопасности) и физические уязвимости, а также изучаются источники информации об уязвимостях (базы CVE, бюллетени безопасности)

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 3.3. Сканирование уязвимостей и управление конфигурациями

В рамках темы рассматриваются практические инструменты выявления уязвимостей: работа автоматических сканеров (Nessus, OpenVAS), принципы тестов на проникновение (pentest) и анализа конфигураций, а также процесс управления уязвимостями как непрерывный цикл

Раздел 4. Методы моделирования угроз и оценки рисков ИБ

Тема 4.1. Методологии моделирования угроз: STRIDE, PASTA, Attack Trees

Содержание темы включает изучение проактивных подходов к выявлению угроз: детальный разбор методологии STRIDE, построение деревьев атак (Attack Trees) для анализа векторов атак, а также методология PASTA, ориентированная на бизнес-риски приложений

Тема 4.2. Качественные и количественные методы оценки рисков

В данной теме проводится сравнение двух парадигм измерения риска: качественный метод с использованием шкал и построением матриц, и количественный метод с вычислением математических ожиданий потерь (ALE, SLE, ARO), а также обсуждаются сильные и слабые стороны каждого подхода

Тема 4.3. Практическое применение матриц рисков и вычисление уровня риска

Рассматривается практикум по созданию профиля рисков: построение двухмерных и трехмерных матриц для визуализации приоритетов, формулы расчета уровня риска и отработка навыка определения уровня приемлемого (остаточного) риска

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 5. Методы обработки рисков ИБ. Виды мер для снижения рисков ИБ

Тема 5.1. Стратегии обработки рисков: модификация, сохранение, избегание, передача

Анализ четырех основных вариантов реагирования на идентифицированные риски: стратегия модификации (снижения) через внедрение защитных мер и контролей, стратегия сохранения (принятия) как осознанное решение рисковать с фиксацией уровня приемлемого риска, стратегия избегания путем отказа от рискованных процессов или технологий, а также стратегия передачи риска (например, аутсорсинг или страхование кибер-рисков). Условия применения и последствия выбора каждой стратегии для организации

Тема 5.2. Классификация мер защиты и выбор средств обеспечения безопасности

Виды мер для снижения рисков ИБ.

Текущий контроль
Вид (форма) контроля
Тестирование

Раздел 6. Мониторинг и пересмотр рисков ИБ

Тема 6.1. Непрерывный мониторинг событий и управление инцидентами ИБ

Процессы сбора, корреляции и анализа событий безопасности с использованием SIEM-систем для раннего выявления инцидентов. Влияние инцидентов ИБ на текущий профиль рисков организации. Роль систем класса SOAR (Security Orchestration, Automation and Response) в автоматизации реагирования и управления инцидентами как элемент контура обратной связи для риск-менеджмента

Текущий контроль
Вид (форма) контроля
Тестирование

Тема 6.2. Процедуры пересмотра и актуализации оценки рисков

Триггеры для внеочередного пересмотра рисков: существенные изменения в ИТ-инфраструктуре и бизнес-процессах, появление новых критических уязвимостей и векторов атак, результаты внутренних и внешних аудитов. Регламенты планового периодического пересмотра рисков. Актуализация реестра рисков и карты рисков на основе изменений во внешней и внутренней среде организации

Раздел 7. Подготовка отчетности. Заказчики результатов оценки рисков ИБ

Тема 7.1. Адаптация отчетности по рискам ИБ для различных уровней управления

Дифференциация отчетных форм в зависимости от целевой аудитории: детальные технические отчеты с описанием уязвимостей и конкретных рекомендаций для ИТ-специалистов и руководителей технических подразделений. Агрегированные отчеты и дашборды для топ-менеджмента, содержащие ключевые метрики рисков, динамику изменений и фокус на бизнес-последствиях (финансовых, репутационных)

Тема 7.2. Взаимодействие с заинтересованными сторонами и предоставление результатов оценки

Определение круга внутренних и внешних стейкхолдеров (заказчиков) оценки рисков: совет директоров, акционеры, регуляторы (ФСТЭК, ЦБ РФ), аудиторы, партнеры. Форматы предоставления результатов (отчеты, презентации, заключения). Использование ключевых индикаторов риска (KRI) для донесения информации до неспециалистов в области ИБ. Учет требований внешних регуляторов при подготовке отчетности

Текущий контроль

Вид (форма) контроля
Тестирование

Раздел 8. Методологии управления проектами

Тема 8.1. Классические и гибкие подходы к управлению проектами в сфере ИБ

Сравнительный анализ каскадной модели (Waterfall) и гибких методологий (Agile, Scrum) применительно к проектам в области информационной безопасности. Области применения Waterfall для проектов с фиксированными требованиями и жесткими сроками (например, аттестация объектов информатизации). Использование гибких подходов (Scrum, Kanban) в проектах с высокой степенью неопределенности, таких как разработка средств защиты или внедрение DevSecOps

Текущий контроль

Вид (форма) контроля
Тестирование

Тема 8.2. Процессы управления проектами создания подсистем защиты информации

Применение стандартных процессов проектного управления (инициация, планирование, исполнение, контроль, завершение) к специфическим ИБ-проектам. Инструменты планирования: построение иерархической структуры работ (WBS), разработка сетевых графиков и расписания проекта. Особенности управления командой проекта, коммуникациями и рисками при внедрении сложных технических решений и организационных изменений в области защиты информации

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: Зачет, 7 семестр.

Зачет оценивается по следующей шкале:

- оценка «зачтено» 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; а также автоматически, когда обучающийся за промежуточную аттестацию имеет оценки «отлично»;

- оценка «не зачтено» выставляется обучающемуся в случае наличия грубых ошибок при изложении ответа на основные вопросы программы, свидетельствующих о неправильном понимании предмета; при решении практических задач показано незнание способов их решения, материал изложен беспорядочно и неуверенно.

7. Оценочные материалы текущего контроля

Раздел 1. Управление рисками ИБ. Основные термины и определения. Место управления рисками ИБ в организации

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 1.3. Нормативно-правовая база и стандартизация в области управления рисками ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое риск в контексте информационной безопасности?
 1. Вероятность успешной атаки на систему
 2. Сочетание вероятности события и его последствий для организации
 3. Любая угроза, направленная на информационные активы
 4. Аппаратный сбой в системе
2. Что такое "остаточный риск"?
 1. Риск, который невозможно устранить
 2. Риск, оставшийся после применения мер защиты
 3. Риск, связанный с человеческим фактором
 4. Риск, который не был выявлен при оценке
3. Какой метод оценки рисков основан на качественных показателях?
 1. Количественный анализ
 2. Качественный анализ
 3. Статистический анализ
 4. Факторный анализ
4. Что такое "угроза" в контексте ИБ?
 1. Уязвимость системы
 2. Потенциальная причина нежелательного инцидента
 3. Реализованная атака на систему
 4. Ошибка в коде программы

Раздел 2. Основные методологии управления рисками ИБ

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 2.1. Сравнительный анализ подходов к управлению рисками: базовый и продвинутый подходы

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой метод снижения рисков предполагает установку межсетевого экрана?
 1. Принятие риска
 2. Передача риска
 3. Снижение риска

4. Избегание риска

2. Что такое "уязвимость" в ИБ?

1. Атака на систему
2. Слабость, которая может быть использована угрозой
3. Неправильная настройка сети
4. Отказ оборудования

3. Какой этап управления рисками следует после оценки рисков?

1. Идентификация активов
2. Обработка рисков
3. Мониторинг
4. Аудит

4. Какой подход предполагает расчет риска в денежном эквиваленте?

1. Качественный анализ
2. Количественный анализ
3. Сценарный анализ
4. Экспертный анализ

5. Какой инструмент используется для визуализации и приоритезации рисков?

1. Матрица рисков
2. Дерево атак
3. Диаграмма Ишикавы
4. SWOT-анализ

6. Что означает "риск-аппетит" организации?

1. Максимальный уровень риска, который готова принять организация
2. Минимальный уровень защиты
3. Количество инцидентов в год
4. Бюджет на безопасность

Раздел 3. Идентификация активов. Виды уязвимостей

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 3.2. Природа и классификация уязвимостей

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что из нижеперечисленного относится к методу передачи риска?

1. Проведение тестирования на проникновения
2. Страхование рисков
3. Резервирование данных
4. Шифрование

2. Какой стандарт описывает методы оценки рисков OCTAVE?

1. NIST SP 800-30
2. ISO 27005
3. OCTAVE Allegro
4. COBIT

3. Какой процесс помогает выявить новые риски после изменений в ИТ-инфраструктуре?

1. Тестирование на проникновение
2. Пересмотр рисков
3. Резервное копирование
4. Мониторинг трафика

4. Какой из перечисленных факторов НЕ влияет на оценку рисков?

1. Стоимость актива

2. Вероятность угрозы
3. Количество сотрудников в компании
4. Уровень защиты
5. Какой вид мер для снижения рисков предполагает обучение сотрудников?
1. Технические меры
2. Организационные меры
3. Физические меры
4. Страхование

Раздел 4. Методы моделирования угроз и оценки рисков ИБ

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 4.3. Практическое применение матриц рисков и вычисление уровня риска

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой документ фиксирует выявленные риски и меры по их обработке?
1. Реестр рисков
2. Политика безопасности
3. Инструкция по реагированию
4. Отчет аудита
2. Какой подход предполагает анализ рисков на основе сценариев атак?
1. Матрица рисков
2. Анализ дерева событий
3. Метод Дельфи
4. Оценка стоимости риска
3. Какой показатель используется в количественном анализе для оценки потенциальных потерь?
1. ALE (Annual Loss Expectancy)
2. ROI (Return on Investment)
3. MTBF (Service Level Agreement)
4. SLA (Service Level Agreement)
4. Какой метод оценки рисков основан на мнении экспертов?
1. Статистический анализ
2. Метод Дельфи
3. Матрица вероятностей
4. Анализ уязвимостей
5. Какой процесс позволяет минимизировать последствия реализовавшегося риска?
1. Превентивные меры
2. Реагирование на инциденты
3. Шифрование данных
4. Резервное копирование
6. Какой метод управления рисками предполагает полный отказ от опасной деятельности?
1. Снижение риска
2. Принятие риска
3. Избегание риска
4. Передача риска

Раздел 5. Методы обработки рисков ИБ. Виды мер для снижения рисков ИБ

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 5.2. Классификация мер защиты и выбор средств обеспечения безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой показатель определяет частоту реализации угрозы?
 1. ARO (Annual Rate of Occurrence)
 2. SLE (Single Loss Expectancy)
 3. RPO (Recovery Point Objective)
 4. RTO (Recovery Time Objective)
2. Какой этап управления рисками выполняется последним?
 1. Идентификация рисков
 2. Оценка рисков
 3. Мониторинг и пересмотр рисков
 4. Обработка рисков
3. Какой из перечисленных методов НЕ является методом качественной оценки рисков?
 1. Матрица вероятностей и последствий
 2. Метод Дельфи
 3. Анализ ALE (Annual Loss Expectancy)
 4. Сценарный анализ
4. Какой термин описывает процесс уменьшения вероятности реализации угрозы?
 1. Минимизация риска
 2. Принятие риска
 3. Передача риска
 4. Избегание риска

Раздел 6. Мониторинг и пересмотр рисков ИБ

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 6.1. Непрерывный мониторинг событий и управление инцидентами ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое «SLE» (Single Loss Expectancy) в количественном анализе рисков?
 1. Ожидаемая частота инцидента в год
 2. Ожидаемый ущерб от одного инцидента
 3. Стоимость внедрения средств защиты
 4. Вероятность успешной атаки
2. Какой метод управления рисками предполагает использование резервных систем?
 1. Избегание риска
 2. Передача риска
 3. Снижение риска
 4. Принятие риска
3. Какой документ определяет действия при реализации риска?
 1. Политика безопасности
 2. План реагирования на инциденты
 3. Реестр активов
 4. Инструкция по резервному копированию
4. Какой показатель определяет максимально допустимое время простоя системы?
 1. RTO (Recovery Time Objective)
 2. RPO (Recovery Point Objective)
 3. MTBF (Mean Time Between Failures)

4. SLA (Service Level Agreement)

Раздел 7. Подготовка отчетности. Заказчики результатов оценки рисков ИБ

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 7.2. Взаимодействие с заинтересованными сторонами и предоставление результатов оценки

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой метод оценки рисков использует числовые значения вероятности и ущерба?
 1. Качественный анализ
 2. Количественный анализ
 3. Экспертный анализ
 4. Сравнительный анализ
2. Какой из перечисленных факторов относится к внешним угрозам?
 1. Ошибки сотрудников
 2. Хакерские атаки
 3. Устаревшее ПО
 4. Отказ оборудования
3. Какой процесс помогает выявить скрытые уязвимости в системе?
 1. Управление инцидентами
 2. Тестирование на проникновение
 3. Резервное копирование
 4. Мониторинг трафика

Раздел 8. Методологии управления проектами

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 УК-3.1 УК-3.2 УК-3.3 УК-3.4 УК-3.5

Тема 8.1. Классические и гибкие подходы к управлению проектами в сфере ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое "риск-менеджмент"?
 1. Процесс идентификации, оценки и контроля рисков
 2. Устранение всех возможных угроз
 3. Страхование ИТ-инфраструктуры
 4. Проведение аудита безопасности
2. Какой вид мер снижения рисков предполагает использование многофакторной аутентификации?
 1. Организационные меры
 2. Технические меры
 3. Физические меры
 4. Страхование
3. Какой показатель определяет максимально допустимый объем потери данных?
 1. RTO (Recovery Time Objective)
 2. RPO (Recovery Point Objective)
 3. ALE (Annual Loss Expectancy)
 4. SLE (Single Loss Expectancy)

8. Оценочные материалы промежуточной аттестации

7 семестр, Зачет

Контролируемые ИДК: УК-2.1 УК-3.1 УК-2.2 УК-3.2 УК-2.3 УК-3.3 УК-2.4 УК-3.4 УК-2.5 УК-3.5

Вопросы/Задания:

1. Специфика процесса управления рисками ИБ согласно ISO/IEC 27005/ГОСТ Р ИСО/МЭК
2. Процесс управления рисками ИБ согласно ISO/IEC 27005/ГОСТ Р ИСО/МЭК
3. Специфика процесса управления рисками ИБ согласно NIST SP 800-30
4. Процесс управления рисками ИБ согласно NIST SP 800-30
5. Специфика процесса управления рисками ИБ согласно OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
6. Процесс управления рисками ИБ согласно OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
7. Специфика процесса управления рисками ИБ согласно FRAP (Facilitated Risk Analysis Process)
8. Процесс управления рисками ИБ согласно FRAP (Facilitated Risk Analysis Process)
9. Специфика процесса управления рисками ИБ согласно FAIR (Factor Analysis of Information Risk)
10. Процесс управления рисками ИБ согласно FAIR (Factor Analysis of Information Risk)
11. Место управления рисками в ИБ
12. Почему необходимо управление рисками ИБ в компании
13. Заказчики рисков ИБ
14. Активы, для которых следует проводить анализ рисков ИБ
15. Что такое PMBoK?
16. Основные части PMBoK
17. Основные принципы управления проектами согласно PMBoK
18. Этапы управления проектами согласно PMBoK
19. Домены знаний согласно PMBoK
20. Что такое методология Waterfall? Преимущества, недостатки

21. Что такое методология Agile? Преимущества, недостатки, подходящие проекты
22. Что такое методология Scrum? Преимущества, недостатки
23. Что такое методология Kanban? Принципы
24. Что такое методология Six Sigma? Принципы и алгоритмы
25. Что такое методология Экстремальное программирование (XP)? Ценности и основные практики
26. Методология моделирования угроз STRIDE
27. Методология ранжирования угроз DREAD
28. Методология моделирования угроз PASTA
29. Методология моделирования угроз VAST
30. Моделирование угроз Trike
31. Количественная оценка рисков ИБ
32. Анализ дерева событий (ETA)
33. Метод анализа иерархий (МАИ)
34. Моделирование методом Монте-Карло
35. Оценка стоимости риска (RAV)
36. Ожидаемая годовая потеря (ALE)
37. Качественная оценка рисков ИБ
38. Анализ рисков на основе экспертных оценок
39. Матрица рисков
40. Метод Дельфи
41. SWOT-анализ
42. PESTEL-анализ

9. Материально-техническое и учебно-методическое обеспечение дисциплины

9.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Тумбинская М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник: учебник / М. В. Тумбинская, М. В. Петровский. - Санкт-Петербург: Лань, 2022. - 344 с. - 978-5-8114-3940-9. - Текст: электронный. // Издательство Лань: [сайт]. - URL: <https://e.lanbook.com/img/cover/book/207095.jpg> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Милославская Н. Г. Управление информационной безопасностью. Конспект лекций: учебное пособие: учебное пособие / Н. Г. Милославская, А. И. Толстой. - Управление информационной безопасностью. Конспект лекций - Москва: Национальный исследовательский ядерный университет «МИФИ», 2020. - 534 с. - 978-5-7262-2694-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/125513.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Газизов А. Р. Управление информационной безопасностью: учебное пособие: учебное пособие / А. Р. Газизов, С. Б. Петренкова, Д. В. Фатхи. - Управление информационной безопасностью - Ростов-на-Дону: Донской государственный технический университет, 2019. - 115 с. - 978-5-7890-1775-3. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/117771.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

2. Шилов А. К. Управление информационной безопасностью: учебное пособие: учебное пособие / А. К. Шилов. - Управление информационной безопасностью - Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2018. - 120 с. - 978-5-9275-2742-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/87643.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://znanium.ru/> - Электронно-библиотечная система "Znaniy"
2. <https://www.elibrary.ru/> - НЭБ eLIBRARY
3. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"
4. <https://www.elibrary.ru/> - НЭБ eLIBRARY
5. <https://rusneb.ru/> - Национальная электронная библиотека (НЭБ)

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 - 1 шт.

Моноблок - 32 шт.

Проектор - 3 шт.

Автоматизированное рабочее место (АРМ) - 15 шт.

Плоттер - 1 шт.

Сканер - 1 шт.

Лекционная аудитория

Лекционный мультимедийный комплекс - 3 шт.

Проектор - 3 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;
- Методическими рекомендациями по организации самостоятельной работы студентов МИИГАиК;

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.