



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.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
«Б1.О.19.07 КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА
ИНФОРМАТИЗАЦИИ»**

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:

Доцент кафедры Информационно-измерительных систем, к.т.н.

Дубов С. С.

Преподаватель кафедры Информационно-измерительных систем

Носенко О. В.

Фонд оценочных средств по дисциплине (модулю) составлен 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

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

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

ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба

ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты

Знать:

ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности

Уметь:

ОПК-2.1.1/Ум1 Выявлять угрозы информационной безопасности применительно к объектам защиты

Владеть:

ОПК-2.1.1/Нв1 Навыками описания объекта информатизации как совокупности информационных, технических, программных и человеческих ресурсов, объединенных для реализации конкретного функционального процесса

ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели

Знать:

ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации

Уметь:

ОПК-2.1.2/Ум1 Определять меры необходимые для снижения рисков реализации угроз информационной безопасности

Владеть:

ОПК-2.1.2/Нв1 Методиками анализа и категорирования потенциальных угроз информационной безопасности (нарушение конфиденциальности, целостности, доступности) применительно к конкретным элементам объекта защиты

ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб

Знать:

ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации

Уметь:

ОПК-2.1.3/Ум1 Определять объект защиты и методы дестабилизирующего воздействия на него

Владеть:

ОПК-2.1.3/Нв1 Навыками построения сценариев реализации угроз, описывающих возможные пути проникновения и деструктивного воздействия на объект

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
---	-------------------	---

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	Повышенный	ИДК 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 ИДК 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
--	-------------------	--

ИДК 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)

ИДК 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

	ИДК 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
Базовый	ИДК 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 ИДК 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

ИДК 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

ИДК 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

ИДК 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
Пороговый	ИДК 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 ИДК 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 ИДК 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 ИДК 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

		ИДК 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
ОПК-2.1 Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Повышенный	ИДК ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты Знать: ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности Уметь: ОПК-2.1.1/Ум1 Выявлять угрозы информационной безопасности применительно к объектам защиты Владеть: ОПК-2.1.1/Нв1 Навыками описания объекта информатизации как совокупности информационных, технических, программных и человеческих ресурсов, объединенных для реализации конкретного функционального процесса ИДК ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели Знать: ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации Уметь: ОПК-2.1.2/Ум1 Определять меры необходимые для снижения рисков реализации угроз информационной безопасности Владеть: ОПК-2.1.2/Нв1 Методиками анализа и категорирования потенциальных угроз информационной безопасности (нарушение конфиденциальности, целостности, доступности) применительно к конкретным элементам объекта защиты

	ИДК ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб Знать: ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации Уметь: ОПК-2.1.3/Ум1 Определять объект защиты и методы дестабилизирующего воздействия на него Владеть: ОПК-2.1.3/Нв1 Навыками построения сценариев реализации угроз, описывающих возможные пути проникновения и деструктивного воздействия на объект
Базовый	ИДК ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты Знать: ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности Уметь: ОПК-2.1.1/Ум1 Выявлять угрозы информационной безопасности применительно к объектам защиты ИДК ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели Знать: ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации Уметь: ОПК-2.1.2/Ум1 Определять меры необходимые для снижения рисков реализации угроз информационной безопасности ИДК ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб Знать: ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации Уметь: ОПК-2.1.3/Ум1 Определять объект защиты и методы дестабилизирующего воздействия на него

	Пороговый ИДК ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты Знать: ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности ИДК ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели Знать: ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации ИДК ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб Знать: ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации
--	---

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	УК-2.1 Формулирует проблему, решение которой напрямую связано с достижением цели проекта 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 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 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

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

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

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

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

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

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

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

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

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

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

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

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

	ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности ОПК-2.1.1/Ум1 Выявлять угрозы информационной безопасности применительно к объектам защиты ОПК-2.1.1/Нв1 Навыками описания объекта информатизации как совокупности информационных, технических, программных и человеческих ресурсов, объединенных для реализации конкретного функционального процесса ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации ОПК-2.1.2/Ум1 Определять меры необходимые для снижения рисков реализации угроз информационной безопасности ОПК-2.1.2/Нв1 Методиками анализа и категорирования потенциальных угроз информационной безопасности (нарушение конфиденциальности, целостности, доступности) применительно к конкретным элементам объекта защиты ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации ОПК-2.1.3/Ум1 Определять объект защиты и методы дестабилизирующего воздействия на него ОПК-2.1.3/Нв1 Навыками построения сценариев реализации угроз, описывающих возможные пути проникновения и деструктивного воздействия на объект
Хорошо	УК-2.1 Формулирует проблему, решение которой напрямую связано с достижением цели проекта 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 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 УК-2.2 Определяет связи между поставленными задачами и ожидаемые результаты их решения УК-2.2/Зн1 Методики декомпозиции задач и планирования проектов, основы логической структуры проектной деятельности, показатели эффективности решений в сфере информационной безопасности 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

	УК-2.3 Анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач УК-2.3/Зн1 Принципы календарного и сетевого планирования проектов, методы оптимизации проектных решений, ограничения и риски в реализации проектов по информационной безопасности УК-2.3/Ум1 Читать и анализировать план-графики реализации проектов, сравнивать альтернативные способы достижения задач УК-2.4 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы УК-2.4/Зн1 Основы ресурсного обеспечения проектов, действующее законодательство в области информационной безопасности и смежных областях, ограничения, накладываемые нормативными актами и регуляторами УК-2.4/Ум1 Идентифицировать правовые, ресурсные и организационные ограничения, оценивать доступные ресурсы (трудовые, временные, информационные), применять правовые нормы в контексте проектной деятельности 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 УК-2.5/Зн1 Подходы к контролю и оценке проектных результатов, методы оценки эффективности реализованных мероприятий, критерии качества выполнения задач в области информационной безопасности 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 ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности ОПК-2.1.1/Ум1 Выявлять угрозы информационной безопасности применительно к объектам защиты ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации ОПК-2.1.2/Ум1 Определять меры необходимые для снижения рисков реализации угроз информационной безопасности ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации ОПК-2.1.3/Ум1 Определять объект защиты и методы дестабилизирующего воздействия на него
Удовлетворительно	УК-2.1 Формулирует проблему, решение которой напрямую связано с достижением цели проекта 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

	УК-2.2 Определяет связи между поставленными задачами и ожидаемые результаты их решения УК-2.2/Зн1 Методики декомпозиции задач и планирования проектов, основы логической структуры проектной деятельности, показатели эффективности решений в сфере информационной безопасности УК-2.3 Анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач УК-2.3/Зн1 Принципы календарного и сетевого планирования проектов, методы оптимизации проектных решений, ограничения и риски в реализации проектов по информационной безопасности УК-2.4 В рамках поставленных задач определяет имеющиеся ресурсы и ограничения, действующие правовые нормы УК-2.4/Зн1 Основы ресурсного обеспечения проектов, действующее законодательство в области информационной безопасности и смежных областях, ограничения, накладываемые нормативными актами и регуляторами 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 УК-2.5/Зн1 Подходы к контролю и оценке проектных результатов, методы оценки эффективности реализованных мероприятий, критерии качества выполнения задач в области информационной безопасности ОПК-2.1.1 Формулирует характеристики объекта защиты, его функциональных составляющих, понимает сущность функционального процесса объекта защиты ОПК-2.1.1/Зн1 Цели, задачи, принципы и основные направления обеспечения информационной безопасности ОПК-2.1.2 Выявляет потенциальные угрозы объекта защиты, их возможные цели ОПК-2.1.2/Зн1 Методологические подходы к защите информации и принципы ее организации ОПК-2.1.3 Прогнозирует пути реализации потенциальных угроз и оценивает предполагаемый ущерб ОПК-2.1.3/Зн1 Кадровое и ресурсное обеспечение защиты информации
Неудовлетворительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование
Промежуточная аттестация	Экзамен

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Введение	УК-2.1 УК-2.2 ОПК-2.1.1 ОПК-2.1.2	Тестирование	Экзамен

2	Методы оргпроектирования систем защиты информации	УК-2.1 УК-2.4 ОПК-2.1.2 ОПК-2.1.3	Тестирование	Экзамен
3	Разработка документации оргпроцессов при проектировании систем защиты информации	УК-2.2 УК-2.3 ОПК-2.1.1 ОПК-2.1.2	Тестирование	Экзамен
4	Методика определения структурного построения и состава сотрудников службы защиты информации и разработка организационно-нормативных документов, регламентирующих деятельность службы	УК-2.2 УК-2.3 ОПК-2.1.2 ОПК-2.1.3	Тестирование	Экзамен
5	Выбор оборудования и технических средств для оснащения рабочих мест сотрудников, разработка мероприятий по охране труда, технике безопасности и пожарной безопасности	УК-2.4 УК-2.5 ОПК-2.1.1	Тестирование	Экзамен
6	Проектирование информационного обеспечения системы защиты информации	УК-2.1 УК-2.3 УК-2.5 ОПК-2.1.2	Тестирование	Экзамен
7	Разработка мероприятий по работе в «особом периоде» и в «чрезвычайных обстоятельствах»	УК-2.5 ОПК-2.1.2 ОПК-2.1.3	Тестирование	Экзамен
8	Внедрение и оценка эффективности оргпроекта	УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3	Тестирование	Экзамен

5. 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, 7 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 наличия 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.

6. Оценочные материалы текущего контроля

Раздел 1. Введение

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 УК-2.1 УК-2.2

Тема 1.1. Введение

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что понимается под оргпроектированием в области защиты информации?
 1. Процесс закупки средств защиты для объекта информатизации
 2. Деятельность по созданию или совершенствованию системы ЗИ
 3. Разработка инструкций для пользователей ПЭВМ
 4. План проведения проверок режима секретности
2. Какой принцип оргпроектирования ЗИ предполагает учет всех возможных каналов утечки информации?
 1. Принцип законности
 2. Принцип иерархичности
 3. Принцип комплексности
 4. Принцип непрерывности
3. В чем заключается особенность оргпроектирования систем защиты информации?
 1. Проект не требует дальнейшей корректировки
 2. Система ЗИ является подсистемой системы управления объектом
 3. Основной упор делается на технические средства защиты
 4. Проектирование всегда выполняется только сторонними организациями

Раздел 2. Методы оргпроектирования систем защиты информации

Контролируемые ИДК: ОПК-2.1.2 ОПК-2.1.3 УК-2.1 УК-2.4

Тема 2.1. Методы оргпроектирования систем защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой этап является первым в процессе оргпроектирования ЗИ?
 1. Разработка рабочей документации
 2. Техническое проектирование
 3. Внедрение оргпроекта

4. Предпроектное обследование

2. Чем комплексное оргпроектирование отличается от локального?

1. Сроком проектирования
2. Количеством разработчиков в группе
3. Стоимостью работ
4. Охватом всех элементов системы ЗИ и стадий жизненного цикла объекта

3. Что из перечисленного является направлением оргпроектирования?

1. Проектирование организационной структуры службы ЗИ
2. Разработка архитектуры здания
3. Выбор офисной мебели для службы ЗИ
4. Проектирование интерфейса пользователя

4. Какое требование относится к основному составу требований к оргпроектированию ЗИ?

1. Требование минимальной численности сотрудников
2. Требование использования только импортного оборудования
3. Требование соответствия законодательству РФ
4. Требование максимальной стоимости проекта

Раздел 3. Разработка документации оргпроцессов при проектировании систем защиты информации

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 УК-2.2 УК-2.3

Тема 3.1. Разработка документации оргпроцессов при проектировании систем защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой методический документ обеспечивает процесс оргпроектирования ЗИ?

1. Устав организации
2. Должностная инструкция системного администратора
3. Трудовой кодекс РФ
4. Техническое задание на создание системы ЗИ

2. Какой метод относится к методам, используемым в оргпроектировании ЗИ?

1. Метод инвентаризации
2. Метод моделирования
3. Метод проб и ошибок
4. Метод хронометража

3. Какова цель диагностики объекта оргпроектирования?

1. Назначение ответственных лиц за защиту информации
2. Проведение инвентаризации основных средств
3. Установка антивирусного программного обеспечения
4. Получение полной и достоверной информации о состоянии объекта и системы ЗИ

Раздел 4. Методика определения структурного построения и состава сотрудников службы защиты информации и разработка организационно- нормативных документов, регламентирующих деятельность службы

Контролируемые ИДК: ОПК-2.1.2 ОПК-2.1.3 УК-2.2 УК-2.3

Тема 4.1. Методика определения структурного построения и состава сотрудников службы защиты информации и разработка организационно- нормативных документов, регламентирующих деятельность службы

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. К методам сбора информации при оргпроектировании относится:

1. Произвольное наблюдение
2. Штрафование персонала
3. Анкетирование сотрудников
4. Штатное расписание

2. Чем матричные методы проектирования отличаются от графических?

1. Графические методы всегда точнее матричных
2. Матричные методы позволяют отразить параметрические связи между элементами
3. Отличий не существует, это одно и то же
4. Матричные методы проще в разработке

3. Кто выступает в роли субъекта оргпроектирования ЗИ?

1. Объект информатизации
2. Защищаемая информация
3. Технические средства защиты
4. Разработчик оргпроекта (проектная группа)

4. Для чего определяется параметрическая зависимость между элементами объекта и субъекта оргпроектирования?

1. Для увеличения бюджета проекта
2. Для определения графика отпусков
3. Для расчета штатной численности подразделений службы ЗИ
4. Для обоснования выбора организационной структуры службы ЗИ

Раздел 5. Выбор оборудования и технических средств для оснащения рабочих мест сотрудников, разработка мероприятий по охране труда, технике безопасности и пожарной безопасности

Контролируемые ИДК: ОПК-2.1.1 УК-2.4 УК-2.5

Тема 5.1. Выбор оборудования и технических средств для оснащения рабочих мест сотрудников, разработка мероприятий по охране труда, технике безопасности и пожарной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В чем особенность иерархического построения службы ЗИ?

1. Наличие нескольких уровней управления с распределением полномочий
2. Подчинение только внешним консультантам
3. Все сотрудники подчиняются напрямую главному инженеру
4. Полное отсутствие подчинения

2. На основе чего производится расчет штатной численности подразделений службы ЗИ?

1. Случайным образом
2. На основе нормативов и объемов решаемых задач
3. По количеству компьютеров в офисе, умноженному на два
4. Исходя из пожеланий начальника службы

3. Каков порядок разработки положения о службе ЗИ?

1. Сбор информации, разработка проекта, согласование, утверждение
2. Разработка инструкций для сотрудников, затем разработка положения
3. Положение не требуется, достаточно устного распоряжения
4. Утверждение, подписание, согласование

4. Что относится к документационному обеспечению оргпроекта службы ЗИ?

1. Приказы о приеме на работу
2. Табель учета рабочего времени
3. Личные дела сотрудников

4. Техническая документация на средства защиты

Раздел 6. Проектирование информационного обеспечения системы защиты информации

Контролируемые ИДК: ОПК-2.1.2 УК-2.1 УК-2.3 УК-2.5

Тема 6.1. Проектирование информационного обеспечения системы защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является результатом проектирования организационной модели службы ЗИ?

1. План эвакуации при пожаре
2. Схема организационной структуры
3. График дежурств на месяц
4. Смета расходов на канцелярию

2. Какой фактор влияет на структурное построение службы ЗИ?

1. Наличие свободных кабинетов
2. Количество уровней управления на предприятии
3. Личные предпочтения руководителя предприятия
4. Размер и структура объекта информатизации

3. Что подлежит проектированию при разработке информационного обеспечения деятельности системы ЗИ?

1. График проведения планерок
2. Дизайн пропусков
3. Система классификации и кодирования информации
4. Система оплаты труда сотрудников

4. На этапе анализа объекта информатизации специалистом по защите информации было установлено, что сотрудники организации имеют доступ к серверу с конфиденциальными данными в нерабочее время без использования средств видеонаблюдения и без письменного разрешения руководства. К какой категории следует отнести данный недостаток при построении модели угроз?

1. Аппаратная уязвимость
2. Программная уязвимость
3. Организационная уязвимость
4. Естественная угроза

Раздел 7. Разработка мероприятий по работе в «особом периоде» и в «чрезвычайных обстоятельствах»

Контролируемые ИДК: ОПК-2.1.2 ОПК-2.1.3 УК-2.5

Тема 7.1. Разработка мероприятий по работе в «особом периоде» и в «чрезвычайных обстоятельствах»

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие требования к технике безопасности учитываются при разработке проекта?

1. Требования к освещению рабочих мест с дисплеями
2. Требования к организации режима труда и отдыха персонала
3. Требования к параметрам микроклимата в серверных помещениях
4. Требования электробезопасности при эксплуатации средств ЗИ

2. Какое требование предъявляется к проекту функционирования системы ЗИ в период ЧС?

1. Отключение всех средств сигнализации
2. Обеспечение сохранности носителей информации и бесперебойной связи
3. Эвакуация всей оргтехники в первую очередь

4. Полное прекращение работы системы ЗИ

3. Что входит в состав оргпроекта технического оснащения системы ЗИ?

1. Инструкция по использованию принтера
2. Гарантийные талоны на оборудование
3. Ведомость потребности в технических средствах защиты
4. План проведения ремонтных работ

Раздел 8. Внедрение и оценка эффективности оргпроекта

Контролируемые ИДК: ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5

Тема 8.1. Внедрение и оценка эффективности оргпроекта

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой критерий используется для оценки эффективности оргпроекта?
 1. Степень достижения поставленных целей защиты информации
 2. Удобство пользования документацией для сотрудников
 3. Соответствие проекта современным тенденциям дизайна
 4. Количество внесенных в проект изменений в процессе разработки
2. Какой метод оценки эффективности используется при оргпроектировании?
 1. Метод индукции
 2. Дедуктивный метод
 3. Метод «черного ящика»
 4. Метод сравнения с базовым вариантом
3. Что разрабатывается в рамках документации оргпроцессов при проектировании систем ЗИ?
 1. Устав организации
 2. Должностные инструкции сотрудников службы ЗИ
 3. Приказ о создании предприятия
 4. Штатное расписание всего предприятия
4. Какой фактор определяет состав проектных работ при рационализации системы ЗИ?
 1. Требования вышестоящей организации
 2. Результаты анализа эффективности действующей системы ЗИ
 3. Наличие свободных финансовых средств
 4. Плановые сроки проведения модернизации
5. Что является завершающим этапом организации процесса внедрения оргпроекта?
 1. Обучение персонала работе с новой системой
 2. Закупка оборудования
 3. Написание технического задания
 4. Подписание акта о приемке в эксплуатацию

7. Оценочные материалы промежуточной аттестации

7 семестр, Экзамен

Контролируемые ИДК: УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-2.1.1 ОПК-2.1.2 ОПК-2.1.3

Вопросы/Задания:

1. Сущность и понятие оргпроектирования в области защиты информации.
2. Принципы оргпроектирования защиты информации.
3. Особенности оргпроектирования систем защиты информации.

4. Этапы процесса оргпроектирования защиты информации.
5. Отличия локального оргпроектирования от комплексного.
6. Направления оргпроектирования.
7. Основной состав требований к оргпроектированию защиты информации.
8. Методические документы, обеспечивающие процесс оргпроектирования защиты информации.
9. Методы, используемые в оргпроектировании защиты информации.
10. Диагностика объекта оргпроектирования защиты информации.
11. Методы, используемые для проведения диагностики системы защиты информации при оргпроектировании.
12. Методы сбора информации при оргпроектировании.
13. Отличия матричных методов проектирования от графических методов.
14. Понятие и состав объектов и субъектов оргпроектирования защиты информации.
15. Определение параметрической зависимости между элементами объекта и субъекта оргпроектирования.
16. Особенности иерархического построения службы ЗИ при оргпроектировании.
17. Методика расчета штатной численности подразделений службы ЗИ.
18. Порядок разработки положений о службе ЗИ и ее структурных подразделений.
19. Документационное обеспечение оргпроекта службы ЗИ.
20. Проектирование организационной и функциональной модели службы ЗИ.
21. Условия и факторы, влияющие на структурное построение службы ЗИ.
22. Основные элементы, подлежащие проектированию при разработке информационного обеспечения деятельности системы ЗИ.
23. Требования к технике безопасности и пожарной безопасности при разработке проекта.
24. Требования, предъявляемые к проекту функционирования системы ЗИ в период чрезвычайных ситуаций.
25. Состав оргпроекта технического оснащения системы ЗИ.

26. Критерии оценки эффективности оргпроекта.
27. Методы оценки эффективности, используемые при оргпроектировании.
28. Разработка документации оргпроцессов при проектировании систем защиты информации.
29. Состав проектных работ и факторы, определяющие их при рационализации системы ЗИ.
30. Этапы организации процесса внедрения оргпроекта.