



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.19.05 ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА 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
Калмыков С. А.

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

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности

ОПК-2.1 Осуществляет профессиональную деятельность с учетом экономических ограничений на всех этапах жизненного цикла технических объектов и процессов

Знать:

ОПК-2.1/Зн8 Структуру затрат жизненного цикла мер ИБ

Уметь:

ОПК-2.1/Ум7 Выбирать состав мер защиты и инструментов с учетом ограничений бюджета и трудоемкости сопровождения

Владеть:

ОПК-2.1/Нв7 Навыками приоритизации мер защиты по критичности активов и ожидаемому эффекту, подготовки укрупненного обоснования затрат и плана внедрения

ОПК-2.2 Осуществляет профессиональную деятельность с учетом экологических ограничений на всех этапах жизненного цикла технических объектов и процессов

Знать:

ОПК-2.2/Зн8 Факторы экологического воздействия ИТ/ИБ-инфраструктуры и принципы ресурсной эффективности

Уметь:

ОПК-2.2/Ум6 Проектировать режимы эксплуатации мер защиты с учетом ресурсных ограничений

Владеть:

ОПК-2.2/Нв7 Навыками настройки параметров мониторинга и хранения данных безопасности с учетом устойчивости системы и рационального потребления ресурсов

ОПК-2.3 Осуществляет профессиональную деятельность с учетом социальных и других ограничений на всех этапах жизненного цикла технических объектов и процессов

Знать:

ОПК-2.3/Зн7 Принципы учета человеческого фактора и организационных ограничений

Уметь:

ОПК-2.3/Ум6 Формулировать правила и требования к пользователям и администраторам с учетом ролей и процессов организации

Владеть:

ОПК-2.3/Нв7 Навыками разработки кратких инструкций и регламентов, проведения инструктажа и документирования ответственности и процедур

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики

Знать:

ОПК-10.1/Зн2 Процесс разработки политики ИБ и комплекта организационно-распорядительных документов

Уметь:

ОПК-10.1/Ум2 Разрабатывать проект Политики ИБ, включая цели, принципы, область действия, роли/ответственность и различные требования

Владеть:

ОПК-10.1/Нв2 Навыками анализа документов при разработке Политики ИБ

ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности

Знать:

ОПК-10.2/Зн3 Типовые процессы управления доступом/ролями, конфигурациями, обновлениями, уязвимостями, журналированием/мониторингом, реагированием

Уметь:

ОПК-10.2/Ум3 Планировать и организовывать внедрение доступных инструментов для организации защиты информации

Владеть:

ОПК-10.2/Нв4 Навыками эксплуатации и поддержки доступных инструментов для организации защиты информации

ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности

Знать:

ОПК-10.3/Зн3 Основы управления процессами ИБ, риск-ориентированный подход к выбору и контролю мер защиты

Уметь:

ОПК-10.3/Ум3 Анализировать результаты мониторинга и сканирования и принимать корректирующие решения по мерам защиты

Владеть:

ОПК-10.3/Нв3 Навыками подготовки отчетности по состоянию ИБ и управления изменениями в конфигурации защитных средств

ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы

ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих

Знать:

ОПК-2.2.1/Зн2 Процесс проектирования подсистемы защиты информационной системы

Уметь:

ОПК-2.2.1/Ум2 Анализировать структуру защиты ИС и выявлять недостатки

Владеть:

ОПК-2.2.1/Нв2 Навыками формирования модели угроз на основании актуальной нормативно-методической базы

ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы

Знать:

ОПК-2.2.2/Зн2 Классы угроз для информационной системы

Уметь:

ОПК-2.2.2/Ум2 Формировать модель угроз для информационной системы, спроектированной на основе доступных инструментов

Владеть:

ОПК-2.2.2/Нв2 Защитных мер против деструктивных воздействий

ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта

Знать:

ОПК-2.2.3/Зн2 Принципы оптимизации защиты

Уметь:

ОПК-2.2.3/Ум2 Разрабатывать предложения по улучшению организации защиты с учетом ограничений и целей информационных систем

Владеть:

ОПК-2.2.3/Нв2 Навыками подготовки плана внедрения мероприятий и их документирования для определения эффективности процессов ИБ

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	Повышенный	ИДК ОПК-2.1 Осуществляет профессиональную деятельность с учетом экономических ограничений на всех этапах жизненного цикла технических объектов и процессов <i>Знать:</i> ОПК-2.1/Зн8 Структуру затрат жизненного цикла мер ИБ <i>Уметь:</i> ОПК-2.1/Ум7 Выбирать состав мер защиты и инструментов с учетом ограничений бюджета и трудоемкости сопровождения <i>Владеть:</i> ОПК-2.1/Нв7 Навыками приоритизации мер защиты по критичности активов и ожидаемому эффекту, подготовки укрупненного обоснования затрат и плана внедрения ИДК ОПК-2.2 Осуществляет профессиональную деятельность с учетом экологических ограничений на всех этапах жизненного цикла технических объектов и процессов <i>Знать:</i> ОПК-2.2/Зн8 Факторы экологического воздействия ИТ/ИБ-инфраструктуры и принципы ресурсной эффективности <i>Уметь:</i> ОПК-2.2/Ум6 Проектировать режимы эксплуатации мер защиты с учетом ресурсных ограничений

	Владеть: ОПК-2.2/Нв7 Навыками настройки параметров мониторинга и хранения данных безопасности с учетом устойчивости системы и рационального потребления ресурсов ИДК ОПК-2.3 Осуществляет профессиональную деятельность с учетом социальных и других ограничений на всех этапах жизненного цикла технических объектов и процессов Знать: ОПК-2.3/Зн7 Принципы учета человеческого фактора и организационных ограничений Уметь: ОПК-2.3/Ум6 Формулировать правила и требования к пользователям и администраторам с учетом ролей и процессов организации Владеть: ОПК-2.3/Нв7 Навыками разработки кратких инструкций и регламентов, проведения инструктажа и документирования ответственности и процедур
Базовый	ИДК ОПК-2.1 Осуществляет профессиональную деятельность с учетом экономических ограничений на всех этапах жизненного цикла технических объектов и процессов Знать: ОПК-2.1/Зн8 Структуру затрат жизненного цикла мер ИБ Уметь: ОПК-2.1/Ум7 Выбирать состав мер защиты и инструментов с учетом ограничений бюджета и трудоемкости сопровождения ИДК ОПК-2.2 Осуществляет профессиональную деятельность с учетом экологических ограничений на всех этапах жизненного цикла технических объектов и процессов Знать: ОПК-2.2/Зн8 Факторы экологического воздействия ИТ/ИБ-инфраструктуры и принципы ресурсной эффективности Уметь: ОПК-2.2/Ум6 Проектировать режимы эксплуатации мер защиты с учетом ресурсных ограничений

	ИДК ОПК-2.3 Осуществляет профессиональную деятельность с учетом социальных и других ограничений на всех этапах жизненного цикла технических объектов и процессов Знать: ОПК-2.3/Зн7 Принципы учета человеческого фактора и организационных ограничений Уметь: ОПК-2.3/Ум6 Формулировать правила и требования к пользователям и администраторам с учетом ролей и процессов организации
Пороговый	ИДК ОПК-2.1 Осуществляет профессиональную деятельность с учетом экономических ограничений на всех этапах жизненного цикла технических объектов и процессов Знать: ОПК-2.1/Зн8 Структуру затрат жизненного цикла мер ИБ ИДК ОПК-2.2 Осуществляет профессиональную деятельность с учетом экологических ограничений на всех этапах жизненного цикла технических объектов и процессов Знать: ОПК-2.2/Зн8 Факторы экологического воздействия ИТ/ИБ-инфраструктуры и принципы ресурсной эффективности ИДК ОПК-2.3 Осуществляет профессиональную деятельность с учетом социальных и других ограничений на всех этапах жизненного цикла технических объектов и процессов Знать: ОПК-2.3/Зн7 Принципы учета человеческого фактора и организационных ограничений

ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	Повышенный	ИДК ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики Знать: ОПК-10.1/Зн2 Процесс разработки политики ИБ и комплекта организационно-распорядительных документов Уметь: ОПК-10.1/Ум2 Разрабатывать проект Политики ИБ, включая цели, принципы, область действия, роли/ответственность и различные требования Владеть: ОПК-10.1/Нв2 Навыками анализа документов при разработке Политики ИБ ИДК ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности Знать: ОПК-10.2/Зн3 Типовые процессы управления доступом/ролями, конфигурациями, обновлениями, уязвимостями, журналированием/мониторингом, реагированием Уметь: ОПК-10.2/Ум3 Планировать и организовывать внедрение доступных инструментов для организации защиты информации Владеть: ОПК-10.2/Нв4 Навыками эксплуатации и поддержки доступных инструментов для организации защиты информации ИДК ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности Знать: ОПК-10.3/Зн3 Основы управления процессами ИБ, риск-ориентированный подход к выбору и контролю мер защиты Уметь: ОПК-10.3/Ум3 Анализировать результаты мониторинга и сканирования и принимать корректирующие решения по мерам защиты Владеть: ОПК-10.3/Нв3 Навыками подготовки отчетности по состоянию ИБ и управления изменениями в конфигурации защитных средств
--	-------------------	--

Базовый	ИДК ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики Знать: ОПК-10.1/Зн2 Процесс разработки политики ИБ и комплекта организационно-распорядительных документов Уметь: ОПК-10.1/Ум2 Разрабатывать проект Политики ИБ, включая цели, принципы, область действия, роли/ответственность и различные требования ИДК ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности Знать: ОПК-10.2/Зн3 Типовые процессы управления доступом/ролями, конфигурациями, обновлениями, уязвимостями, журналированием/мониторингом, реагированием Уметь: ОПК-10.2/Ум3 Планировать и организовывать внедрение доступных инструментов для организации защиты информации ИДК ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности Знать: ОПК-10.3/Зн3 Основы управления процессами ИБ, риск-ориентированный подход к выбору и контролю мер защиты Уметь: ОПК-10.3/Ум3 Анализировать результаты мониторинга и сканирования и принимать корректирующие решения по мерам защиты
Пороговый	ИДК ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики Знать: ОПК-10.1/Зн2 Процесс разработки политики ИБ и комплекта организационно-распорядительных документов

		ИДК ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности Знать: ОПК-10.2/Зн3 Типовые процессы управления доступом/ролями, конфигурациями, обновлениями, уязвимостями, журналированием/мониторингом, реагированием ИДК ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности Знать: ОПК-10.3/Зн3 Основы управления процессами ИБ, риск-ориентированный подход к выбору и контролю мер защиты
ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы	Повышенный	ИДК ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих Знать: ОПК-2.2.1/Зн2 Процесс проектирования подсистемы защиты информационной системы Уметь: ОПК-2.2.1/Ум2 Анализировать структуру защиты ИС и выявлять недостатки Владеть: ОПК-2.2.1/Нв2 Навыками формирования модели угроз на основании актуальной нормативно-методической базы ИДК ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы Знать: ОПК-2.2.2/Зн2 Классы угроз для информационной системы Уметь: ОПК-2.2.2/Ум2 Формировать модель угроз для информационной системы, спроектированной на основе доступных инструментов Владеть: ОПК-2.2.2/Нв2 Защитных мер против деструктивных воздействий ИДК ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта Знать: ОПК-2.2.3/Зн2 Принципы оптимизации защиты

	Уметь: ОПК-2.2.3/Ум2 Разрабатывать предложения по улучшению организации защиты с учетом ограничений и целей информационных систем Владеть: ОПК-2.2.3/Нв2 Навыками подготовки плана внедрения мероприятий и их документирования для определения эффективности процессов ИБ
Базовый	ИДК ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих Знать: ОПК-2.2.1/Зн2 Процесс проектирования подсистемы защиты информационной системы Уметь: ОПК-2.2.1/Ум2 Анализировать структуру защиты ИС и выявлять недостатки ИДК ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы Знать: ОПК-2.2.2/Зн2 Классы угроз для информационной системы Уметь: ОПК-2.2.2/Ум2 Формировать модель угроз для информационной системы, спроектированной на основе доступных инструментов ИДК ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта Знать: ОПК-2.2.3/Зн2 Принципы оптимизации защиты Уметь: ОПК-2.2.3/Ум2 Разрабатывать предложения по улучшению организации защиты с учетом ограничений и целей информационных систем
Пороговый	ИДК ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих Знать: ОПК-2.2.1/Зн2 Процесс проектирования подсистемы защиты информационной системы ИДК ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы Знать: ОПК-2.2.2/Зн2 Классы угроз для информационной системы

		ИДК ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта Знать: ОПК-2.2.3/Зн2 Принципы оптимизации защиты
--	--	--

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ОПК-2.1 Осуществляет профессиональную деятельность с учетом экономических ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.1/Зн8 Структуру затрат жизненного цикла мер ИБ ОПК-2.1/Ум7 Выбирать состав мер защиты и инструментов с учетом ограничений бюджета и трудоемкости сопровождения ОПК-2.1/Нв7 Навыками приоритизации мер защиты по критичности активов и ожидаемому эффекту, подготовки укрупненного обоснования затрат и плана внедрения ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики ОПК-10.1/Зн2 Процесс разработки политики ИБ и комплекта организационно-распорядительных документов ОПК-10.1/Ум2 Разрабатывать проект Политики ИБ, включая цели, принципы, область действия, роли/ответственность и различные требования ОПК-10.1/Нв2 Навыками анализа документов при разработке Политики ИБ ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих ОПК-2.2.1/Зн2 Процесс проектирования подсистемы защиты информационной системы ОПК-2.2.1/Ум2 Анализировать структуру защиты ИС и выявлять недостатки ОПК-2.2.1/Нв2 Навыками формирования модели угроз на основании актуальной нормативно-методической базы ОПК-2.2 Осуществляет профессиональную деятельность с учетом экологических ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.2/Зн8 Факторы экологического воздействия ИТ/ИБ-инфраструктуры и принципы ресурсной эффективности ОПК-2.2/Ум6 Проектировать режимы эксплуатации мер защиты с учетом ресурсных ограничений ОПК-2.2/Нв7 Навыками настройки параметров мониторинга и хранения данных безопасности с учетом устойчивости системы и рационального потребления ресурсов

	ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности ОПК-10.2/Зн3 Типовые процессы управления доступом/ролями, конфигурациями, обновлениями, уязвимостями, журналированием/мониторингом, реагированием ОПК-10.2/Ум3 Планировать и организовывать внедрение доступных инструментов для организации защиты информации ОПК-10.2/Нв4 Навыками эксплуатации и поддержки доступных инструментов для организации защиты информации ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы ОПК-2.2.2/Зн2 Классы угроз для информационной системы ОПК-2.2.2/Ум2 Формировать модель угроз для информационной системы, спроектированной на основе доступных инструментов ОПК-2.2.2/Нв2 Защитных мер против деструктивных воздействий ОПК-2.3 Осуществляет профессиональную деятельность с учетом социальных и других ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.3/Зн7 Принципы учета человеческого фактора и организационных ограничений ОПК-2.3/Ум6 Формулировать правила и требования к пользователям и администраторам с учетом ролей и процессов организации ОПК-2.3/Нв7 Навыками разработки кратких инструкций и регламентов, проведения инструктажа и документирования ответственности и процедур ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности ОПК-10.3/Зн3 Основы управления процессами ИБ, риск-ориентированный подход к выбору и контролю мер защиты ОПК-10.3/Ум3 Анализировать результаты мониторинга и сканирования и принимать корректирующие решения по мерам защиты ОПК-10.3/Нв3 Навыками подготовки отчетности по состоянию ИБ и управления изменениями в конфигурации защитных средств ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта ОПК-2.2.3/Зн2 Принципы оптимизации защиты ОПК-2.2.3/Ум2 Разрабатывать предложения по улучшению организации защиты с учетом ограничений и целей информационных систем ОПК-2.2.3/Нв2 Навыками подготовки плана внедрения мероприятий и их документирования для определения эффективности процессов ИБ
Хорошо	ОПК-2.1 Осуществляет профессиональную деятельность с учетом экономических ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.1/Зн8 Структуру затрат жизненного цикла мер ИБ ОПК-2.1/Ум7 Выбирать состав мер защиты и инструментов с учетом ограничений бюджета и трудоемкости сопровождения ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики ОПК-10.1/Зн2 Процесс разработки политики ИБ и комплекта организационно-распорядительных документов ОПК-10.1/Ум2 Разрабатывать проект Политики ИБ, включая цели, принципы, область действия, роли/ответственность и различные требования

	ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих ОПК-2.2.1/Зн2 Процесс проектирования подсистемы защиты информационной системы ОПК-2.2.1/Ум2 Анализировать структуру защиты ИС и выявлять недостатки ОПК-2.2 Осуществляет профессиональную деятельность с учетом экологических ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.2/Зн8 Факторы экологического воздействия ИТ/ИБ-инфраструктуры и принципы ресурсной эффективности ОПК-2.2/Ум6 Проектировать режимы эксплуатации мер защиты с учетом ресурсных ограничений ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности ОПК-10.2/Зн3 Типовые процессы управления доступом/ролями, конфигурациями, обновлениями, уязвимостями, журналированием/мониторингом, реагированием ОПК-10.2/Ум3 Планировать и организовывать внедрение доступных инструментов для организации защиты информации ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы ОПК-2.2.2/Зн2 Классы угроз для информационной системы ОПК-2.2.2/Ум2 Формировать модель угроз для информационной системы, спроектированной на основе доступных инструментов ОПК-2.3 Осуществляет профессиональную деятельность с учетом социальных и других ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.3/Зн7 Принципы учета человеческого фактора и организационных ограничений ОПК-2.3/Ум6 Формулировать правила и требования к пользователям и администраторам с учетом ролей и процессов организации ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности ОПК-10.3/Зн3 Основы управления процессами ИБ, риск-ориентированный подход к выбору и контролю мер защиты ОПК-10.3/Ум3 Анализировать результаты мониторинга и сканирования и принимать корректирующие решения по мерам защиты ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта ОПК-2.2.3/Зн2 Принципы оптимизации защиты ОПК-2.2.3/Ум2 Разрабатывать предложения по улучшению организации защиты с учетом ограничений и целей информационных систем
Удовлетворительно	ОПК-2.1 Осуществляет профессиональную деятельность с учетом экономических ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.1/Зн8 Структуру затрат жизненного цикла мер ИБ ОПК-10.1 Разрабатывает Политику информационной безопасности, включая цели, задачи, принципы обеспечения информационной безопасности, ответственность за нарушение Политики ОПК-10.1/Зн2 Процесс разработки политики ИБ и комплекта организационно-распорядительных документов

	ОПК-2.2.1 Выявляет достоинства и недостатки структуры и функциональных процессов защиты, его информационных составляющих ОПК-2.2.1/Зн2 Процесс проектирования подсистемы защиты информационной системы ОПК-2.2 Осуществляет профессиональную деятельность с учетом экологических ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.2/Зн8 Факторы экологического воздействия ИТ/ИБ-инфраструктуры и принципы ресурсной эффективности ОПК-10.2 Организует и поддерживает выполнение работы по применению мер обеспечения информационной безопасности ОПК-10.2/Зн3 Типовые процессы управления доступом/ролями, конфигурациями, обновлениями, уязвимостями, журналированием/мониторингом, реагированием ОПК-2.2.2 Выявляет возможные деструктивные воздействия на информационные ресурсы ОПК-2.2.2/Зн2 Классы угроз для информационной системы ОПК-2.3 Осуществляет профессиональную деятельность с учетом социальных и других ограничений на всех этапах жизненного цикла технических объектов и процессов ОПК-2.3/Зн7 Принципы учета человеческого фактора и организационных ограничений ОПК-10.3 Осуществляет управление процессом обеспечения информационной безопасности ОПК-10.3/Зн3 Основы управления процессами ИБ, риск-ориентированный подход к выбору и контролю мер защиты ОПК-2.2.3 Формулирует конструктивные предложения по оптимизации структуры и функциональных процессов защиты объекта ОПК-2.2.3/Зн2 Принципы оптимизации защиты
Неудовлетворительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

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

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Введение в программно-аппаратные средства защиты информации	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-10.1 ОПК-10.2	Тестирование	Курсовая работа Экзамен

2	Проектирование подсистемы защиты информации	ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-2.2.1 ОПК-2.2.2 ОПК-2.2.3	Тестирование	Курсовая работа 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, 6 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.

Промежуточная аттестация: Курсовая работа, 6 семестр.

Курсовая работа оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется за глубокий анализ темы, оригинальные выводы и рекомендации, высокое качество оформления и отсутствие ошибок, убедительную защиту работы с полным пониманием темы;
- зачтено с оценкой «хорошо» выставляется за полное выполнение задания с хорошим уровнем анализа, четкую структуру и логику изложения материала, соответствие оформления основным требованиям;
- зачтено с оценкой «удовлетворительно» выставляется за выполнение всех заданий с незначительными недостатками, наличие основных разделов, но недостаточная глубина

анализа, оформление работы с небольшими ошибками;

- не зачтено («не удовлетворительно») – выставляется за отсутствие темы или неуместный выбор, неполное выполнение заданий (отсутствие ключевых разделов), плагиат или отсутствие оригинальности, низкое качество оформления (нарушение стандартов).

6. Оценочные материалы текущего контроля

Раздел 1. Введение в программно-аппаратные средства защиты информации

Контролируемые ИДК: ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-10.1 ОПК-10.2

Тема 1.1. Введение в программно-аппаратные средства защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является примером системы централизованной аутентификации в учебном стенде?

1. Keycloak
2. Syft
3. Gripe

2. Что используется в OAuth2/OpenID Connect для представления прав доступа?

1. Токены
2. RAID-массивы
3. Архивы

Тема 1.2. Средства идентификации и аутентификации пользователей

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какая мера помогает снизить риск подбора пароля?

1. Отключение журналирования
2. Блокировка учетной записи после серии неуспешных входов
3. Уменьшение длины пароля

2. Что является основной задачей шифрования данных?

1. Сжатие данных
2. Обеспечение конфиденциальности данных
3. Ускорение работы процессора

3. Чем симметричное шифрование отличается от асимметричного?

1. В симметричном используется один общий ключ
2. В симметричном всегда не нужен ключ
3. В симметричном используются только сертификаты

Тема 1.3. Средства шифрования данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Для чего обычно применяется TLS?

1. Для защиты данных при передаче по сети
2. Для разметки диска
3. Для настройки ролей пользователей

2. Что такое хэш-функция в задачах ИБ?

1. Метод шифрования с секретным ключом
2. Функция вычисления контрольного значения для проверки целостности
3. Средство резервного копирования

3. Для чего применяется электронная подпись?

1. Для подтверждения подлинности и целостности электронного документа
2. Для ускорения сети
3. Для удаления вредоносных файлов

Тема 1.4. Средства аутентификации электронных данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое PKI?
 1. Система резервного питания
 2. Инфраструктура открытых ключей
 3. Формат контейнерного образа
2. Что включает управление криптографическими ключами?
 1. Только генерацию ключей
 2. Генерацию, хранение, ротацию и отзыв ключей
 3. Только удаление ключей

Тема 1.5. Средства управления криптографическими ключами

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что следует сделать при компрометации ключа?
 1. Продолжить использовать его без изменений
 2. Немедленно заменить (отозвать/ротация) ключ
 3. Увеличить размер файла
2. Что из перечисленного относится к обеспечению доступности данных?
 1. Резервное копирование
 2. Хэширование паролей
 3. Назначение ролей в Keycloak

Тема 1.6. Средства обеспечения доступности данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что показывает RPO в задачах резервного копирования?
 1. Максимально допустимую потерю данных по времени
 2. Скорость шифрования
 3. Количество пользователей в системе
2. Почему важно проверять восстановление из резервной копии?
 1. Чтобы убедиться, что копия действительно пригодна к восстановлению
 2. Чтобы уменьшить число логов
 3. Чтобы отключить мониторинг
3. Что из перечисленного относится к вредоносному ПО?
 1. Троянская программа
 2. Docker Compose
 3. Сертификат TLS

Тема 1.7. Средства защиты от вредоносных программ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой подход к защите от ВПО является базовым?
 1. Минимизация поверхности атаки и контроль источников ПО
 2. Отключение обновлений
 3. Хранение всех паролей в открытом виде

2. Для чего используется межсетевое экранирование?

1. Для фильтрации сетевого трафика по правилам
2. Для генерации SBOM
3. Для создания учетных записей

3. Что означает принцип "минимально необходимый доступ" в сетевых правилах?

1. Разрешить весь трафик по умолчанию
2. Разрешать только необходимые соединения
3. Запретить все логи

Тема 1.8. Средства межсетевого экранирования

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что такое уязвимость в контексте ИБ?

1. Ошибка или слабое место, которое может быть использовано для нарушения безопасности
2. Любой журнал событий
3. Метод сжатия данных

2. Для чего нужен SBOM?

1. Для учета состава программных компонентов и зависимостей
2. Для настройки клавиатуры
3. Для замены пароля администратора

3. Какую задачу решает Ggure в учебном контуре?

1. Генерацию ролей в Keycloak
2. Анализ уязвимостей в образе/зависимостях
3. Настройку сетевого маршрута

Тема 1.9. Средства обнаружения уязвимостей

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какую задачу решает Syft в учебном контуре?

1. Генерацию SBOM
2. Сброс блокировки пользователя
3. Шифрование диска

2. Для чего используется Wazuh в учебном стенде?

1. Для мониторинга и анализа событий безопасности
2. Для создания презентаций
3. Для работы с электронной подписью

3. Что является целью модели угроз?

1. Описать возможные угрозы, уязвимости и меры защиты для системы
2. Увеличить количество пользователей
3. Настроить резервное питание сервера

Раздел 2. Проектирование подсистемы защиты информации

Контролируемые ИДК: ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-10.1 ОПК-10.2 ОПК-10.3 ОПК-2.2.1 ОПК-2.2.2 ОПК-2.2.3

Тема 2.1. Нормативные основы проектирования защищенных информационных систем

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что обычно включает модель угроз?

1. Только список программ
2. Активы, нарушителей, угрозы, уязвимости и меры защиты

3. Только перечень паролей

2. Что такое граница доверия в модели угроз?

1. Участок системы, где меняется уровень доверия к данным/компонентам
2. Размер оперативной памяти сервера
3. Список резервных копий

3. Зачем нужна трассировка "требование → мера → контроль → артефакт"?

1. Для проверки обоснованности и подтверждаемости мер защиты
2. Для ускорения компиляции кода
3. Для замены модели угроз

Тема 2.2. Формирование модели угроз безопасности информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что является примером артефакта подтверждения выполнения меры защиты?

1. Лог события, конфигурационный файл или отчет сканирования
2. Название предмета в расписании
3. Список студентов группы

2. Что такое SAST?

1. Статический анализ кода/артефактов без запуска приложения
2. Сетевая сегментация контейнеров
3. Резервное копирование базы данных

3. Что такое DAST?

1. Анализ работающего приложения через внешнее тестирование
2. Генерация SBOM
3. Управление ключами шифрования

Тема 2.3. Порядок реализации подсистемы защиты информации

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой результат обычно дает сканирование уязвимостей?

1. Перечень найденных уязвимостей, требующих анализа и приоритизации
2. Гарантию полной безопасности
3. Автоматическое исправление всех проблем без проверки

2. Что важно учитывать при выборе мер защиты в проекте?

1. Только удобство администратора
2. Угрозы, риски, требования и ограничения системы
3. Только количество установленных сервисов

7. Оценочные материалы промежуточной аттестации

6 семестр, Экзамен

Контролируемые ИДК: ОПК-2.1 ОПК-10.1 ОПК-2.2.1 ОПК-2.2 ОПК-10.2 ОПК-2.2.2 ОПК-2.3 ОПК-10.3 ОПК-2.2.3

Вопросы/Задания:

1. Приведите классификацию программно-аппаратных средств защиты информации по функциональному назначению.

2. Сравните программные, аппаратные и программно-аппаратные средства защиты информации: преимущества, ограничения, типовые области применения.

3. Опишите средства идентификации и аутентификации пользователей и их роль в обеспечении безопасности информационных систем.
4. Сравните основные методы аутентификации по критериям безопасности, удобства и стоимости внедрения.
5. Объясните назначение централизованной аутентификации и SSO в корпоративной инфраструктуре. Какие задачи безопасности они решают?
6. Раскройте назначение OAuth2 и OpenID Connect в современных системах аутентификации и авторизации.
7. Опишите основные меры защиты от перебора паролей в прикладных системах и сервисах аутентификации.
8. Назовите и охарактеризуйте средства шифрования данных и основные задачи, которые они решают.
9. Объясните различие между симметричным и асимметричным шифрованием, укажите типовые сценарии применения каждого подхода.
10. Что такое аутентификация электронных данных? Раскройте роль хэш-функций, MAC/имитовставки и электронной подписи.
11. Какие требования предъявляются к криптографическим хэш-функциям и почему коллизия важна для задач аутентификации электронных данных?
12. Электронная подпись: назначение, основные свойства.
13. Инфраструктура открытых ключей: основные компоненты, процессы и назначение в корпоративных информационных системах.
14. Средства управления криптографическими ключами: жизненный цикл ключей, классификация ключей, хранение, учет, ротация, отзыв/замена при компрометации.
15. Что включает режим безопасной работы с носителями ключевой информации и какие организационно-технические меры при этом обязательны?
16. Средства обеспечения доступности данных: назначение резервного копирования, архивирования, RAID, источник бесперебойного питания и их место в программно-аппаратных средствах защиты информации.
17. Классификация вредоносного программного обеспечения и основные принципы защиты от вредоносного программного обеспечения в составе программно-аппаратных средств защиты информации.
18. Методы обнаружения и нейтрализации вредоносного программного обеспечения: сигнатурные, эвристические, поведенческие, белые/черные списки; их сильные и слабые стороны.
19. Средства межсетевого экранирования: назначение, базовые принципы фильтрации.

20. Средства обнаружения уязвимостей: цели, место в цикле управления уязвимостями, ограничения результатов сканирования и необходимость верификации.
21. Назначение SAST и DAST в безопасной разработке: что проверяет каждый подход, когда применяется и как результаты используются в процессе защиты.
22. Понятие SBOM: назначение, практическая ценность для управления зависимостями и уязвимостями.
23. Роль инструментов анализа состава программного обеспечения и уязвимостей зависимостей в контуре программно-аппаратных средств защиты информации.
24. Назначение систем мониторинга и корреляции событий информационной безопасности: какие события собираются и как используются для реагирования.
25. Нормативные основы проектирования защищенных информационных систем: какие группы документов необходимо учитывать.
26. Назначение модели угроз безопасности информации и ее место в проектировании подсистемы защиты информации.
27. Опишите порядок формирования модели угроз: активы, границы доверия, источники угроз, нарушители, уязвимости, сценарии реализации угроз, последствия.
28. Как выполняется выбор и обоснование мер защиты на основе модели угроз и требований нормативной базы? Приведите общую логику принятия решений.
29. Что такое трассировка в проектировании подсистемы защиты (“требование → мера → контроль → артефакт подтверждения”) и зачем она нужна для аудита и сопровождения?
30. Дайте определение программно-аппаратных средств защиты информации (ПАСЗИ) и объясните их место в комплексной системе защиты информации.

6 семестр, Курсовая работа

Контролируемые ИДК: ОПК-2.1 ОПК-10.1 ОПК-2.2.1 ОПК-2.2 ОПК-10.2 ОПК-2.2.2 ОПК-2.3 ОПК-10.3 ОПК-2.2.3

Вопросы/Задания:

1. Анализ средств идентификации и аутентификации пользователей в информационной системе
2. Настройка централизованной аутентификации пользователей в учебной системе с использованием Keycloak
3. Анализ политики паролей и мер защиты от подбора паролей в системе аутентификации
4. Сравнительный анализ локальной и централизованной аутентификации пользователей

5. Разработка регламента управления учетными записями пользователей в информационной системе

6. Анализ применения OAuth2/OpenID Connect в системах централизованной аутентификации

7. Разработка схемы аутентификации и авторизации для веб-приложения с использованием Keycloak

8. Анализ средств шифрования данных в информационных системах

9. Анализ применения хэш-функций для контроля целостности файлов

10. Разработка порядка контроля целостности файлов конфигурации в учебной системе

11. Анализ средств аутентификации электронных данных и их роли в защите информации

12. Разработка программного модуля для проверки целостности программных артефактов

13. Анализ подходов к хранению и защите секретов в информационной системе

14. Разработка регламента работы с секретами и ключевыми данными в учебной системе

15. Анализ средств обеспечения доступности данных в информационной системе

16. Разработка плана резервного копирования и восстановления для учебного стенда

17. Анализ угроз вредоносного ПО в современных информационных системах

18. Разработка чек-листа организации безопасности учебного контейнерного стенда

19. Анализ средств межсетевого экранирования и сегментации в сервисных системах

20. Анализ подходов к сетевому разграничению доступа

21. Анализ средств обнаружения уязвимостей программного обеспечения

22. Генерация SBOM для учебного приложения и анализ состава зависимостей

23. Разработка регламента управления уязвимостями для учебной системы

24. Анализ возможностей SBOM в задачах контроля программных компонентов

25. Анализ возможностей системы мониторинга событий безопасности

26. Анализ правил инструмента статического тестирования безопасности приложений

27. Разработка модели угроз для учебного веб-приложения с централизованной аутентификацией

28. Исследование влияния SAST и DAST в процессе безопасной разработки

29. Анализ нормативных требований к проектированию защищенных государственных информационных систем

30. Разработка перечня событий безопасности, подлежащих обязательной регистрации