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

Факультет управления территориями
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
21 апреля 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ «Б1.О.13.03 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Уровень высшего образования: бакалавриат

Направление подготовки: 27.03.03 Системный анализ и управление

Направленность(профиль) подготовки: Управление земельно-информационными системами

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2023

Срок получения образования: 4 года

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

Москва, 2023

Разработчики:
Преподаватель кафедры Информационно-измерительных систем
Пискарев А. Д.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 27.03.03 Системный анализ и управление, утвержденного приказом Минобрнауки от 07.08.2020 № 902

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Управления территориями	Председатель ученого совета факультета	Воронцова А. А.	Рассмотрено	15.12.2022, № 2-2022

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

УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов

УК-8.1 Анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)

Знать:

УК-8.1/Зн1 Факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)

УК-8.1/Зн2 Идентификацию травмирующих, вредных и поражающих факторов чрезвычайных ситуаций

Уметь:

УК-8.1/Ум1 Анализировать факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)

Владеть:

УК-8.1/Нв1 Навыками анализа факторов вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)

УК-8.2 Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности

Знать:

УК-8.2/Зн1 Опасные и вредные факторы в рамках осуществляемой деятельности

УК-8.2/Зн2 Физиологические последствия воздействия на человека травмирующих, вредных и поражающих факторов

Уметь:

УК-8.2/Ум1 Идентифицировать опасные и вредные факторы в рамках осуществляемой деятельности

Владеть:

УК-8.2/Нв1 Методами защиты от опасностей применительно к сфере своей профессиональной деятельности

УК-8.3 Выявляет проблемы, связанные с нарушением техники безопасности на рабочем месте, предлагает мероприятия по предотвращению чрезвычайных ситуаций

Знать:

УК-8.3/Зн1 Технику безопасности на рабочем месте и меры предотвращения чрезвычайных ситуаций

УК-8.3/Зн2 Средства и методы повышения безопасности и устойчивости технических средств и технологических процессов

Уметь:

УК-8.3/Ум1 Выявлять нарушения технику безопасности на рабочем месте

Владеть:

УК-8.3/Нв1 Навыками предотвращения нарушений техники безопасности на рабочем месте

УК-8.4 Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях

Знать:

УК-8.4/Зн1 Принципы безопасности жизнедеятельности и порядок применения их в работе

УК-8.4/Зн2 Правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения

Уметь:

УК-8.4/Ум1 Соблюдать и разъяснять правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения

Владеть:

УК-8.4/Нв1 Методикой и навыками оценки допустимого риска

ОПК-2 Способен формулировать задачи профессиональной деятельности на основе знаний профильных разделов математических и естественнонаучных дисциплин (модулей)

ОПК-2.1 Использует знание алгоритма организации выполнения работ в процессе проектной деятельности

Знать:

ОПК-2.1/Зн1 Основные этапы и алгоритмы организации проектной деятельности, включая планирование, инициацию, реализацию, сопровождение, контроль и оценку проекта

Уметь:

ОПК-2.1/Ум1 Формулировать задачи профессиональной деятельности в области информационной безопасности, опираясь на знания математических и естественнонаучных дисциплин

Владеть:

ОПК-2.1/Нв1 Навыками эффективного взаимодействия с участниками проекта, распределения обязанностей и оценки качества выполнения задач

ОПК-2.2 Формулирует цели выполнения работ и предлагает пути их достижения при организации производства и управлении в профессиональной сфере

Знать:

ОПК-2.2/Зн1 Основы постановки целей и задач в профессиональной деятельности с учетом специфики информационной безопасности

Уметь:

ОПК-2.2/Ум1 Формулировать цели выполнения работ в области информационной безопасности, исходя из требований профессиональной деятельности и профильных знаний

ОПК-2.2/Ум2 Предлагать обоснованные пути и методы достижения поставленных целей с использованием математических моделей и научных методов

Владеть:

ОПК-2.2/Нв1 Навыками системного анализа и синтеза при формулировании целей и задач в профессиональной деятельности

ОПК-2.3 Осуществляет сбор исходных данных для составления научно- технической, проектной и служебной документации

Знать:

ОПК-2.3/Зн1 Основные источники и виды исходных данных, необходимых для составления научно-технической, проектной и служебной документации в области информационной безопасности

Уметь:

ОПК-2.3/Ум1 Проводить систематический сбор и первичный анализ исходных данных, необходимых для разработки документации

Владеть:

ОПК-2.3/Нв1 Навыками применения современных инструментов и программных средств для сбора и анализа данных в области информационной безопасности

ОПК-2.4 Выбирает соответствующие программные продукты или их части для решения конкретных профессиональных задач

Знать:

ОПК-2.4/Зн1 Основные категории и функциональные возможности программных продуктов, применяемых в информационной безопасности

Уметь:

ОПК-2.4/Ум1 Оценивать и сравнивать программные продукты и их компоненты по функциональности, безопасности, надежности и совместимости

Владеть:

ОПК-2.4/Нв1 Навыками работы с современными программными средствами и инструментами, применяемыми в информационной безопасности

ОПК-2.5 Демонстрирует навыки автоматизированного проектирования технологических процессов

Знать:

ОПК-2.5/Зн1 Основы автоматизированного проектирования технологических процессов и их применение в информационной безопасности

Уметь:

ОПК-2.5/Ум1 Использовать специализированное программное обеспечение для автоматизированного проектирования технологических процессов

Владеть:

ОПК-2.5/Нв1 Навыками работы с инструментами автоматизированного проектирования, включая создание, редактирование и оптимизацию моделей процессов

ОПК-2.6 Владеет навыками разработки и составления отдельных научно- технических, проектных и служебных документов, оформления научно- технических отчетов, обзоров, публикаций по результатам выполненных работ

Знать:

ОПК-2.6/Зн1 Структуру и требования к научно-технической, проектной и служебной документации в профессиональной сфере информационной безопасности

Уметь:

ОПК-2.6/Ум1 Разрабатывать и составлять отдельные виды профессиональной документации: научно-технические отчеты, проектные документы, служебные записки

Владеть:

ОПК-2.6/Нв1 Навыками системного подхода к подготовке и оформлению профессиональной документации

ОПК-2.7 Владеет современными технологиями и геоинформационными системами для оформления научно- технических отчетов, обзоров, публикаций, рецензий

Знать:

ОПК-2.7/Зн1 Базовые понятия и возможности геоинформационных систем (ГИС) и их потенциал применения в контексте профессиональной деятельности

ОПК-2.7/Зн2 Принципы работы современных текстовых процессоров, издательских систем и инструментов для оформления документации

Уметь:

ОПК-2.7/Ум1 Использовать современные программные средства для подготовки и оформления научно-технических отчетов, обзоров и публикаций

Владеть:

ОПК-2.7/Нв1 Навыками использования современных офисных и издательских программ для профессионального оформления документов

ОПК-10 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПК-10.1 Демонстрирует знание современных информационных технологий, принципов взаимодействия со службами информационных технологий.

Знать:

ОПК-10.1/Зн1 Современные информационные технологии, включая архитектуру компьютерных систем, сети, облачные сервисы и базы данных

Уметь:

ОПК-10.1/Ум1 Анализировать и оценивать возможности ИТ-систем с точки зрения безопасности и соответствия требованиям профессиональной деятельности

Владеть:

ОПК-10.1/Нв1 Навыками работы с современными ИТ-системами и сервисами, включая средства коммуникации и управления ИТ-ресурсами

ОПК-10.2 Применяет методы и программные средства обработки деловой информации во взаимодействии со службами информационных технологий

Знать:

ОПК-10.2/Зн1 Основные методы обработки деловой информации и их значение в профессиональной деятельности

Уметь:

ОПК-10.2/Ум1 Использовать программные средства для эффективной обработки деловой информации: создание, редактирование, хранение и передача документов и данных

Владеть:

ОПК-10.2/Нв1 Навыками работы с современными программными продуктами для обработки деловой информации, включая специализированные системы и инструменты

ОПК-10.3 Владеет навыками эффективного использования корпоративных информационных систем при решении задач профессиональной деятельности

Знать:

ОПК-10.3/Зн1 Основные компоненты и архитектуру корпоративных информационных систем, их функции и назначение

Уметь:

ОПК-10.3/Ум1 Использовать функциональные возможности корпоративных информационных систем для решения профессиональных задач

Владеть:

ОПК-10.3/Нв1 Навыками работы с современными корпоративными информационными системами и их основными модулями

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	Повышенный	ИДК УК-8.1 Анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) Знать: УК-8.1/Зн1 Факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) УК-8.1/Зн2 Идентификацию травмирующих, вредных и поражающих факторов чрезвычайных ситуаций Уметь: УК-8.1/Ум1 Анализировать факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) Владеть: УК-8.1/Нв1 Навыками анализа факторов вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) ИДК УК-8.2 Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности Знать: УК-8.2/Зн1 Опасные и вредные факторы в рамках осуществляемой деятельности УК-8.2/Зн2 Физиологические последствия воздействия на человека травмирующих, вредных и поражающих факторов Уметь: УК-8.2/Ум1 Идентифицировать опасные и вредные факторы в рамках осуществляемой деятельности Владеть: УК-8.2/Нв1 Методами защиты от опасностей применительно к сфере своей профессиональной деятельности

			ИДК УК-8.3 Выявляет проблемы, связанные с нарушением техники безопасности на рабочем месте, предлагает мероприятия по предотвращению чрезвычайных ситуаций Знать: УК-8.3/Зн1 Технику безопасности на рабочем месте и меры предотвращения чрезвычайных ситуаций УК-8.3/Зн2 Средства и методы повышения безопасности и устойчивости технических средств и технологических процессов Уметь: УК-8.3/Ум1 Выявлять нарушения технику безопасности на рабочем месте Владеть: УК-8.3/Нв1 Навыками предотвращения нарушений техники безопасности на рабочем месте ИДК УК-8.4 Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях Знать: УК-8.4/Зн1 Принципы безопасности жизнедеятельности и порядок применения их в работе УК-8.4/Зн2 Правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения Уметь: УК-8.4/Ум1 Соблюдать и разъяснять правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения Владеть: УК-8.4/Нв1 Методикой и навыками оценки допустимого риска

	Базовый	ИДК УК-8.1 Анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) Знать: УК-8.1/Зн1 Факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) УК-8.1/Зн2 Идентификацию травмирующих, вредных и поражающих факторов чрезвычайных ситуаций Уметь: УК-8.1/Ум1 Анализировать факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) ИДК УК-8.2 Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности Знать: УК-8.2/Зн1 Опасные и вредные факторы в рамках осуществляемой деятельности УК-8.2/Зн2 Физиологические последствия воздействия на человека травмирующих, вредных и поражающих факторов Уметь: УК-8.2/Ум1 Идентифицировать опасные и вредные факторы в рамках осуществляемой деятельности ИДК УК-8.3 Выявляет проблемы, связанные с нарушением техники безопасности на рабочем месте, предлагает мероприятия по предотвращению чрезвычайных ситуаций Знать: УК-8.3/Зн1 Технику безопасности на рабочем месте и меры предотвращения чрезвычайных ситуаций УК-8.3/Зн2 Средства и методы повышения безопасности и устойчивости технических средств и технологических процессов Уметь: УК-8.3/Ум1 Выявлять нарушения технику безопасности на рабочем месте

		ИДК УК-8.4 Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях Знать: УК-8.4/Зн1 Принципы безопасности жизнедеятельности и порядок применения их в работе УК-8.4/Зн2 Правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения Уметь: УК-8.4/Ум1 Соблюдать и разъяснять правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения
	Пороговый	ИДК УК-8.1 Анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) Знать: УК-8.1/Зн1 Факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) УК-8.1/Зн2 Идентификацию травмирующих, вредных и поражающих факторов чрезвычайных ситуаций ИДК УК-8.2 Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности Знать: УК-8.2/Зн1 Опасные и вредные факторы в рамках осуществляемой деятельности УК-8.2/Зн2 Физиологические последствия воздействия на человека травмирующих, вредных и поражающих факторов ИДК УК-8.3 Выявляет проблемы, связанные с нарушением техники безопасности на рабочем месте, предлагает мероприятия по предотвращению чрезвычайных ситуаций Знать: УК-8.3/Зн1 Технику безопасности на рабочем месте и меры предотвращения чрезвычайных ситуаций УК-8.3/Зн2 Средства и методы повышения безопасности и устойчивости технических средств и технологических процессов

		ИДК УК-8.4 Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях Знать: УК-8.4/Зн1 Принципы безопасности жизнедеятельности и порядок применения их в работе УК-8.4/Зн2 Правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения
ОПК-2 Способен формулировать задачи профессиональной деятельности на основе знаний профильных разделов математических и естественнонаучных дисциплин (модулей)	Повышенный	ИДК ОПК-2.1 Использует знание алгоритма организации выполнения работ в процессе проектной деятельности Знать: ОПК-2.1/Зн1 Основные этапы и алгоритмы организации проектной деятельности, включая планирование, инициацию, реализацию, сопровождение, контроль и оценку проекта Уметь: ОПК-2.1/Ум1 Формулировать задачи профессиональной деятельности в области информационной безопасности, опираясь на знания математических и естественнонаучных дисциплин Владеть: ОПК-2.1/Нв1 Навыками эффективного взаимодействия с участниками проекта, распределения обязанностей и оценки качества выполнения задач
ОПК-2 Способен формулировать задачи профессиональной деятельности на основе знаний профильных разделов математических и естественнонаучных дисциплин (модулей)	Повышенный	ИДК ОПК-2.2 Формулирует цели выполнения работ и предлагает пути их достижения при организации производства и управлении в профессиональной сфере Знать: ОПК-2.2/Зн1 Основы постановки целей и задач в профессиональной деятельности с учетом специфики информационной безопасности Уметь: ОПК-2.2/Ум1 Формулировать цели выполнения работ в области информационной безопасности, исходя из требований профессиональной деятельности и профильных знаний ОПК-2.2/Ум2 Предлагать обоснованные пути и методы достижения поставленных целей с использованием математических моделей и научных методов Владеть: ОПК-2.2/Нв1 Навыками системного анализа и синтеза при формулировании целей и задач в профессиональной деятельности

		ИДК ОПК-2.3 Осуществляет сбор исходных данных для составления научно- технической, проектной и служебной документации Знать: ОПК-2.3/Зн1 Основные источники и виды исходных данных, необходимых для составления научно-технической, проектной и служебной документации в области информационной безопасности Уметь: ОПК-2.3/Ум1 Проводить систематический сбор и первичный анализ исходных данных, необходимых для разработки документации Владеть: ОПК-2.3/Нв1 Навыками применения современных инструментов и программных средств для сбора и анализа данных в области информационной безопасности ИДК ОПК-2.4 Выбирает соответствующие программные продукты или их части для решения конкретных профессиональных задач Знать: ОПК-2.4/Зн1 Основные категории и функциональные возможности программных продуктов, применяемых в информационной безопасности Уметь: ОПК-2.4/Ум1 Оценивать и сравнивать программные продукты и их компоненты по функциональности, безопасности, надежности и совместимости Владеть: ОПК-2.4/Нв1 Навыками работы с современными программными средствами и инструментами, применяемыми в информационной безопасности ИДК ОПК-2.5 Демонстрирует навыки автоматизированного проектирования технологических процессов Знать: ОПК-2.5/Зн1 Основы автоматизированного проектирования технологических процессов и их применение в информационной безопасности Уметь: ОПК-2.5/Ум1 Использовать специализированное программное обеспечение для автоматизированного проектирования технологических процессов

		Владеть: ОПК-2.5/Нв1 Навыками работы с инструментами автоматизированного проектирования, включая создание, редактирование и оптимизацию моделей процессов ИДК ОПК-2.6 Владеет навыками разработки и составления отдельных научно- технических, проектных и служебных документов, оформления научно- технических отчетов, обзоров, публикаций по результатам выполненных работ Знать: ОПК-2.6/Зн1 Структуру и требования к научно-технической, проектной и служебной документации в профессиональной сфере информационной безопасности Уметь: ОПК-2.6/Ум1 Разрабатывать и составлять отдельные виды профессиональной документации: научно-технические отчеты, проектные документы, служебные записки Владеть: ОПК-2.6/Нв1 Навыками системного подхода к подготовке и оформлению профессиональной документации ИДК ОПК-2.7 Владеет современными технологиями и геоинформационными системами для оформления научно- технических отчетов, обзоров, публикаций, рецензий Знать: ОПК-2.7/Зн1 Базовые понятия и возможности геоинформационных систем (ГИС) и их потенциал применения в контексте профессиональной деятельности ОПК-2.7/Зн2 Принципы работы современных текстовых процессоров, издательских систем и инструментов для оформления документации Уметь: ОПК-2.7/Ум1 Использовать современные программные средства для подготовки и оформления научно-технических отчетов, обзоров и публикаций Владеть: ОПК-2.7/Нв1 Навыками использования современных офисных и издательских программ для профессионального оформления документов

	Базовый	ИДК ОПК-2.1 Использует знание алгоритма организации выполнения работ в процессе проектной деятельности Знать: ОПК-2.1/Зн1 Основные этапы и алгоритмы организации проектной деятельности, включая планирование, инициацию, реализацию, сопровождение, контроль и оценку проекта Уметь: ОПК-2.1/Ум1 Формулировать задачи профессиональной деятельности в области информационной безопасности, опираясь на знания математических и естественнонаучных дисциплин
	Базовый	ИДК ОПК-2.2 Формулирует цели выполнения работ и предлагает пути их достижения при организации производства и управлении в профессиональной сфере Знать: ОПК-2.2/Зн1 Основы постановки целей и задач в профессиональной деятельности с учетом специфики информационной безопасности Уметь: ОПК-2.2/Ум1 Формулировать цели выполнения работ в области информационной безопасности, исходя из требований профессиональной деятельности и профильных знаний ОПК-2.2/Ум2 Предлагать обоснованные пути и методы достижения поставленных целей с использованием математических моделей и научных методов ИДК ОПК-2.3 Осуществляет сбор исходных данных для составления научно- технической, проектной и служебной документации Знать: ОПК-2.3/Зн1 Основные источники и виды исходных данных, необходимых для составления научно-технической, проектной и служебной документации в области информационной безопасности Уметь: ОПК-2.3/Ум1 Проводить систематический сбор и первичный анализ исходных данных, необходимых для разработки документации

			ИДК ОПК-2.4 Выбирает соответствующие программные продукты или их части для решения конкретных профессиональных задач Знать: ОПК-2.4/Зн1 Основные категории и функциональные возможности программных продуктов, применяемых в информационной безопасности Уметь: ОПК-2.4/Ум1 Оценивать и сравнивать программные продукты и их компоненты по функциональности, безопасности, надежности и совместимости ИДК ОПК-2.5 Демонстрирует навыки автоматизированного проектирования технологических процессов Знать: ОПК-2.5/Зн1 Основы автоматизированного проектирования технологических процессов и их применение в информационной безопасности Уметь: ОПК-2.5/Ум1 Использовать специализированное программное обеспечение для автоматизированного проектирования технологических процессов ИДК ОПК-2.6 Владеет навыками разработки и составления отдельных научно- технических, проектных и служебных документов, оформления научно- технических отчетов, обзоров, публикаций по результатам выполненных работ Знать: ОПК-2.6/Зн1 Структуру и требования к научно-технической, проектной и служебной документации в профессиональной сфере информационной безопасности Уметь: ОПК-2.6/Ум1 Разрабатывать и составлять отдельные виды профессиональной документации: научно-технические отчеты, проектные документы, служебные записки ИДК ОПК-2.7 Владеет современными технологиями и геоинформационными системами для оформления научно- технических отчетов, обзоров, публикаций, рецензий Знать: ОПК-2.7/Зн1 Базовые понятия и возможности геоинформационных систем (ГИС) и их потенциал применения в контексте профессиональной деятельности

		ОПК-2.7/Зн2 Принципы работы современных текстовых процессоров, издательских систем и инструментов для оформления документации Уметь: ОПК-2.7/Ум1 Использовать современные программные средства для подготовки и оформления научно-технических отчетов, обзоров и публикаций
	Пороговый	ИДК ОПК-2.1 Использует знание алгоритма организации выполнения работ в процессе проектной деятельности Знать: ОПК-2.1/Зн1 Основные этапы и алгоритмы организации проектной деятельности, включая планирование, инициацию, реализацию, сопровождение, контроль и оценку проекта ИДК ОПК-2.2 Формулирует цели выполнения работ и предлагает пути их достижения при организации производства и управлении в профессиональной сфере Знать: ОПК-2.2/Зн1 Основы постановки целей и задач в профессиональной деятельности с учетом специфики информационной безопасности ИДК ОПК-2.3 Осуществляет сбор исходных данных для составления научно- технической, проектной и служебной документации Знать: ОПК-2.3/Зн1 Основные источники и виды исходных данных, необходимых для составления научно-технической, проектной и служебной документации в области информационной безопасности ИДК ОПК-2.4 Выбирает соответствующие программные продукты или их части для решения конкретных профессиональных задач Знать: ОПК-2.4/Зн1 Основные категории и функциональные возможности программных продуктов, применяемых в информационной безопасности ИДК ОПК-2.5 Демонстрирует навыки автоматизированного проектирования технологических процессов Знать: ОПК-2.5/Зн1 Основы автоматизированного проектирования технологических процессов и их применение в информационной безопасности

		ИДК ОПК-2.6 Владеет навыками разработки и составления отдельных научно- технических, проектных и служебных документов, оформления научно- технических отчетов, обзоров, публикаций по результатам выполненных работ Знать: ОПК-2.6/Зн1 Структуру и требования к научно-технической, проектной и служебной документации в профессиональной сфере информационной безопасности ИДК ОПК-2.7 Владеет современными технологиями и геоинформационными системами для оформления научно- технических отчетов, обзоров, публикаций, рецензий Знать: ОПК-2.7/Зн1 Базовые понятия и возможности геоинформационных систем (ГИС) и их потенциал применения в контексте профессиональной деятельности ОПК-2.7/Зн2 Принципы работы современных текстовых процессоров, издательских систем и инструментов для оформления документации
ОПК-10 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	Повышенный	ИДК ОПК-10.1 Демонстрирует знание современных информационных технологий, принципов взаимодействия со службами информационных технологий. Знать: ОПК-10.1/Зн1 Современные информационные технологии, включая архитектуру компьютерных систем, сети, облачные сервисы и базы данных Уметь: ОПК-10.1/Ум1 Анализировать и оценивать возможности ИТ-систем с точки зрения безопасности и соответствия требованиям профессиональной деятельности Владеть: ОПК-10.1/Нв1 Навыками работы с современными ИТ-системами и сервисами, включая средства коммуникации и управления ИТ-ресурсами ИДК ОПК-10.2 Применяет методы и программные средства обработки деловой информации во взаимодействии со службами информационных технологий Знать: ОПК-10.2/Зн1 Основные методы обработки деловой информации и их значение в профессиональной деятельности

		Уметь: ОПК-10.2/Ум1 Использовать программные средства для эффективной обработки деловой информации: создание, редактирование, хранение и передача документов и данных Владеть: ОПК-10.2/Нв1 Навыками работы с современными программными продуктами для обработки деловой информации, включая специализированные системы и инструменты ИДК ОПК-10.3 Владеет навыками эффективного использования корпоративных информационных систем при решении задач профессиональной деятельности Знать: ОПК-10.3/Зн1 Основные компоненты и архитектуру корпоративных информационных систем, их функции и назначение Уметь: ОПК-10.3/Ум1 Использовать функциональные возможности корпоративных информационных систем для решения профессиональных задач Владеть: ОПК-10.3/Нв1 Навыками работы с современными корпоративными информационными системами и их основными модулями
	Базовый	ИДК ОПК-10.1 Демонстрирует знание современных информационных технологий, принципов взаимодействия со службами информационных технологий. Знать: ОПК-10.1/Зн1 Современные информационные технологии, включая архитектуру компьютерных систем, сети, облачные сервисы и базы данных Уметь: ОПК-10.1/Ум1 Анализировать и оценивать возможности ИТ-систем с точки зрения безопасности и соответствия требованиям профессиональной деятельности ИДК ОПК-10.2 Применяет методы и программные средства обработки деловой информации во взаимодействии со службами информационных технологий Знать: ОПК-10.2/Зн1 Основные методы обработки деловой информации и их значение в профессиональной деятельности

		Уметь: ОПК-10.2/Ум1 Использовать программные средства для эффективной обработки деловой информации: создание, редактирование, хранение и передача документов и данных ИДК ОПК-10.3 Владеет навыками эффективного использования корпоративных информационных систем при решении задач профессиональной деятельности Знать: ОПК-10.3/Зн1 Основные компоненты и архитектуру корпоративных информационных систем, их функции и назначение Уметь: ОПК-10.3/Ум1 Использовать функциональные возможности корпоративных информационных систем для решения профессиональных задач
	Пороговый	ИДК ОПК-10.1 Демонстрирует знание современных информационных технологий, принципов взаимодействия со службами информационных технологий. Знать: ОПК-10.1/Зн1 Современные информационные технологии, включая архитектуру компьютерных систем, сети, облачные сервисы и базы данных ИДК ОПК-10.2 Применяет методы и программные средства обработки деловой информации во взаимодействии со службами информационных технологий Знать: ОПК-10.2/Зн1 Основные методы обработки деловой информации и их значение в профессиональной деятельности ИДК ОПК-10.3 Владеет навыками эффективного использования корпоративных информационных систем при решении задач профессиональной деятельности Знать: ОПК-10.3/Зн1 Основные компоненты и архитектуру корпоративных информационных систем, их функции и назначение

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)

Зачтено	УК-8.1 Анализирует факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) УК-8.1/Зн2 Идентификацию травмирующих, вредных и поражающих факторов чрезвычайных ситуаций УК-8.1/Зн1 Факторы вредного влияния на жизнедеятельность элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений) УК-8.2 Идентифицирует опасные и вредные факторы в рамках осуществляемой деятельности УК-8.2/Зн1 Опасные и вредные факторы в рамках осуществляемой деятельности УК-8.2/Зн2 Физиологические последствия воздействия на человека травмирующих, вредных и поражающих факторов УК-8.3 Выявляет проблемы, связанные с нарушением техники безопасности на рабочем месте, предлагает мероприятия по предотвращению чрезвычайных ситуаций УК-8.3/Зн2 Средства и методы повышения безопасности и устойчивости технических средств и технологических процессов УК-8.3/Зн1 Технику безопасности на рабочем месте и меры предотвращения чрезвычайных ситуаций УК-8.4 Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях УК-8.4/Зн2 Правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения УК-8.4/Зн1 Принципы безопасности жизнедеятельности и порядок применения их в работе ОПК-2.1 Использует знание алгоритма организации выполнения работ в процессе проектной деятельности ОПК-2.1/Зн1 Основные этапы и алгоритмы организации проектной деятельности, включая планирование, инициацию, реализацию, сопровождение, контроль и оценку проекта ОПК-10.1 Демонстрирует знание современных информационных технологий, принципов взаимодействия со службами информационных технологий. ОПК-10.1/Зн1 Современные информационные технологии, включая архитектуру компьютерных систем, сети, облачные сервисы и базы данных ОПК-10.2 Применяет методы и программные средства обработки деловой информации во взаимодействии со службами информационных технологий ОПК-10.2/Зн1 Основные методы обработки деловой информации и их значение в профессиональной деятельности ОПК-2.2 Формулирует цели выполнения работ и предлагает пути их достижения при организации производства и управлении в профессиональной сфере ОПК-2.2/Зн1 Основы постановки целей и задач в профессиональной деятельности с учетом специфики информационной безопасности

	ОПК-2.3 Осуществляет сбор исходных данных для составления научно- технической, проектной и служебной документации ОПК-2.3/Зн1 Основные источники и виды исходных данных, необходимых для составления научно-технической, проектной и служебной документации в области информационной безопасности ОПК-10.3 Владеет навыками эффективного использования корпоративных информационных систем при решении задач профессиональной деятельности ОПК-10.3/Зн1 Основные компоненты и архитектуру корпоративных информационных систем, их функции и назначение ОПК-2.4 Выбирает соответствующие программные продукты или их части для решения конкретных профессиональных задач ОПК-2.4/Зн1 Основные категории и функциональные возможности программных продуктов, применяемых в информационной безопасности ОПК-2.5 Демонстрирует навыки автоматизированного проектирования технологических процессов ОПК-2.5/Зн1 Основы автоматизированного проектирования технологических процессов и их применение в информационной безопасности ОПК-2.6 Владеет навыками разработки и составления отдельных научно- технических, проектных и служебных документов, оформления научно- технических отчетов, обзоров, публикаций по результатам выполненных работ ОПК-2.6/Зн1 Структуру и требования к научно-технической, проектной и служебной документации в профессиональной сфере информационной безопасности ОПК-2.7 Владеет современными технологиями и геоинформационными системами для оформления научно- технических отчетов, обзоров, публикаций, рецензий ОПК-2.7/Зн1 Базовые понятия и возможности геоинформационных систем (ГИС) и их потенциал применения в контексте профессиональной деятельности ОПК-2.7/Зн2 Принципы работы современных текстовых процессоров, издательских систем и инструментов для оформления документации
Не зачтено	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование
Промежуточная аттестация	Контрольная работа Зачет

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация

1	Информационная безопасность в системе национальной безопасности Российской Федерации	УК-8.1 УК-8.2 УК-8.3 УК-8.4 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4 ОПК-2.5 ОПК-2.6 ОПК-2.7		Зачет
2	Информационная война, методы и средства ее ведения	УК-8.1 УК-8.2 УК-8.3 УК-8.4 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4 ОПК-2.5 ОПК-2.6 ОПК-2.7		Зачет
3	Обеспечения информационной безопасности компьютерных систем	ОПК-2.6 ОПК-2.7 ОПК-10.1 ОПК-10.2 ОПК-10.3	Тестирование	Зачет

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: Зачет, 5 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.

6. Оценочные материалы текущего контроля

Раздел 3. Обеспечения информационной безопасности компьютерных систем

Контролируемые ИДК: ОПК-2.6 ОПК-2.7 ОПК-10.1 ОПК-10.2 ОПК-10.3

Тема 3.1. Методы и средства обеспечения информационной безопасности компьютерных систем

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Основные принципы информационной безопасности:

1) Конфиденциальность, целостность, доступность
2) Конфиденциальность, аутентичность, доступность
3) Конфиденциальность, целостность, актуальность
4) Целостность, доступность, отказоустойчивость

2. Что является основной целью атаки типа социальной инженерии?

1) Обход технических средств защиты (брандмауэров, антивирусов) путем взлома уязвимостей ПО.
2) Манипуляция людьми с целью получения конфиденциальной информации или совершения определенных действий.
3) Заражение компьютеров вредоносным ПО через уязвимости в операционной системе.
4) Кража физических носителей информации (жестких дисков, флешек).

3. Как называется техника социальной инженерии, при которой злоумышленник заранее придумывает правдоподобный сценарий (легенду) для установления доверия и получения информации?

1) Фишинг (Phishing)
2) Кви про кви (Quid pro quo)
3) Претекстинг (Pretexting)
4) Байтинг (Baiting)

4. Что означает принцип "Целостность" в контексте информационной безопасности?

1) Обеспечение того, что информация доступна только тем, кто имеет на это право.
2) Обеспечение того, что информация является точной, полной и защищенной от несанкционированного или случайного изменения.
3) Обеспечение того, что информация и системы доступны авторизованным пользователям, когда это необходимо.
4) Защита информации от искажения или потери при передаче по каналам связи из-за технических помех.

5. Какая атака направлена на нарушение принципа доступности путем перегрузки целевого ресурса (сервера, сети) огромным количеством запросов, делая его недоступным для легитимных пользователей?

1) Фишинг (Phishing)
2) Внедрение SQL-кода (SQL Injection)
3) Отказ в обслуживании (DoS / DDoS атака)
4) Человек посередине (Man-in-the-Middle, MitM)

Тема 3.2. Механизмы защиты информации в автоматизированных системах

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что из перечисленного наиболее точно определяет понятие "Угроза" в информационной безопасности?

1) Конкретная слабость или недостаток в системе, процедуре или контроле, который может быть использован.
2) Потенциальная причина наступления нежелательного события , которое может нанести ущерб системе или организации.

3) Техническая атака, такая как вирус или фишинг.
4) Фактически произошедшее нарушение безопасности, повлекшее ущерб.

2. Какой вариант классификации угроз информационной безопасности является наиболее фундаментальным и широко используемым, учитывает источник и природу происхождения угрозы?

1) По объекту атаки: угрозы данным, угрозы программному обеспечению, угрозы оборудованию, угрозы каналам связи.
2) По используемым средствам атаки: программные, аппаратные, физические, социально-психологические.
3) По источнику происхождения: внутренние и внешние; а также по природе: естественные и искусственные.
4) По типу нарушаемого принципа ИБ: угрозы конфиденциальности, угрозы целостности, угрозы доступности.

3. Какой метод анализа угроз использует древовидную структуру, где "корнем" является конечная цель злоумышленника (например, кража данных, отказ сервиса), а "ветвями" и "листьями" представляются все возможные пути (сценарии, шаги атаки, необходимые условия) для достижения этой цели, позволяя систематически оценить уязвимости и контрмеры?

1) Анализ дерева атак (Attack Tree Analysis)
2) Оценка критичности уязвимостей (CVSS - Common Vulnerability Scoring System)
3) Качественный анализ рисков (Qualitative Risk Assessment)
4) Цепочка киберугроз (Cyber Kill Chain)

4. Что из перечисленного является ключевой целью хеширования?

1) Обеспечение конфиденциальности данных путем их шифрования.
2) Гарантирование целостности данных путем создания уникального "отпечатка" (хеша), чувствительного к любым изменениям.
3) Обеспечение доступности данных путем их сжатия.
4) Аутентификация пользователей с помощью пароля.

5. Какое из перечисленных вредоносных программ ПРЕИМУЩЕСТВЕННО предназначено для тайного сбора информации о действиях пользователя (нажатия клавиш, посещенные сайты) и ее передачи злоумышленнику?

1) Вирус (Virus)
2) Червяк (Worm)
3) Кейлоггер (Keylogger)
4) Рекламное ПО (Adware)

Тема 3.3. Формальные модели безопасности автоматизированных систем

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Принцип "Наименьших привилегий" (Principle of Least Privilege) в управлении доступом означает, что:

1) Все пользователи должны иметь одинаковый уровень доступа к ресурсам для упрощения управления.
2) Пользователи должны получать доступ только после прохождения сложной многофакторной аутентификации.
3) Пользователям и процессам должны предоставляться только те права доступа (привилегии), которые абсолютно необходимы для выполнения их заранее определенных задач.
4) Администраторы должны иметь полный доступ ко всем системам без ограничений.

2. Что из перечисленного относится к мерам ФИЗИЧЕСКОЙ безопасности информационных активов?

1) Установка и настройка межсетевого экрана (брандмауэра).
2) Регулярное обновление антивирусного ПО на рабочих станциях.

3) Оборудование серверных помещений системой контроля доступа и системой видеонаблюдения.
4) Использование протокола HTTPS для шифрования трафика веб-сайта.

3. Что является основной целью регулярного создания резервных копий критически важных данных в контексте информационной безопасности?

1) Обеспечение конфиденциальности данных.
2) Предотвращение атак типа "Человек посередине" (MitM).
3) Поддержание доступности данных и возможности их восстановления после инцидентов.
4) Гарантирование целостности данных в реальном времени.

4. Какой тип атаки предполагает внедрение злоумышленником вредоносного кода в доверенный веб-сайт, с целью выполнения этого кода в браузере, ничего не подозревающего пользователя при посещении этого сайта?

1) SQL-инъекция (SQL Injection)
2) Межсайтовый скриптинг (Cross-Site Scripting)
3) Подмена DNS (DNS Spoofing)
4) Фишинг (Phishing)

5. Какое понятие описывает процесс выявления, оценки и принятия решений по обработке рисков для минимизации их потенциального негативного воздействия на информационные активы организации?

1) Управление инцидентами (Incident Management)
2) Аудит информационной безопасности (Security Audit)
3) Проведение пентестов (Penetration Testing)
4) Управление рисками информационной безопасности (Information Security Risk Management)

Тема 3.4. Особенности дискреционной и мандатной модели безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Что из перечисленного является КЛЮЧЕВЫМ отличием асимметричного шифрования (например, RSA) от симметричного шифрования (например, AES)?

1) Асимметричное шифрование всегда быстрее симметричного.
2) Асимметричное шифрование используется только для шифрования больших объемов данных.
3) Асимметричное шифрование использует пару ключей (открытый и закрытый), в то время как симметричное использует один общий секретный ключ.
4) Симметричное шифрование не обеспечивает конфиденциальность.

2. Для чего в первую очередь используется цифровой сертификат?

1) Для шифрования конфиденциальных данных при передаче по сети.
2) Для сжатия данных перед передачей.
3) Для привязки открытого ключа к идентификатору и подтверждения подлинности этого соответствия доверенной третьей стороной.
4) Для замены парольной аутентификации.

3. Что из перечисленного является ПРЕИМУЩЕСТВЕННОЙ целью системы обнаружения вторжений (Intrusion Detection System)?

1) Автоматический мониторинг сети или систем на предмет признаков злонамеренной активности или нарушений политик безопасности и генерация оповещений.
2) Автоматическая блокировка выявленных атак в реальном времени без вмешательства человека.
3) Замена межсетевого экрана (брандмауэра) для фильтрации трафика.
4) Шифрование всего сетевого трафика.

4. Какой тип политики безопасности описывает правила допустимого использования корпоративных информационных ресурсов (интернета, почты, компьютеров) сотрудниками организации?

1) Политика классификации данных (Data Classification Policy)

2) Политика управления доступом (Access Control Policy)
3) Политика допустимого использования (Acceptable Use Policy)
4) Политика резервного копирования и восстановления (Backup and Recovery Policy)

5. Что из перечисленного НАИБОЛЕЕ точно описывает концепцию "Защиты в глубину" (Defense in Depth)?

1) Установка самого дорогого и современного антивируса на все компьютеры.
2) Фокусировка всех усилий безопасности на защите периметра сети.
3) Реализация множественных, разнородных и перекрывающихся слоев защиты для создания комплексной безопасности, где прорыв одного слоя не ведет к полной компромитации системы.
4) Полное отключение всех систем от интернета.

Тема 3.5. Методы и критерии оценки защищенности компьютерных систем

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какая атака направлена на захват сеанса аутентифицированного пользователя путем похищения файла cookie сессии или токена, что позволяет злоумышленнику действовать от имени жертвы без знания ее логина и пароля?

1) SQL-инъекция (SQL Injection)
2) Кросс-сайтовая подделка запроса (Cross-Site Request Forgery - CSRF)
3) Захват сессии (Session Hijacking)
4) Фишинг (Phishing)

2. Какой криптографический примитив гарантирует ЦЕЛОСТНОСТЬ данных, генерируя уникальную "цифровую подпись" фиксированной длины из произвольного объема данных, при этом процесс необратим?

1) Симметричное шифрование (AES)
2) Хеш-функция (SHA-256, MD5)
3) Асимметричное шифрование (RSA)
4) Цифровая подпись (ЭЦП)

3. Какой метод аутентификации считается наиболее надежным для защиты от компрометации учетных записей из-за украденных паролей?

1) Использование сложных паролей (12+ символов)
2) Регулярная смена паролей (каждые 90 дней)
3) Многофакторная аутентификация (MFA)
4) Использование единого пароля для всех служебных систем

4. Что является главной целью этапа "Оценка рисков" в процессе управления рисками информационной безопасности?

1) Устранение всех обнаруженных уязвимостей
2) Идентификация активов, угроз и уязвимостей, оценка вероятности и последствий реализации угроз для определения уровня риска
3) Приобретение страховки от киберинцидентов
4) Назначение ответственных за безопасность каждого актива

5. Какой сетевой сегмент специально предназначен для размещения общедоступных сервисов (веб-сервер, почтовый сервер), изолируя их от внутренней сети и выступая буферной зоной?

1) Локальная сеть (LAN)
2) Беспроводная сеть (WLAN)
3) Виртуальная частная сеть (VPN)
4) Демилитаризованная зона (DMZ)

Тема 3.7. Защита информации, обрабатываемой в автоматизированных системах от технических разведок

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой тип атака, входящий в OWASP Top 10, позволяет внедрять и выполнить произвольный код на сервере или получить несанкционированный доступ к данным?

1) Межсайтовый скриптинг (XSS)
2) Внедрение (Injection)
3) Небезопасная десериализация
4) Подделка межсайтовых запросов (CSRF)

2. Какое правило резервного копирования считается минимально достаточным для защиты от потери данных в результате сбоя оборудования, программной ошибки или атаки шифровальщика (ransomware)?

1) Ежедневное копирование на внешний диск
2) Копирование на ленту (tape) раз в неделю
3) Правило 3-2-1: 3 копии данных, 2 разных носителя, 1 копия на удаленном носителе
4) Использование RAID-массива

3. Какой тип шифрования использует ОДИН ключ, как для шифрования, так и для расшифрования информации?

1) Симметричное шифрование (AES, DES, 3DES)
2) Асимметричное шифрование (RSA, ECC)
3) Хеширование (SHA-256)
4) Цифровая подпись (DSA)

4. Какая мера физической безопасности НАИБОЛЕЕ эффективно предотвращает несанкционированный доступ в серверное помещение?

1) Табличка "Посторонним вход воспрещен"
2) Замок с ключом на двери
3) Система контроля доступа (СКУД) с использованием идентификационных карт и постоянным мониторингом.
4) Установка камеры наблюдения над дверью

5. Что является ПЕРВОЙ ключевой фазой управления инцидентами информационной безопасности?

1) Устранение (сдерживание и ликвидация угрозы)
2) Восстановление (возврат систем в рабочее состояние)
3) Подготовка (разработка плана, назначение ролей, создание инструментов)
4) Постинцидентный анализ (извлечение уроков)

7. Оценочные материалы промежуточной аттестации

5 семестр, Зачет

Контролируемые ИДК: УК-8.1 УК-8.2 УК-8.3 УК-8.4 ОПК-2.1 ОПК-10.1 ОПК-2.2 ОПК-10.2 ОПК-2.3 ОПК-10.3 ОПК-2.4 ОПК-2.5 ОПК-2.6 ОПК-2.7

Вопросы/Задания:

1. Понятие национальной безопасности Российской Федерации.

2. Национальные интересы РФ и стратегические национальные приоритеты.

3. Роль информационной безопасности в обеспечении национальной безопасности государства.

4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

5. Понятие информационной безопасности Российской Федерации.

6. Интересы личности общества и государства в информационной сфере.

7. Виды угроз информационной безопасности Российской Федерации.

8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.

9. Методы обеспечения информационной безопасности Российской Федерации.

10. Источники понятий в области информационной безопасности.

11. Основные понятия информационной безопасности.

12. Общеметодологические принципы теории информационной безопасности.

13. Понятие и сущность защищаемой информации.

14. Права и обязанности обладателя информации.

15. Виды защищаемой информации.

16. Перечень сведений конфиденциального характера.

17. Понятие интеллектуальной собственности и особенности ее защиты.

18. Понятие угрозы информационной безопасности.

19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.

20. Классификация и виды угроз информационной безопасности.

21. Протоколирование и аудит как сервисы безопасности.

22. Криптографические сервисы безопасности.

23. Экранирование как сервис безопасности.

24. Анализ защищенности как сервис безопасности.

25. Управление как сервис безопасности.

26. Назначение формальных моделей безопасности. Политика безопасности.

27. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.

28. Мандатная модель безопасности. Модель Белла-ЛаПадулы.

29. Формальные модели целостности.

30. Понятие ролевого управления доступом.

31. Модели, стратегии и системы обеспечения информационной безопасности.

32. Критерии безопасности компьютерных систем «Оранжевая книга».

33. Общие критерии безопасности информационных технологий.

34. Критерии и классы защищенности СВТ и АС. Руководящие документы ФСТЭК России.

35. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

36. Классификация и возможности технических разведок.

37. Компьютерная разведка.

38. Технические каналы утечки информации при эксплуатации автоматизированных систем.

39. Электромагнитное воздействие и эффекты его воздействия.

40. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.