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: 5BFEE1D286E9C95A0C0D2C611E434BD5
Владелец: Степанченко Алексей Леонидович
Действителен: с 23.09.2026 по 17.12.2027

«УТВЕРЖДАЮ»
Проректор
А. Л. Степанченко
24 марта 2025 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) «Б1.В.01 ЗАЩИТА ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ ГЕОИНФОРМАЦИОННЫХ СИСТЕМАХ»

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль) подготовки: Защита информации в геоинформационных системах и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2025

Срок получения образования: 2 года

Объем: в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2025

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Ширинкин С. Г.

Старший преподаватель кафедры
Информационно-измерительных систем Сутягин Д. Д.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

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	14.10.2024, № 10-24

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

ПК-1 Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-1.1 Разрабатывает профили защиты компьютерных систем

Знать:

ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных

Уметь:

ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы

Владеть:

ПК-1.1/Нв1 Разрабатывать комплексные профили защиты для различных типов компьютерных систем, учитывая их специфику и назначение

ПК-1.2 Формирует политики безопасности компьютерных систем и сетей

Знать:

ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

Уметь:

ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

Владеть:

ПК-1.2/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации

ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)

ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности

Знать:

ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности

ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем

Уметь:

ПК-2.1/Ум1 Оценивать эффективность защиты информации

ПК-2.1/Ум2 Оценивать реальный уровень защищенности анализируемых компьютерных систем

Владеть:

ПК-2.1/Нв1 Навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных

Знать:

ПК-2.2/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации

ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения

ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия

Уметь:

ПК-2.2/Ум1 Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных

ПК-2.2/Ум2 Выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем

Владеть:

ПК-2.2/Нв1 Навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия

ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

Знать:

ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности

Уметь:

ПК-2.3/Ум1 Подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

Владеть:

ПК-2.3/Нв1 Навыками работы с инструментами анализа защищенности

ПК-2.3/Нв2 Навыками анализа журналов событий и других источников информации о состоянии компьютерной системы

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)

ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности

Знать:

ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности

Уметь:

ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

Владеть:

ПК-3.1/Нв2 Навыками по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты

Знать:

ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа

ПК-3.2/Зн2 Принципы и методы организационной защиты информации

ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак

Уметь:

ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации

ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений

ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения

Владеть:

ПК-3.2/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа

ПК-3.2/Нв2 Навыками работы с криптографическими библиотеками и инструментами верификации

ПК-3.2/Нв3 Методиками обеспечения безопасности при обработке и верификации криптографических сообщений

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации

Знать:

ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем

ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий

Уметь:

ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем

ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений

ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей

Владеть:

ПК-3.3/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации

ПК-3.3/Нв2 Методами анализа и формализации информационных процессов объекта и связей между ними

ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

Знать:

ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI

Уметь:

ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации

Владеть:

ПК-3.4/Нв1 Навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ПК-1 Способен разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)	Повышенный	ИДК ПК-1.1 Разрабатывает профили защиты компьютерных систем Знать: ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных Уметь: ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы Владеть: ПК-1.1/Нв1 Разрабатывать комплексные профили защиты для различных типов компьютерных систем, учитывая их специфику и назначение ИДК ПК-1.2 Формирует политики безопасности компьютерных систем и сетей Знать: ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности Уметь: ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных) Владеть: ПК-1.2/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации

	Базовый	ИДК ПК-1.1 Разрабатывает профили защиты компьютерных систем Знать: ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных Уметь: ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы ИДК ПК-1.2 Формирует политики безопасности компьютерных систем и сетей Знать: ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности Уметь: ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)
	Пороговый	ИДК ПК-1.1 Разрабатывает профили защиты компьютерных систем Знать: ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных ИДК ПК-1.2 Формирует политики безопасности компьютерных систем и сетей Знать: ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности

ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)	Повышенный	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем Уметь: ПК-2.1/Ум1 Оценивать эффективность защиты информации ПК-2.1/Ум2 Оценивать реальный уровень защищенности анализируемых компьютерных систем Владеть: ПК-2.1/Нв1 Навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия Уметь: ПК-2.2/Ум1 Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Ум2 Выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем Владеть: ПК-2.2/Нв1 Навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия

		ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности Уметь: ПК-2.3/Ум1 Подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах Владеть: ПК-2.3/Нв1 Навыками работы с инструментами анализа защищенности ПК-2.3/Нв2 Навыками анализа журналов событий и других источников информации о состоянии компьютерной системы
	Базовый	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности Уметь: ПК-2.1/Ум2 Оценивать реальный уровень защищенности анализируемых компьютерных систем ПК-2.1/Ум1 Оценивать эффективность защиты информации
	Базовый	ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации Уметь: ПК-2.2/Ум2 Выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем

		ПК-2.2/Ум1 Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности Уметь: ПК-2.3/Ум1 Подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах
	Пороговый	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности
	Пороговый	ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия ПК-2.2/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности

ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)	Повышенный	ИДК ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности Знать: ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности Уметь: ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности Владеть: ПК-3.1/Нв2 Навыками по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации
ПК-3 Способен разрабатывать проектные решения по защите информации автоматизированных систем (в том числе в геоинформационных системах)	Повышенный	ИДК ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты Знать: ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа ПК-3.2/Зн2 Принципы и методы организационной защиты информации ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак Уметь: ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения Владеть: ПК-3.2/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа ПК-3.2/Нв2 Навыками работы с криптографическими библиотеками и инструментами верификации ПК-3.2/Нв3 Методиками обеспечения безопасности при обработке и верификации криптографических сообщений

			ИДК ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации Знать: ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий Уметь: ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей Владеть: ПК-3.3/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации ПК-3.3/Нв2 Методами анализа и формализации информационных процессов объекта и связей между ними ИДК ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Знать: ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI Уметь: ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации Владеть: ПК-3.4/Нв1 Навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования

	Базовый	ИДК ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности Знать: ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности Уметь: ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности
	Базовый	ИДК ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты Знать: ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак ПК-3.2/Зн2 Принципы и методы организационной защиты информации ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа Уметь: ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения ИДК ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации Знать: ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем Уметь: ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений

		ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем ИДК ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Знать: ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Уметь: ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации
	Пороговый	ИДК ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности Знать: ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности
	Пороговый	ИДК ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты Знать: ПК-3.2/Зн2 Принципы и методы организационной защиты информации ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа ИДК ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации Знать: ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем

		ИДК ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) Знать: ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем)

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ПК-1.1 Разрабатывает профили защиты компьютерных систем ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы ПК-1.1/Нв1 Разрабатывать комплексные профили защиты для различных типов компьютерных систем, учитывая их специфику и назначение ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Ум1 Оценивать эффективность защиты информации ПК-2.1/Ум2 Оценивать реальный уровень защищенности анализируемых компьютерных систем ПК-2.1/Нв1 Навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Нв2 Навыками по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации

ПК-1.2 Формирует политики безопасности компьютерных систем и сетей
ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности
ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)
ПК-1.2/Нв1 Формировать и внедрять политики безопасности для компьютерных систем и сетей на уровне организации

ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных
ПК-2.2/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации
ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения
ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия
ПК-2.2/Ум1 Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных
ПК-2.2/Ум2 Выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем
ПК-2.2/Нв1 Навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты
ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа
ПК-3.2/Зн2 Принципы и методы организационной защиты информации
ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак
ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации
ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений
ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения
ПК-3.2/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа
ПК-3.2/Нв2 Навыками работы с криптографическими библиотеками и инструментами верификации
ПК-3.2/Нв3 Методиками обеспечения безопасности при обработке и верификации криптографических сообщений

ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах
ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности
ПК-2.3/Ум1 Подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах
ПК-2.3/Нв1 Навыками работы с инструментами анализа защищенности
ПК-2.3/Нв2 Навыками анализа журналов событий и других источников информации о состоянии компьютерной системы

	ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей ПК-3.3/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации ПК-3.3/Нв2 Методами анализа и формализации информационных процессов объекта и связей между ними ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации ПК-3.4/Нв1 Навыками проектирования и построения локальных и глобальных компьютерных сетей с использованием современных технологий и оборудования
Хорошо	ПК-1.1 Разрабатывает профили защиты компьютерных систем ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных ПК-1.1/Ум2 Разрабатывать модель угроз для распределенной геоинформационной системы ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Ум1 Оценивать эффективность защиты информации ПК-2.1/Ум2 Оценивать реальный уровень защищенности анализируемых компьютерных систем ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-3.1/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности

ПК-1.2 Формирует политики безопасности компьютерных систем и сетей
ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности
ПК-1.2/Ум1 Умеет разрабатывать требования по защите и формировать политики безопасности компьютерных систем и сетей (в том числе в геоинформационных системах и системах сбора пространственных данных)

ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных
ПК-2.2/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации
ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения
ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия
ПК-2.2/Ум1 Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных
ПК-2.2/Ум2 Выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем

ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты
ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа
ПК-3.2/Зн2 Принципы и методы организационной защиты информации
ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак
ПК-3.2/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации
ПК-3.2/Ум2 Выполнять проверку цифровых подписей и других криптографических атрибутов сообщений
ПК-3.2/Ум3 Анализировать результаты верификации и выявлять случаи нарушения целостности или подлинности сообщения

ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах
ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности
ПК-2.3/Ум1 Подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации
ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем
ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий
ПК-3.3/Ум1 Разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности распределенных информационных систем
ПК-3.3/Ум2 Развертывать веб-приложения в безопасной среде и поддерживать безопасность веб-приложений
ПК-3.3/Ум3 Осуществлять разработку и проектирование информационных систем в соответствии с поставленной задачей

	ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации
Удовлетворительно	ПК-1.1 Разрабатывает профили защиты компьютерных систем ПК-1.1/Зн2 Специфику защиты пространственных данных в геоинформационных системах и системах сбора пространственных данных ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн1 Способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 Основные нормативные документы в области анализа безопасности компьютерных систем ПК-3.1 Классифицирует защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Зн1 Нормативно-правовые документы в области защиты информации, определяющие виды тайн и устанавливающие степени конфиденциальности ПК-1.2 Формирует политики безопасности компьютерных систем и сетей ПК-1.2/Зн3 Знать стандарты в области информационной безопасности, необходимые при работе с программно-аппаратными и техническими средствами защиты информации в составе комплексов средств защиты с целью противодействия угрозам нарушения информационной безопасности ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн1 Методы и методики оценки безопасности программно-аппаратных средств защиты информации ПК-2.2/Зн2 Основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн3 Классы инструментов тестирования на про-никновения, принципы их действия ПК-3.2 Определяет типы субъектов доступа и объектов доступа, являющихся объектами защиты ПК-3.2/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа ПК-3.2/Зн2 Принципы и методы организационной защиты информации ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Зн1 Методы и инструменты оценки уровня защищенности

	ПК-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ПК-3.3/Зн2 Программные, технические и методические средства информационных технологий ПК-3.4 Понимает принципы построения и функционирования современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн1 Принципы построения и функционирования, примеры реализации современных локальных и глобальных компьютерных сетей и их компонентов (в том числе геоинформационных систем) ПК-3.4/Зн2 Стек протоколов TCP/IP и модель OSI
Неудовле-творительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

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

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Введение в проблематику защиты пространственных данных	ПК-1.1 ПК-2.1 ПК-3.4	Практическая работа Тестирование	Экзамен
2	Распределенные системы	ПК-1.1 ПК-2.2 ПК-2.3 ПК-3.2 ПК-3.4	Практическая работа Тестирование	Экзамен
3	Распределенные геоинформационные системы	ПК-2.1 ПК-2.2 ПК-3.3 ПК-3.4	Практическая работа Тестирование	Экзамен
4	Защита информации в распределенных геоинформационных системах	ПК-1.1 ПК-1.2 ПК-2.1 ПК-3.1	Практическая работа Тестирование	Экзамен

5. Порядок проведения промежуточной аттестации

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

Промежуточная аттестация: Экзамен, 3 семестр.
Промежуточная аттестация по дисциплине проводится в форме экзамена. Конкретная форма проведения — компьютерное тестирование по теоретическому материалу или устное собеседование по вопросам билетов — утверждается кафедрой и доводится до сведения обучающихся не позднее чем за месяц до начала промежуточной аттестации. При компьютерном тестировании итоговый результат определяется как отношение количества набранных баллов к максимально возможному количеству баллов. При устном собеседовании билет включает вопросы из перечня вопросов; преподаватель вправе задать дополнительные и уточняющие вопросы.

Критерии оценивания при проведении промежуточной аттестации в форме компьютерного тестирования:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- оценка «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если основное содержание освоено; допущены отдельные неточности, не влияющие на общее понимание материала;
- оценка «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и ошибки;
- оценка «неудовлетворительно» выставляется, если обучающийся набрал 0–55 баллов; не освоен необходимый минимум содержания дисциплины; результаты обучения не достигнуты.

Критерии оценивания при проведении промежуточной аттестации в форме устного собеседования по билетам:
Экзамен оценивается по пятибалльной шкале:
- оценка «отлично» выставляется, если даны полные, правильные и логически последовательные ответы; терминология применяется корректно; приведены необходимые обоснования и примеры; дополнительные вопросы раскрыты;
- оценка «хорошо» выставляется обучающемуся, если вопросы раскрыты правильно и достаточно полно; отдельные неточности исправлены после уточняющих вопросов;
- оценка «удовлетворительно» выставляется обучающемуся, если основные положения раскрыты фрагментарно; имеются существенные неточности, однако базовое понимание продемонстрировано;
- оценка «неудовлетворительно» выставляется, если вопросы не раскрыты либо допущены принципиальные ошибки; отсутствует владение базовой терминологией.

6. Оценочные материалы текущего контроля

Раздел 1. Введение в проблематику защиты пространственных данных

Контролируемые ИДК: ПК-1.1 ПК-2.1 ПК-3.4

Тема 1.1. Введение в проблематику защиты пространственных данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Описание защищаемых геоданных

На учебной карте выделить точки, линии, полигоны и растровый слой; для каждого набора указать геометрию, атрибуты, назначение и чувствительные сведения. Объяснить, какие объекты требуется защищать при хранении и обмене.

2. Классификация сведений в ГИС

Рассмотреть три условных набора: адреса названных жителей, внутренние коммерчески ценные сведения и материалы, законно отнесенные к государственной тайне. Указать правовое основание каждого режима, необходимые исходные факты и случаи, когда данных для классификации недостаточно. Не присваивать грифы условным сведениям без основания.

3. Модель угроз пространственным данным

Для учебной ГИС с филиалом, веб-порталом и общим хранилищем выделить данные, участников и каналы обмена. Описать три коротких сценария нарушения конфиденциальности, целостности или доступности; связать каждый с возможностями нарушителя и последствиями для работы с картой

4. Субъекты, объекты и правила обращения

По заданным функциям наблюдателя, редактора и администратора определить доступные им слои и операции. Подготовить небольшой проект правил обращения с данными: кто разрешает доступ, как фиксируется изменение роли и что происходит при отсутствии разрешения. Сопоставить правила с нормативным основанием из предыдущей работы.

5. Учебный проект профиля защиты

Подготовить учебный проект ПЗ для типа «сервер геоинформационных данных». Описать тип объекта и среду, угрозы, политики и предположения, цели защиты, направления функциональных требований и требований доверия с обоснованием связей. Отдельно отметить разделы утверждений о соответствии и расширенных компонентов. Если точный компонент требований не изучен, обозначить его подбор как незавершенный, не придумывать обозначение. Сопоставить полученный проект со структурой приложения В ГОСТ Р ИСО/МЭК 15408-1-2012.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется привязка растрового изображения к положению на земной поверхности?

2. Какой тип объекта GeoJSON содержит массив объектов Feature?

3. Что означает третье число в позиции GeoJSON [37.6, 55.7, 180] по RFC 7946?

4. Как называется отдельная точка с координатами, из последовательности которых строится ломаная?

5. Какой растр подробнее представляет местность при одинаковом качестве исходной съемки: с ячейкой 2 м или 20 м?

6. Дороги должны соединяться на перекрестке, но их концы не соприкасаются. Какой дефект связности следует исправить?

7. В GeoJSON дописали к координатам четыре нуля после запятой. Доказывает ли это повышение точности измерения?

8. ГИС хранит закрытый слой на сервере и его выгрузки на рабочих станциях. В модель угроз включен только сервер. Какие экземпляры данных пропущены?

Раздел 2. Распределенные системы

Контролируемые ИДК: ПК-1.1 ПК-2.2 ПК-2.3 ПК-3.2 ПК-3.4

Тема 2.1. Распределенные системы

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Схема распределенного обмена

Изобразить клиент, веб-сервис, базу данных и удаленный филиал; подписать направления обмена и используемые прикладные и транспортные протоколы. Сопоставить уровни TCP/IP и OSI и объяснить место TLS между прикладным протоколом и надежным транспортом, не отождествляя название TLS с точным номером уровня OSI.

2. Сравнение интерфейсов REST и SOAP

Изучить два небольших примера обмена одной и той же геоинформацией: ресурсный HTTP-интерфейс и SOAP-сообщение. Сравнить назначение, структуру сообщений, способы задания операции и доступные точки контроля. Сформулировать, какие наблюдения нужны для анализа безопасности каждого варианта; не объявлять один подход безопасным только по названию

3. Проверка повторного запроса

На изолированном учебном сервисе выполнить повтор одинакового PUT и повтор операции создания, для которой защита от дублей не задана. Сохранить состояние ресурса и ответы, сравнить предусмотренный эффект. Для случая потерянного ответа предложить проверку состояния операции перед повтором. Реальные внешние сервисы не используются.

4. Анализ отставания реплики

На учебном стенде или по выданному журналу синхронизации сравнить версии основного узла и асинхронной реплики. Оценить, какие данные увидит клиент при переключении, и подготовить отчет с условиями опыта, наблюдаемыми различиями, риском и ограничениями вывода. Не считать единственный успешный опыт доказательством общей надежности.

5. Построение виртуальной сети распределенной ГИС

Выбрать простую топологию для клиента, сервиса и базы данных в двух сегментах; обосновать размещение узлов и необходимые соединения. Собрать эту сеть в доступной среде виртуализации, настроить адресацию и разрешенные потоки, проверить связность и запрет ненужного прямого доступа к базе.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой HTTP-метод позволяет получить метаданные представления, не передавая его содержимое в ответе?

2. Как называется элемент SOAP, который сообщает об ошибке обработки сообщения?

3. Какой HTTP-код означает успешное выполнение обычного GET-запроса: 200 или 500?

4. Какое поле заголовка HTTP сообщает формат содержимого ответа, например application/json?

5. API поддерживает контроль версии через ETag. Какое условие заголовка отправляют при изменении, чтобы не затереть чужую правку: If-Match или Content-Language?

6. Как называется сохранение ответа для повторного использования без обязательного нового получения того же содержимого с исходного сервера?

7. Сервер записывает обращение GET в журнал. Делает ли одна эта запись метод небезопасным в смысле семантики HTTP?

8. REST-сервис хранит геообъекты в базе. Противоречит ли само хранение ресурсов ограничению отсутствия состояния клиентского сеанса?

Раздел 3. Распределенные геоинформационные системы

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-3.3 ПК-3.4

Тема 3.1. Распределенные геоинформационные системы.

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка выдачи геообъекта

На учебном сервисе получить представление отдельного объекта и сопоставить его геометрию и атрибуты с исходным набором. Проверить понятный случай неверного идентификатора и зафиксировать ответ. Объяснить, какие наблюдения характеризуют корректность выдачи и какие вопросы безопасности этот опыт еще не решает.

2. Сопоставление карты и исходных данных

Получить изображение территории и представление геообъектов по одному учебному набору. Сравнить, какие сведения раскрываются в каждом результате, включая подписи и атрибуты. Предложить критерии проверки допустимости публикации каждого результата.

3. Права на операции геосервиса

Настроить на учебном сервисе роли наблюдателя и редактора, разделить чтение и изменение объектов. Проверить разрешенные действия, запрещенную правку и обращение к чужому закрытому объекту по известному идентификатору. Оформить примененную политику и порядок ее пересмотра при смене обязанностей.

4. Правила публикации каталога

Подготовить проект регламента публикации метаданных: состав открытого описания, ответственный за согласование, проверка ссылок, условия изменения и снятия записи. Для закрытого набора отдельно определить доступность описания и самого ресурса; связать решения с правовым режимом данных

5. Проверка обрабатывающего сервиса

Выполнить на учебных данных простую операцию отбора объектов по заданной области. Проверить корректный результат, отсутствие необходимых прав и недоступность входного набора; сопоставить наблюдаемое поведение с заранее указанными ожиданиями. Описать, какие выводы можно сделать о проверенных механизмах.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какое значение rel у ссылки OGC API — Features указывает на следующую страницу результатов?

2. Какой параметр OGC API — Features задает прямоугольную область пространственного отбора?

3. Что считает поле numberReturned: объекты в текущем ответе или все объекты, подходящие под запрос?

4. В метаданных набора указано «глубина», но неизвестно, в метрах или сантиметрах. Какое описание измерения нужно добавить?

5. Обрабатывающий геосервис ответил HTTP 202 Accepted. Означает ли это, что обработка уже завершена?

6. Разрешено ли в GeoJSON значение geometry: null для Feature, местоположение которого не задано?

7. Сервис принимает размер выходной карты от 1 до 2000 пикселей. Запрошено 100000 пикселей. Следует выполнить запрос или отклонить его по заданному ограничению?

Раздел 4. Защита информации в распределенных геоинформационных системах

Контролируемые ИДК: ПК-1.1 ПК-1.2 ПК-2.1 ПК-3.1

Тема 4.1. Защита информации в распределенных геоинформационных системах

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Защищенный канал и прикладные полномочия

Подключить учебный клиент к сервису по TLS с предусмотренной проверкой подлинности сервера; сравнить успешное соединение с отказом при недоверенном удостоверении. Затем проверить разрешенное чтение и запрещенное изменение под одной учетной записью. Объяснить, какие свойства относятся к каналу, а какие — к прикладной политике.

2. Анализ журнала геосервиса

По учебному журналу найти успешное чтение, отказ в изменении и повторный запрос; связать записи по времени, субъекту, объекту и идентификатору операции. Подготовить краткое заключение, отделив наблюдаемые факты от предположений. Предложить недостающие поля, не включая пароли и секретные ключи.

3. Оценка исправления контроля доступа

В двух конфигурациях учебного сервиса проверить одинаковые разрешенные и запрещенные обращения, включая подмену идентификатора объекта. Зафиксировать версии, условия и результаты; оценить, устраняет ли исправление обнаруженное нарушение и не ломает ли разрешенный доступ. Подготовить отчет о проверенной защищенности и основаниях доверия без присвоения оценочного уровня.

4. Согласование модели защиты ГИС

Для ранее построенной сети собрать единую схему данных, сервисов, границ доверия и механизмов защиты. Проверить цепочки «угроза — цель — требование — механизм — проверка» и согласованность с учебным проектом ПЗ; устранить один обнаруженный пробел и объяснить принятое решение.

5. Порядок изменения защищенной ГИС

Подготовить небольшой регламент добавления нового слоя: анализ назначения и правового режима, определение объектов и субъектов доступа, согласование прав, настройка, проверка и публикация. Применить его к искусственному примеру и показать, какие документы и настройки меняются. Итог согласовать с действующей учебной политикой.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется принцип выдачи сервисной учетной записи только тех прав, которые нужны для ее работы?

2. Какое общее значение в журналах нескольких сервисов помогает собрать события одного пользовательского обращения?

3. Какие сведения, кроме названия, помогают отличить две редакции одного профиля защиты?

4. Допустимо ли сохранять введенный пароль открытым текстом в журнале входа?

5. Учебное правило разрешает с клиента только TCP-порт 443 сервера. Разрешает ли это же правило подключение к TCP-порту 8443?

6. Имя сервиса в проверенном сертификате не соответствует запрошенному имени. Что правильно: отключить проверку имени или устранить несоответствие?

7. Обязательно ли каждый TLS 1.3-клиент предъявляет серверу собственный сертификат?

7. Оценочные материалы промежуточной аттестации

3 семестр, Экзамен

Контролируемые ИДК: ПК-1.1 ПК-2.1 ПК-3.1 ПК-1.2 ПК-2.2 ПК-3.2 ПК-2.3 ПК-3.3 ПК-3.4

Вопросы/Задания:

1. Чем геометрия отличается от атрибутов пространственного объекта?

2. В чем основное различие векторного и растрового представления?

3. Когда сведения о местоположении относятся к персональным данным?

4. Что нужно указать в простом сценарии угрозы геоданным?

5. Для чего нужен профиль защиты и какова его связь с конкретным продуктом?

6. Почему отсутствие ответа распределенного сервиса не доказывает отсутствие выполненного действия?

7. Что означает идемпотентность HTTP-метода?

8. Какие признаки помогают отличить REST от произвольного обмена JSON?

9. Из каких основных частей состоит сообщение SOAP?

10. Как отставание реплики влияет на чтение и переключение?

11. Что получает клиент при запросе карты WMS?

12. Для чего нужен доступ к отдельным геообъектам через API?

13. Чем обрабатывающий сервис отличается от простой выдачи исходного набора?

14. Почему право читать слой не означает права изменять его?

15. Что защищает TLS и чего наличие TLS само по себе не подтверждает?

16. Почему разрешение проверяют при каждом обращении к объекту?

17. Какие сведения журнала помогают объяснить отказ в доступе?

18. Как определить необходимые сетевые правила между сервисом и базой?

19. Как связать модель угроз с проверкой защитного механизма?

20. Какую задачу решает сервис каталога метаданных?