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
15 мая 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ) «Б1.В.ДВ.01.02 РАЗРАБОТКА БЕЗОПАСНЫХ ГЕОСЕРВИСОВ»

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): 2026

Срок получения образования: 2 года

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

Москва, 2026

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	05.11.2025, № 12-25

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

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

ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности

ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации

Уметь:

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

ПК-3.1/Ум2 Выявлять и устранять потенциальные угрозы безопасности в веб-приложениях

ПК-3.1/Ум3 Обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей

Владеть:

ПК-3.1/Нв1 Методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным 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-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/Зн4 Форматы криптографических сообщений и стандарты их представления

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/Зн3 Технологии проектирования и построения защищенных информационных систем

ПК-3.4/Зн4 Особенности архитектуры распределённых информационных систем и роли системного программного обеспечения в них

Уметь:

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

ПК-3.4/Ум2 Выполнять настройку системного программного обеспечения с учетом требований информационной безопасности

Владеть:

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

ПК-3.4/Нв2 Навыками работы с системным программным обеспечением различных платформ в распределённых ИС

2. Показатели и критерии оценивания компетенций

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

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 ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	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/Зн2 Методы безопасности веб-приложения от критических угроз безопасности ПК-3.1/Зн3 Систему нормативных правовых актов, нормативных и методических документов в области информационной безопасности и защиты информации
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	Основы безопасных геосервисов	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа Тестирование	Экзамен
2	Безопасная разработка программного обеспечения	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа Тестирование	Экзамен
3	Сетевая безопасность	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа Тестирование	Экзамен
4	Шифрование	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа	Экзамен

5	Инструменты и технологии	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа	Экзамен
6	Тематические исследования и проекты	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа	Экзамен
7	Профессиональное развитие	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Практическая работа	Экзамен

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

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

Промежуточная аттестация: Экзамен, 1 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. Основы безопасных геосервисов
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 1.1. Геопространственные системы и безопасность

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Классификация данных геосервиса

Разобрать учебный перечень наборов: общедоступная карта, маршруты определяемых лиц, сведения с установленным режимом коммерческой тайны и сведения, законно отнесенные к государственной тайне. Для каждого набора указать основание режима и необходимые ограничения, не назначая гриф по одному названию.

2. Состав данных сервиса местоположения

Для учебного сервиса подсчета посещаемости районов определить действительно нужные поля. Отметить сведения, позволяющие связать маршрут с человеком, и предложить состав выдачи для заявленной цели.

3. Угрозы геосервису

По схеме клиента, API, геобазы и выгрузок выделить защищаемые объекты и описать несколько коротких сценариев воздействия. Связать каждый сценарий с последствиями для данных или работы сервиса.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Расположите этапы подготовки описания угрозы для нового интерфейса.

А. Определить возможное воздействие на эти данные
Б. Описать последствия выбранного воздействия
В. Описать назначение интерфейса и обрабатываемые данные

2. Упорядочьте работу по проверке необходимости полей формы сбора персональных данных.

А. Исключить поля, избыточные для указанной цели
Б. Зафиксировать цель обработки
В. Сопоставить каждое поле с этой целью

3. Восстановите порядок принятия сервером решения о чтении закрытого объекта.

А. Проверить его разрешение на запрошенный объект
Б. Получить запрос и установить субъекта доступа
В. Выдать данные только при положительном решении

4. В организации уже утвержден режим коммерческой тайны. Упорядочьте предоставление доступа новому сотруднику по установленному порядку.

А. Предоставить предусмотренный доступ и учесть получившее его лицо
Б. Оформить допуск и обязательства по установленным правилам
В. Определить необходимые для его работы сведения

5. Упорядочьте преобразование подготовленной геометрии в GeoJSON Feature для передачи клиенту.

А. Добавить согласованные атрибуты в properties

Б. Собрать Feature и проверить корректность представления
В. Получить геометрию в системе координат, требуемой GeoJSON

Раздел 2. Безопасная разработка программного обеспечения
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 2.1. Методологии безопасной разработки программного обеспечения

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Матрица доступа к слоям и объектам

Для читателя, редактора и администратора определить разрешенные действия с учебными слоями. Проверить примеры разрешенных и запрещенных запросов, включая обращение к чужому объекту.

2. Проверка входных данных геоAPI

Разобрать учебный обработчик координат и поискового условия. Установить проверки формата и допустимых диапазонов; представить параметризованный запрос к данным и короткие примеры его проверки.

3. Правила внесения безопасных изменений

Подготовить краткий проект регламента исправления дефекта геосервиса: регистрация, ответственные лица, проверка правки, согласование и фиксация версии. Применить его к одной учебной ошибке.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте работу с подтвержденным дефектом программы.

А. Зарегистрировать воспроизводимое описание дефекта
Б. Повторить проверку и зафиксировать результат
В. Внести исправление в проверяемую версию

2. Расположите шаги выполнения запроса с отдельно передаваемым значением параметра.

А. Передать значение через механизм связывания параметров
Б. Подготовить текст SQL с местом для параметра
В. Выполнить подготовленный запрос

3. Упорядочьте проверку строкового параметра широты перед вычислением.

А. Проверить допустимый диапазон полученного числа
Б. Проверить возможность преобразования строки в число
В. Использовать прошедшее проверки значение

4. Упорядочьте включение согласованной правки в общий проект.

А. Передать ее на проверку
Б. Включить одобренную правку в общую версию
В. Зафиксировать правку в рабочей ветке

5. Упорядочьте формирование записи о завершенной операции доступа.

А. Передать подготовленную запись в журнал
Б. Получить результат операции и контекст запроса
В. Сформировать запись без запрещенных к журналированию секретов

Раздел 3. Сетевая безопасность
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 3.1. Настройка WAF и управление им

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Сетевые связи учебного геосервиса

Построить схему клиент — сервер приложения — геобаза. Для необходимых соединений определить стороны, протоколы и порты; составить ограничивающие правила и проверить разрешенное и лишнее соединение на выделенном стенде либо по предоставленной конфигурации.

2. Разбор срабатываний WAF

Исследовать небольшую учебную выборку событий WAF: определить сработавшие правила, накопленные баллы и решения при заданном пороге. Отделить подтвержденные атаки от запросов, требующих уточнения.

3. Регламент изменения правил WAF

Подготовить проект порядка изменения правил для подтвержденного ложного срабатывания. Ограничить область исключения и описать проверку допустимых и контрольных запросов, согласование и возможность возврата настройки.

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Упорядочьте обработку входящего запроса в обычном режиме оценки аномалий CRS без ранней блокировки.

А. Принять решение о передаче запроса приложению
Б. Выполнить правила проверки входящего запроса
В. Сравнить накопленный балл с порогом

2. Упорядочьте разбор ошибочной блокировки допустимого запроса WAF.

А. Проверить причину и подтвердить ложное срабатывание
Б. Найти запись срабатывания и соответствующий запрос
В. Внести обоснованное ограниченное исключение и проверить его

Раздел 4. Шифрование

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 4.1. Технологии шифрования данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка удостоверения геосервиса

По учебным сертификатам и именам узлов определить, какие соединения проходят проверку имени и срока. Объяснить, где выполняется проверка доверия и почему ее нельзя заменять нажатием «продолжить».

2. Доступ к ключам приложения

Составить схему хранения и использования ключей учебного геосервиса. Определить роли доступа, порядок плановой замены и действия при публикации ключа в репозитории.

3. Защита участков передачи данных

Для схемы браузер — прокси — API — геобаза отметить окончания защищенных соединений. Предложить конфигурацию защиты каждого требуемого участка и показать, какие сведения проверяются на стороне клиента соединения.

Раздел 5. Инструменты и технологии

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 5.1. Программное обеспечение ГИС и геопространственные базы данных

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка набора пространственных данных

Импортировать небольшой разрешенный набор или разобрать предоставленный результат

импорта. Проверить систему координат, типы геометрий, атрибуты и несколько специально заданных ошибок; предложить исправление без подмены системы одним новым SRID.

2. Права учетной записи геобазы

Настроить либо проверить по выданному скрипту отдельную роль приложения для чтения одной таблицы. Проверить эффективные полномочия, включая наследуемые права и владение, затем испытать разрешенное чтение и запрещенное изменение.

3. Публикация открытого и закрытого слоя

Подготовить конфигурацию учебного геосервера для двух слоев с разными режимами доступа. Проверить прямые обращения к каждому слою и отметить, какие атрибуты допустимы в публикуемом наборе.

Раздел 6. Тематические исследования и проекты

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 6.1. Тематические исследования и групповые проекты

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Техническое задание на защищенный геосервис

Для небольшого учебного сценария подготовить фрагмент ТЗ: назначение, данные, роли, требования защиты и наблюдаемые критерии приемки. Связать требования с выбранными сценариями угроз.

2. Проверка согласованности группового проекта

Объединить описания клиента, API и геобазы из учебного проекта. Согласовать поля, роли и реакции на отказ, затем оформить проект инструкции проверки и краткий протокол интеграционного испытания.

3. План восстановления геосервиса

Определить зависимости восстановления учебного сервиса от конфигурации, геоданных и ключей. Подготовить краткий порядок проверки копии на отдельном стенде и сравнить полученное время с заданным целевым.

Раздел 7. Профессиональное развитие

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 7.1. Отраслевые сертификаты и развитие карьеры

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Область действия стандартов и подтверждений

Сопоставить документы, применимые к учебному геосервису: нормативные основания режима данных, технический стандарт обмена и требования проверки безопасности. Для каждого указать область применения, версию и пределы вывода о соответствии.

2. Подготовка профессионального результата проекта

Оформить учебный комплект для передачи проекта другому разработчику: описание версии, вклад участников, правила работы с данными и доступом, результаты проверок и оставшиеся ограничения. По комплекту определить один навык для дальнейшего освоения.

7. Оценочные материалы промежуточной аттестации

1 семестр, Экзамен

Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Вопросы/Задания:

1. Чем геометрия пространственного объекта отличается от его атрибутов?

2. Почему правовой режим данных нельзя определять только по названию файла?

3. Как связать угрозу геосервису с последствиями для его работы?

4. В чем опасность публикации подробной траектории с устойчивым идентификатором пользователя?

5. Зачем различать субъект, объект и операцию при описании доступа?

6. Почему требования защиты формулируют до завершения реализации?

7. Чем проверка формата параметра отличается от проверки его допустимости для задачи?

8. Что означает отделение данных от текста SQL-команды?

9. Почему в тестах нужны как разрешенные, так и запрещенные действия?

10. Что следует сохранить в записи об исправлении дефекта?

11. Почему межсетевой экран и WAF решают разные задачи?

12. Какие сведения помогают разобраться в ложном срабатывании WAF?

13. Как в модели оценки аномалий связано срабатывание правила с блокировкой?

14. Зачем документировать назначение сетевого разрешения?

15. Почему исключение правила WAF нужно проверять и на допустимых, и на вредоносных примерах?

16. Какие разные задачи решают шифрование и подпись?

17. Что проверяет сопоставление имени узла с сертификатом?

18. Почему правила доступа к ключам требуют отдельного описания?

19. Где заканчивается защита данных отдельным TLS-соединением?

20. Чем проверка цепочки доверия отличается от проверки имени сервера?

21. Почему назначение SRID и преобразование координат нельзя смешивать?

22. Чем выдача изображения карты отличается от выдачи пространственных объектов?

23. Почему для приложения следует проверять совокупные права роли?

24. Зачем проверять корректность геометрии после импорта?

25. Чем ограничение операции геосервера отличается от ограничения слоя?

26. Как сделать требование к геосервису проверяемым?

27. Какие сведения важно согласовать между участниками группового проекта?

28. Почему успешное резервное копирование не равно успешному восстановлению?

29. Для чего в протоколе испытания сохраняют условия выполнения?

30. Как показать связь выбранной меры защиты с исходной задачей?