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 ПРАКТИКЕ «Б2.В.02 ПРОЕКТНО-ТЕХНОЛОГИЧЕСКАЯ ПРАКТИКА»

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: 9 з.е.
в академических часах: 324 ак.ч.

Москва, 2025

Разработчики:
Доцент кафедры Информационно-измерительных систем, к.т.н.
Тележников В. Ю.

Фонд оценочных средств по практике 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. 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 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 Владеть: ПК-3.1/Нв1 Методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности 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 Владеть: ПК-3.2/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа

		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 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 Владеть: ПК-3.3/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации
		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 ПК-3.4/Зн3 Технологии проектирования и построения защищенных информационных систем 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/Зн2 Методы безопасности веб-приложения от критических угроз безопасности 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 ПК-3.1/Ум2 Выявлять и устранять потенциальные угрозы безопасности в веб-приложениях 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/Ум1 Определять объекты доступа, которые подлежат защите, на основании их функционального назначения и чувствительности информации 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 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

		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/Зн3 Технологии проектирования и построения защищенных информационных систем 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 ПК-3.1/Зн2 Методы безопасности веб-приложения от критических угроз безопасности
	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/Зн1 Нормативные и методические документые, регламентирующие классификацию субъектов и объектов доступа ПК-3.2/Зн3 Методы атаки и различные методы предотвращения атак 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

		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) ПК-3.4/Зн3 Технологии проектирования и построения защищенных информационных систем

2. 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/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/Нв1 Методами анализа и оценки информации на предмет ее соответствия критериям отнесения к различным видам тайны и степеням конфиденциальности 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/Нв1 Навыками работы с системами управления доступом и средствами контроля доступа

	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/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/Нв1 Навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в организации 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/Зн3 Технологии проектирования и построения защищенных информационных систем 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-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/Ум1 Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности ПК-3.1/Ум2 Выявлять и устранять потенциальные угрозы безопасности в веб-приложениях ПК-3.2 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-3.3 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/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-3.4 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/Зн3 Технологии проектирования и построения защищенных информационных систем ПК-3.4/Ум1 Анализировать и выбирать оптимальную топологию и архитектуру сети с учетом требований и условий эксплуатации
Удовлетворительно	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-3.2 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-3.3 Разрабатывает проекты нормативных документов, регламентирующих работу по защите информации ПК-3.3/Зн1 Регламенты работ по обеспечению информационной безопасности автоматизированных систем автоматизированных систем ПК-3.4 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/Зн3 Технологии проектирования и построения защищенных информационных систем
Неудовле-творительно	Результаты обучения не сформированы на достаточном уровне

3. Контрольные мероприятия по практике

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Устный опрос
Промежуточная аттестация	Зачет с оценкой

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

1	Организационно-методический этап - 24 час. Тема 1.1 Организационно-методический этап - 24 час.	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Устный опрос	Зачет с оценкой
2	Экспериментальные исследования (или практические разработки) - 290 час. Тема 2.1 Экспериментальные исследования (или практические разработки) - 290 час.	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Устный опрос	Зачет с оценкой
3	Заключительный этап - 10 час. Тема 3.1 Заключительный этап - 10 час.	ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4	Устный опрос	Зачет с оценкой

4. 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 с оценкой, 2 семестр.

Промежуточная аттестация по дисциплине проводится в форме «дифференцированный зачет». 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:

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и продемонстрировал системное и полное освоение содержания дисциплины; ответы правильные, обоснованные и терминологически точные;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, в случае, если основное содержание освоено, но допущены отдельные неточности, не влияющие на общее понимание материала;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если освоены базовые понятия и положения, но имеются существенные пробелы и

ошибки;
- не зачтено («не удовлетворительно») – 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:
Зачет оценивается по пятибалльной шкале:
- зачтено с оценкой «отлично» выставляется, если обучающийся набрал 86–100 баллов и дал полные, правильные и логически последовательные ответы; терминология применяется корректно, приведены необходимые обоснования и примеры, дополнительные вопросы раскрыты;
- зачтено с оценкой «хорошо» выставляется обучающемуся, набравшему 71–85 баллов, если вопросы раскрыты правильно и достаточно полно, а отдельные неточности исправлены после уточняющих вопросов;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся, набравшему 56–70 баллов, если основные положения раскрыты фрагментарно, имеются существенные неточности, однако базовое понимание продемонстрировано;
- не зачтено («не удовлетворительно») – если обучающийся набрал 0–55 баллов, вопросы не раскрыты либо допущены принципиальные ошибки, отсутствует владение базовой терминологией.

5. Оценочные материалы текущего контроля

Раздел 1. Организационно-методический этап
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 1.1. Организационно-методический этап
Форма контроля/оценочное средство: Устный опрос
Вопросы/Задания:
1. Виды и объемы работ, выполняемые за время прохождения практики?
2. Какие основные работы должны быть запланированы магистранту на практику?
3. Какие вопросы магистерской ВКР следует рассмотреть в рамках практики?
4. Кто проводит вводный инструктаж в МИИГАиК?
5. Как проводится литературный обзор и патентный поиск?
6. Как оценить достоверность полученной информации?
7. Как оценить стоимость полученной информации?
8. Какие разделы должны быть в общем плане работ по теме практики?
9. Как проводится детализация и уточнение плана работ?
10. Какие вопросы плана работ согласовываются с руководителем практики?
11. Зачем уточняются формулировки плана работ?
12. Кто утверждает план работ по практике?
13. Приведите классификацию основных форм деятельности персонала на данном производстве.

Раздел 2. Экспериментальные исследования (или практические разработки)
Контролируемые ИДК: ПК-3.1 ПК-3.2 ПК-3.3 ПК-3.4

Тема 2.1. Экспериментальные исследования (или практические разработки)
Форма контроля/оценочное средство: Устный опрос
Вопросы/Задания:
1. В чем заключается выбор оптимального метода и разработка программ экспериментальных исследований?

2. В чем заключается новизна и актуальность исследования, решаемые задачи и методы их решения?

3. Что лежит в основе обоснования выбора экспериментальных установок, требуемых физических измерений, выбора технических средств и оценки достоверности полученных результатов?

4. Как проводилась проработка выбранных решений по системотехническому проектированию систем информационной безопасности с использованием современных программных средств компьютерного моделирования?

5. Схемы производственного процесса.

6. Организация работы по охране труда в отрасли и в данной организации.

7. Какие профилактические мероприятия по обеспечению экологической безопасности, носящие рекомендательный характер, вы могли бы предложить к внедрению на предприятии?

8. Анализ негативных факторов и техногенного риска производства и технических систем предприятия.

9. Документы, регламентирующие соблюдение правил и норм охраны труда при работе на различном оборудовании предприятия.

10. Организация и проведение инструктажей по охране труда в организации.

11. Как организовано управление охраной труда на предприятии?

12. Задачи службы охраны труда на предприятии.

13. Меры по защите человека и среды обитания от негативных воздействий на предприятии.

14. Оценка риска реализации опасностей, выбор методов защиты от опасностей и способы обеспечения комфортных условий жизнедеятельности.

Раздел 3. Заключительный этап

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

Тема 3.1. Заключительный этап

Форма контроля/оценочное средство: Устный опрос

Вопросы/Задания:

1. Какие компетенции были освоены за время прохождения практики?

2. Каковы результаты прохождения практики?

3. Средства инструментального контроля различных параметров производственной среды.

4. Способы и технологии защиты в чрезвычайных ситуациях.

5. Порядок проведения инструктажей по охране труда на предприятии и их оформление.

6. Оценочные материалы промежуточной аттестации

2 семестр, Зачет с оценкой

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

Вопросы/Задания:

1. Какие сведения помогают сделать индивидуальное задание проверяемым?

2. Что делать, если для выбранной задачи не разрешен доступ к нужным данным?

3. Как связаны инструктаж и границы допустимых работ на практике?

4. Чем ожидаемый результат отличается от перечня используемых инструментов?

5. Как оформить существенную корректировку плана практики?

6. Почему режим защиты нельзя выбирать только по отметке «конфиденциально» на файле?

7. Что требуется для обоснования правил доступа в выбранной системе?

8. Как использовать TCP/IP и OSI при проектировании сетевого фрагмента?

9. Как подтвердить, что простая ошибка безопасности веб-компонента устранена?

10. Что делает проект регламента исполнимым и проверяемым?

11. Как показать в отчете связь между задачей и полученным результатом?

12. Какие материалы помогают подтвердить личный вклад в командный проект?

13. Почему вывод «решение безопасно» требует уточнения на защите?

14. Как подготовить приложения, если исходные материалы содержат закрытые сведения?

15. Как представить исправление, выполненное после замечания руководителя?