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.О.07 АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

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: 3 з.е.
в академических часах: 108 ак.ч.

Москва, 2025

Разработчики:
Преподаватель кафедры Информационно-измерительных систем
Долгова П. В.

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

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности

ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности

Знать:

ОПК-3.1/Зн2 Регламенты по аудиту информационной безопасности

Уметь:

ОПК-3.1/Ум2 Митигировать риски, выявленные в ходе аудита информационной безопасности

Владеть:

ОПК-3.1/Нв2 Навыками и инструментами для проведения аудита информационной безопасности

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Повышенный	ИДК ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности Знать: ОПК-3.1/Зн2 Регламенты по аудиту информационной безопасности Уметь: ОПК-3.1/Ум2 Митигировать риски, выявленные в ходе аудита информационной безопасности Владеть: ОПК-3.1/Нв2 Навыками и инструментами для проведения аудита информационной безопасности
	Базовый	ИДК ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности Знать: ОПК-3.1/Зн2 Регламенты по аудиту информационной безопасности Уметь: ОПК-3.1/Ум2 Митигировать риски, выявленные в ходе аудита информационной безопасности

	Пороговый	ИДК ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности Знать: ОПК-3.1/Зн2 Регламенты по аудиту информационной безопасности

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Отлично	ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности ОПК-3.1/Зн2 Регламенты по аудиту информационной безопасности ОПК-3.1/Ум2 Митигировать риски, выявленные в ходе аудита информационной безопасности ОПК-3.1/Нв2 Навыками и инструментами для проведения аудита информационной безопасности
Хорошо	ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности ОПК-3.1/Зн2 Регламенты по аудиту информационной безопасности ОПК-3.1/Ум2 Митигировать риски, выявленные в ходе аудита информационной безопасности
Удовлетворительно	ОПК-3.1 Разрабатывает проекты организационно-распорядительной документации, регламентирующей процесс обеспечения информационной безопасности ОПК-3.1/Зн2 Регламенты по аудиту информационной безопасности
Неудовле-творительно	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование Практическая работа
Промежуточная аттестация	Зачет с оценкой

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Аудит	ОПК-3.1	Тестирование Практическая работа	Зачет с оценкой
2	Аудит информационной безопасности	ОПК-3.1	Тестирование Практическая работа	Зачет с оценкой
3	Правовые аспекты аудита информационной безопасности	ОПК-3.1	Тестирование Практическая работа	Зачет с оценкой

4	Управление аудитом информационной безопасности	ОПК-3.1	Тестирование Практическая работа	Зачет с оценкой
5	Методика проведения аудита информационной безопасности на предприятии	ОПК-3.1	Тестирование Практическая работа	Зачет с оценкой
6	Планирование аудиторской проверки	ОПК-3.1	Тестирование Практическая работа	Зачет с оценкой
7	Анализ и управление рисками ИБ	ОПК-3.1	Тестирование Практическая работа	Зачет с оценкой

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

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

Промежуточная аттестация: Зачет 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.

6. Оценочные материалы текущего контроля

Раздел 1. Аудит
Контролируемые ИДК: ОПК-3.1

Тема 1.1. Аудит

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Укажите порядок получения обнаружения: сначала выбирают критерий, затем проверяют информацию и сравнивают ее с критерием.

А. Получить и проверить информацию
Б. Выбрать критерий
В. Записать обнаружение
Г. Сравнить с критерием

2. В учебной подготовке сначала определяют цель, затем границы, после этого критерии проверки. Укажите порядок.

А. Выбрать критерии
Б. Установить область
В. Определить цель

3. Как называется документ, описывающий действия и мероприятия конкретного аудита?

4. Аудитор скрывает факт, который противоречит его выводу. Соблюдается ли объективность?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Критерии и свидетельства аудита

По описанию учебной системы выбрать три установленных требования и для каждого указать, какую информацию нужно получить для проверки. Разделить требования, факты и предварительные предположения.

2. Беспристрастность и конфиденциальность

Разобрать ситуации проверки собственной работы, давления на вывод и передачи отчета постороннему получателю. Подготовить короткие положения о независимости и обращении с материалами для учебного регламента аудита.

Раздел 2. Аудит информационной безопасности
Контролируемые ИДК: ОПК-3.1

Тема 2.1. Аудит информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В данном аудите сначала подтверждают возможность проведения, затем готовят план, выполняют работы и составляют отчет.

А. Составить отчет
Б. Провести работы
В. Подтвердить возможность
Г. Подготовить план

2. Для проверки прав сначала получают правило доступа, затем изучают конфигурацию, выполняют согласованное обращение и сравнивают результат.

А. Сравнить результат с правилом
Б. Получить правило
В. Выполнить обращение
Г. Изучить конфигурацию

3. Как называется метод получения сведений путем беседы с ответственным сотрудником?

4. В каком документе представляют результаты проведенного аудита?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка фактических прав

Сопоставить матрицу ролей учебной базы с предоставленной конфигурацией и результатами контрольных обращений. При наличии стенда выполнить согласованные операции чтения и изменения под тестовыми ролями, описать обнаруженные расхождения.

2. Анализ событий доступа

По небольшому учебному журналу выбрать события заданного периода и проверить наличие субъекта, объекта, действия и результата. Сопоставить их с условиями проверки, отметить, какие выводы можно подтвердить и каких сведений не хватает.

Тема 2.2. Виды аудитов ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Чтобы определить сторону аудита, сначала выясните, кто заказал проверку и от чьего имени она идет, затем установите отношения сторон и классифицируйте аудит.

А. Установить отношения сторон
Б. Определить вид аудита
В. Выяснить заказчика и представляемую сторону

2. В учебном сравнении методов сначала выбирают цель проверки, затем нужное свидетельство, после этого способ его получения.

А. Определить нужное свидетельство
Б. Выбрать метод получения
В. Выбрать цель

3. Какой стороной называют внутренний аудит организации?

4. Заказчик проверяет своего поставщика. Какая это сторона аудита?

Раздел 3. Правовые аспекты аудита информационной безопасности

Контролируемые ИДК: ОПК-3.1

Тема 3.1. Правовые аспекты аудита информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. До технической проверки сначала определяют объект и действия, затем подтверждают полномочия и условия, после этого приступают к согласованной работе.

А. Определить объект и действия

Б. Начать согласованную работу

В. Подтвердить полномочия и условия

2. Для выбора правового критерия сначала устанавливают вид объекта и деятельности, затем находят применимый документ, проверяют редакцию и указывают нужное положение.

А. Найти применимый документ

Б. Проверить редакцию

В. Указать положение

Г. Установить вид объекта

3. Нужно ли подтвердить полномочия на проведение согласованных аудиторских действий до их выполнения?

4. Какой принцип требует надлежащего обращения с закрытыми сведениями, полученными в аудите?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Проверка применимости требований

Для вымышленной организации с заданным видом деятельности составить перечень правовых, договорных и внутренних критериев. По предоставленным документам проверить применимость, редакцию и конкретное положение, не назначая требования только по названию.

2. Согласование полномочий и периметра

Подготовить проект задания на аудит портала: перечислить системы и процессы, допустимые действия, исключения, сроки, контакты и условия остановки. Разобрать запрос на включение внешнего сервиса вне первоначальных границ.

Раздел 4. Управление аудитом информационной безопасности

Контролируемые ИДК: ОПК-3.1

Тема 4.1. Управление аудитом информационной безопасности

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В учебной программе сначала задают цели, затем планируют проверки и ресурсы, выполняют программу и анализируют ее результаты.

А. Проанализировать результаты

Б. Выполнить программу

В. Задать цели

Г. Определить проверки и ресурсы

2. При подборе группы сначала определяют требуемые знания, затем оценивают кандидатов и распределяют участки проверки.

А. Распределить участки

Б. Оценить кандидатов

В. Определить компетенции

3. Как называется набор мероприятий по одному или нескольким аудитам на определенный период ради общей цели?

4. Как называется участник, предоставляющий группе специальные знания, но не получающий автоматически полномочия аудитора?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Программа аудита на учебный период

По описанию трех процессов и их рисков подготовить программу проверок: цели,

приоритеты, охват, сроки, ресурсы и ответственные. Объяснить периодичность через заданные условия и применимые требования.

2. Компетентность и распределение ролей

Сопоставить задачи проверки с навыками условных участников. Выделить пробелы, определить потребность в техническом эксперте и распределить обязанности, учитывая возможный конфликт интересов.

Раздел 5. Методика проведения аудита информационной безопасности на предприятии

Контролируемые ИДК: ОПК-3.1

Тема 5.1. Методика проведения аудита информационной безопасности на предприятии

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Сначала собирают информацию, затем проверяют ее надежность, сопоставляют с требованием и формулируют обнаружение.

А. Сформулировать обнаружение
Б. Проверить надежность
В. Собрать информацию
Г. Сопоставить с требованием

2. Для устранения выявленного нарушения сначала определяют причину, затем выбирают действие, выполняют его и проверяют результативность.

А. Проверить результативность
Б. Определить причину
В. Выбрать действие
Г. Выполнить действие

3. Как называется изучаемая часть совокупности записей при выборочной проверке?

4. Требование выполнено в проверенном случае. Как назвать результат сравнения?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Интервью по выдаче доступа

Подготовить вопросы по заданному порядку предоставления доступа, провести учебное интервью и указать документы или записи, которыми можно подтвердить ответы. Зафиксировать противоречия и дальнейшие действия аудитора.

2. Выборка заявок на доступ

Из предоставленной совокупности учебных заявок выбрать записи по заранее описанному способу. Проверить наличие согласования и сроков, подсчитать охват и сформулировать вывод только в допустимых границах.

Раздел 6. Планирование аудиторской проверки

Контролируемые ИДК: ОПК-3.1

Тема 6.1. Планирование аудиторской проверки

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. В данном планировании сначала задают процессы и критерии, затем методы, после этого ресурсы и график.

А. Назначить ресурсы
Б. Выбрать методы
В. Согласовать график
Г. Указать процессы и критерии

2. Для интервью сначала выбирают вопросы по критерию, затем согласуют участника и время, проводят беседу и проверяют полученные сведения.

А. Согласовать участника и время
Б. Проверить сведения
В. Подготовить вопросы
Г. Провести интервью

3. Нужно ли указывать проверяемый период в границах аудита, если вывод относится к событиям за определенное время?

4. Должна ли совокупная компетентность группы покрывать поставленные цели проверки?

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. План конкретной проверки

Разработать план аудита одного учебного процесса: цель, область, критерии, методы, выборка, участники и график. Проверить доступность нужных документов, людей и стенда.

2. Корректировка графика и области

Внести в план три изменения: перенос интервью, недоступность журнала и запрос на дополнительный компонент. Оценить влияние на цели, согласовать решение и показать обновленные границы выводов.

Раздел 7. Анализ и управление рисками ИБ

Контролируемые ИДК: ОПК-3.1

Тема 7.1. Анализ и управление рисками ИБ

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Для рассматриваемого риска сначала описывают сценарий, затем оценивают вероятность и последствия, после этого выбирают меру.

А. Оценить вероятность и последствия
Б. Описать сценарий
В. Выбрать меру

2. Сначала выполняют меру обработки, затем оценивают остаточный риск и оформляют решение уполномоченного лица.

А. Оценить остаточный риск
Б. Оформить решение
В. Выполнить меру

Форма контроля/оценочное средство: Практическая работа

Вопросы/Задания:

1. Реестр рисков по обнаружениям

По результатам учебного аудита описать три риска: актив, сценарий, предпосылки, последствия и существующие меры. Оценить приоритеты по явно заданной простой шкале и объяснить допущения.

2. План снижения рисков

Для двух приоритетных рисков выбрать подходящие меры, определить ответственных, сроки и критерии результата. Сравнить хотя бы два варианта по ожидаемому влиянию и ограничениям.

7. Оценочные материалы промежуточной аттестации

2 семестр, Зачет с оценкой

Контролируемые ИДК: ОПК-3.1

Вопросы/Задания:

1. Что отличает критерий аудита от свидетельства?

2. Что определяет область аудита?

3. Какие методы получения информации можно сочетать в аудите ИБ?

4. Что сравнивают при проверке прав доступа?

5. Что делает запись журнала полезным свидетельством?

6. Чем аудит третьей стороны отличается от проверки поставщика заказчиком?

7. Зачем сочетать документальную и техническую проверку?

8. Почему слова «внешний» и «технический» описывают разные признаки аудита?

9. Почему техническая доступность объекта не равна полномочию проверять его?

10. Как поступить при необходимости расширить периметр?

11. На чем основывают периодичность проверок?

12. Что делать при нехватке исходных документов?

13. Какие три элемента нужны для обоснования несоответствия?

14. Что указывают при описании выборки?

15. Какие сведения включает план аудита?

16. Почему нужно учитывать проверяемый период?

17. Как учитывать недостаток специальных знаний у группы?

18. Чем снижение риска отличается от его предотвращения?

19. Почему перенос части риска не означает исчезновения всех рисков?

20. Что такое остаточный риск?

21. Когда пересматривают оценку риска?

22. Что описывают при выявлении риска ИБ?

23. Как отражать изменение согласованного плана?

24. Для чего согласуют условия остановки технической проверки?

25. Что подтверждает результативность последующих действий?

26. Чем исправление случая отличается от работы с причиной?

27. Как поступать с противоречащими свидетельствами?

28. Что дает мониторинг программы аудита?

29. Обязательны ли одинаковые навыки у каждого члена группы?

30. Как инциденты влияют на программу аудита?