



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: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

Уровень высшего образования: бакалавриат

Направление подготовки: 10.03.01 Информационная безопасность

Направленность(профиль) подготовки: Организация и технология защиты информации

Квалификация (степень) выпускника: бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 4 года

Объем:
в зачетных единицах: 9 з.е.
в академических часах: 324 ак.ч.

Москва, 2024

Разработчики:

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

Программа государственной итоговой аттестации составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Минобрнауки от 17.11.2020 № 1427

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	14.12.2023, № 7-23

1. Цель, формы и объем государственной итоговой аттестации

Государственная итоговая аттестация проводится в целях определения соответствия результатов освоения обучающимися основной образовательной программы соответствующим требованиям федерального государственного образовательного стандарта по образовательной программе высшего образования: направление подготовки 10.03.01 Информационная безопасность, профиль подготовки Организация и технология защиты информации.

К государственной итоговой аттестации допускаются обучающиеся, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план по образовательной программе высшего образования: направление подготовки 10.03.01 Информационная безопасность, профиль подготовки Организация и технология защиты информации.

Государственная итоговая аттестация обучающихся проводится в форме: защиты выпускной квалификационной работы.

Объем государственной итоговой аттестации составляет 324 академических часов (9 зачетных единиц). Подготовка к защите и защита выпускной квалификационной работы осуществляется в течение 6 недель.

2. Структура и содержание государственной итоговой аттестации

2.1. Вид выпускной квалификационной работы

Вид выпускной квалификационной работы: Дипломная работа

2.2. Перечень тем выпускных квалификационных работ, предлагаемых обучающимся

1. Разработка модели оценки защищенности протоколов маршрутизации от атак типа "отказ в обслуживании"
2. Сравнительный анализ стойкости механизмов аутентификации в протоколах беспроводной связи
3. Анализ возможностей перехвата трафика в сетях стандарта LTE и методы противодействия
4. Исследование методов выявления аномалий в поведении пользователей при работе с базами данных
5. Разработка методики количественной оценки уровня критичности уязвимостей с учетом специфики информационной системы
6. Сравнительный анализ моделей нарушителя для государственных информационных систем и коммерческих структур
7. Сравнительный анализ правовых режимов защиты коммерческой тайны и служебной информации ограниченного распространения
8. Анализ правоприменительной практики по статье 274 Уголовного кодекса в части нарушения правил эксплуатации средств хранения информации
9. Сравнительный анализ эффективности виброакустических генераторов шума различных типов
10. Разработка методики инструментального контроля защищенности выделенных помещений от перехвата акустической информации по виброакустическому каналу
11. Разработка метода оценки защищенности волоконно-оптических линий связи от несанкционированного съема информации
12. Анализ современных технических средств разведки и методов противодействия им
13. Сравнительный анализ протоколов выработки общего ключа при построении защищенных каналов связи
14. Разработка модели угроз для инфраструктуры открытых ключей с распределенным реестром
15. Сравнительный анализ эффективности антивирусных программ разных классов на основе тестирования в контрольной среде

16. Исследование методов обхода средств защиты от эксплуатации уязвимостей класса "переполнение буфера"
17. Разработка метода анализа защищенности доверенной загрузки операционных систем
18. Исследование методов противодействия руткитам на уровне ядра операционной системы
19. Разработка метода тестирования аппаратных межсетевых экранов на максимальную пропускную способность при включенных правилах фильтрации
20. Разработка методики расчета совокупной стоимости владения системой защиты информации с учетом косвенных затрат
21. Разработка модели ключевых показателей эффективности работы подразделения информационной безопасности
22. Анализ методов управления рисками, связанными с действиями привилегированных пользователей
23. Разработка процедуры управления уязвимостями в распределенной корпоративной сети
24. Сравнительный подход к категорированию объектов критической информационной инфраструктуры
25. Разработка модели угроз для объекта информатизации с использованием методологии моделирования процессов
26. Анализ совместимости средств криптографической защиты информации различных производителей
27. Исследование проблем интеграции систем контроля доступа и систем обнаружения вторжений
28. Разработка методики выбора оптимального состава средств защиты для типового объекта информатизации
29. Анализ влияния средств защиты информации на производительность и отказоустойчивость информационных систем
30. Сравнительный анализ архитектур построения защищенных сетей передачи данных для распределенных объектов
31. Построение математической модели оценки надежности системы защиты с резервированием компонентов
32. Моделирование процесса обнаружения вторжений с использованием аппарата нечеткой логики
33. Разработка модели оценки времени восстановления системы защиты после кибератаки
34. Исследование марковских процессов для описания смены состояний защищенности информационной системы
35. Разработка модели прогнозирования появления новых уязвимостей в программном обеспечении
36. Сравнительный анализ требований ФСТЭК к средствам защиты информации различных классов
37. Анализ эволюции требований к защите персональных данных в нормативных документах за последние десять лет
38. Сравнительный подход к классификации угроз в методиках Банка России и ФСТЭК
39. Исследование проблем применения стандартов по безопасности разработки программного обеспечения в малых командах
40. Разработка регламента взаимодействия службы безопасности и IT-подразделения при реагировании на инциденты
41. Сравнительный анализ организационных структур подразделений информационной безопасности на крупных предприятиях
42. Исследование методов мотивации сотрудников к соблюдению требований информационной безопасности
43. Разработка программы тренингов по информационной безопасности для разных категорий персонала

44. Анализ эффективности применения штрафных санкций и поощрений как методов управления поведением пользователей
45. Разработка порядка действий при смене ключевых сотрудников службы информационной безопасности
46. Анализ типовых нарушений, выявляемых в ходе аудита систем электронного документооборота
47. Исследование методов выявления скрытых каналов передачи данных в процессе аудита
48. Сравнительный анализ инструментальных средств для проведения аудита защищенности веб-приложений
49. Сравнительный анализ точности срабатывания систем контроля утечки данных на основе лингвистических и статистических методов
50. Исследование методов обхода систем класса DLP и разработка рекомендаций по противодействию

3. Перечень рекомендуемой основной и дополнительной литературы

Основная литература

1. Информационная безопасность: учебное пособие: учебное пособие / И. Б. Тесленко, Д. В. Виноградов, А. М. Губернаторов [и др.]; под редакцией И. Б. Тесленко. - Информационная безопасность - Владимир: Издательство Владимирского государственного университета, 2023. - 212 с. - 978-5-9984-1783-2. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/143816.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Горюхина Е. Ю. Информационная безопасность: учебное пособие: учебное пособие / Е. Ю. Горюхина, Л. И. Литвинова, Н. В. Ткачева. - Информационная безопасность - Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого, 2015. - 221 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/72672.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
3. Куликов С. С. Информационная безопасность глобальных компьютерных сетей: практикум: практикум / С. С. Куликов. - Информационная безопасность глобальных компьютерных сетей - Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2021. - 66 с. - 978-5-7731-0970-9. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/118613.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

Дополнительная литература

1. Горев А. И. Обработка и защита информации в компьютерных системах: учебно-практическое пособие: учебно-практическое пособие / А. И. Горев, А. А. Симаков. - Обработка и защита информации в компьютерных системах - Омск: Омская академия МВД России, 2016. - 88 с. - 978-5-88651-642-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/72856.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке
2. Газизов А. Р. Техническая защита информации: учебное пособие: учебное пособие / А. Р. Газизов, Д. В. Фатхи. - Техническая защита информации - Ростов-на-Дону: Донской государственный технический университет, 2022. - 108 с. - 978-5-7890-2053-1. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/130429.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

3. Дмитриев В. Т. Защита информации в инфокоммуникационных системах. Ч.1: учебное пособие: учебное пособие / В. Т. Дмитриев. - Защита информации в инфокоммуникационных системах. Ч.1 - Рязань: Рязанский государственный радиотехнический университет, 2023. - 160 с. - 978-5-7722-0370-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/134852.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Дмитриев В. Т. Защита информации в инфокоммуникационных системах. Ч.2: учебное пособие: учебное пособие / В. Т. Дмитриев. - Защита информации в инфокоммуникационных системах. Ч.2 - Рязань: Рязанский государственный радиотехнический университет, 2023. - 148 с. - 978-5-7722-0371-2. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/137319.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

5. Целых А. Н. Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения: учебное пособие: учебное пособие / А. Н. Целых, Э. М. Котов. - Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения - Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2023. - 116 с. - 978-5-9275-4515-5. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/138009.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

6. Ванина А. Г. Гуманитарные проблемы обеспечения информационной безопасности: учебное пособие (курс лекций): учебное пособие (курс лекций) / А. Г. Ванина, Т. В. Минкина. - Гуманитарные проблемы обеспечения информационной безопасности - Ставрополь: Северо-Кавказский федеральный университет, 2021. - 139 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/135681.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

7. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум: лабораторный практикум / М. А. Лапина, Д. М. Марков, Т. А. Гиш, М. В. Песков, В. В. Меденец. - Комплексное обеспечение информационной безопасности автоматизированных систем - Ставрополь: Северо-Кавказский федеральный университет, 2016. - 242 с. - 2227-8397. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/62945.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

8. Жидко Е. А. Методология исследований информационной безопасности экологически опасных и экономически важных объектов: монография: монография / Е. А. Жидко. - Методология исследований информационной безопасности экологически опасных и экономически важных объектов - Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСБ, 2015. - 183 с. - 978-5-89040-535-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/55011.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

9. Киренберг А. Г. Защита информации от утечки по техническим каналам: учебное пособие: учебное пособие / А. Г. Киренберг, В. О. Коротин. - Защита информации от утечки по техническим каналам - Кемерово: Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2023. - 221 с. - 978-5-00137-407-7. - Текст: электронный. // IPR SMART: [сайт]. - URL: <https://www.iprbookshop.ru/135100.html> (дата обращения: 16.03.2025). - Режим доступа: по подписке

4. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. <https://student2.consultant.ru/cgi/online.cgi> - Правовой Сервер КонсультантПлюс
2. <https://www.garant.ru/> - Информационно-правовой портал "Гарант"

1. <https://www.elibrary.ru/> - НЭБ eLIBRARY
2. <https://znanium.ru/> - Электронно-библиотечная система "Znanium"
3. <https://e.lanbook.com/> - Электронная библиотечная система "Лань"

5. Требования к выпускным квалификационным работам и порядок их выполнения

Выпускная квалификационная работа представляет собой выполненную обучающимся (несколькими обучающимися совместно) работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности. ВКР является самостоятельной завершённой работой обучающегося на заданную (выбранную) тему, свидетельствующей об умении обучающегося (нескольких обучающихся совместно) работать с литературой, обобщать и анализировать фактический материал, используя теоретические знания и практические навыки, полученные при освоении образовательной программы. ВКР выполняется лично обучающимся (несколькими обучающимися совместно) под руководством руководителя. ВКР может основываться на обобщении выполненных курсовых работ и содержать материалы, собранные в период производственной практики. Материал ВКР должен быть изложен лаконично, целостно, в логичной последовательности, с соблюдением правил русского языка. При использовании монографий, учебников, статей из журналов, иной литературы и материалов, содержащихся в информационно-телекоммуникационной сети «Интернет», (далее — литературные материалы) необходимо ссылаться на соответствующий источник и формировать библиографический список (список литературы), указывая все использованные источники. Дословное или близкое к тексту воспроизведение литературного материала без указания ссылки на источник квалифицируется как недобросовестное заимствование (плагиат). ВКР, ставящая под сомнение самостоятельность выполнения целиком или одного из ее основных разделов, считается не выполненной.

Оформление ВКР должно соответствовать требованиям, изложенным в соответствующих разделах: "Порядок подготовки и защиты выпускной квалификационной работы по основным профессиональным образовательным программам высшего образования в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии»

6. Критерии оценки защиты выпускных квалификационных работ

К критериям оценки, выставляемой обучающемуся за ВКР, относятся:

- качество ВКР, представленной к защите;
- качество выполненного доклада;
- уровень ответов на вопросы, заданных членами ГЭК после заслушивания доклада, умение дискутировать.

Оценки	Критерии
Отлично	Выставляется обучающемуся, представившему ВКР, содержащую реальные выводы и предложения, вытекающие из проделанного анализа, соответствующую требованиям, а также продемонстрировавшему в ходе защиты ВКР свободное владение материалом, давшему аргументированные, полные и четкие ответы на вопросы членов ГЭК.

Хорошо	Выставляется обучающемуся, представившему ВКР, соответствующую требованиям настоящего Порядка, содержащую выводы и предложения, вытекающие из проделанного анализа, и продемонстрировавшему владение материалом ВКР, ответившему на вопросы, но имеющему отдельные мелкие недочеты по тем или иным аспектам ВКР.
Удовлетворительно	Выставляется обучающемуся, представившему ВКР, соответствующую установленным требованиям, содержащую общие выводы и предложения по совершенствованию предмета исследования, и продемонстрировавшему в процессе защиты слабое владение материалом ВКР, затруднения в ответах на вопросы членов ГЭК.
Неудовлетворительно	Выставляется в том случае, если представленная ВКР в основном соответствует требованиям, но обучающийся не владеет материалом, не ориентируется в теме, не может ответить на вопросы.

7. Описание материально-технической базы государственной итоговой аттестации

Смешанный тип

8 к.3

Автоматизированное рабочее место (АРМ) - 1 шт.

Доска настенная одноэлементная - 2 шт.

Интерактивная панель - 1 шт.

Проектор - 1 шт.

8. Порядок подачи и рассмотрения апелляций

По результатам государственных аттестационных испытаний обучающийся имеет право на апелляцию.

Обучающийся имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленной процедуры проведения государственного аттестационного испытания и (или) несогласии с результатами. Апелляция подается лично обучающимся в апелляционную комиссию не позднее следующего рабочего дня после объявления результатов государственного аттестационного испытания. Для рассмотрения апелляции секретарь ГЭК направляет в апелляционную комиссию протокол заседания ГЭК, заключение председателя ГЭК о соблюдении процедурных вопросов при проведении государственного аттестационного испытания, а также выпускную квалификационную работу, отзыв и рецензию (при наличии) (для рассмотрения апелляции по проведению защиты выпускной квалификационной работы).

Апелляция рассматривается не позднее 2 рабочих дней со дня ее подачи на заседании апелляционной комиссии, на которое приглашаются председатель государственной экзаменационной комиссии и обучающийся, подавший апелляцию. Заседание апелляционной комиссии может проводиться в отсутствие обучающегося, подавшего апелляцию, в случае его неявки на заседание апелляционной комиссии. Решение апелляционной комиссии доводится до сведения обучающегося, подавшего апелляцию, в течение 3 рабочих дней со дня заседания апелляционной комиссии. Факт ознакомления обучающегося, подавшего апелляцию, с решением апелляционной комиссии удостоверяется подписью обучающегося.

При рассмотрении апелляции о нарушении процедуры проведения государственного аттестационного испытания, апелляционная комиссия принимает одно из следующих решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях процедуры проведения государственного аттестационного испытания обучающегося не подтвердились и (или) не повлияли на результат государственного аттестационного испытания;
- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях

процедуры проведения государственного аттестационного испытания обучающегося подтвердились и повлияли на результат государственного аттестационного испытания.

Обучающемуся предоставляется возможность пройти государственное аттестационное испытание в сроки, установленные Университетом.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит. Повторное проведение государственного аттестационного испытания обучающегося, подавшего апелляцию, осуществляется в присутствии председателя или одного из членов апелляционной комиссии не позднее даты завершения обучения в соответствии со стандартом. Апелляция на повторное проведение государственного аттестационного испытания не принимается.