

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
федеральное государственное автономное образовательное учреждение высшего
образования
«Балтийский федеральный университет имени Иммануила Канта»
Образовательно-научный кластер «Институт высоких технологий»
Высшая школа компьютерных наук и искусственного интеллекта

**ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**
Период обучения по образовательной программе 2026-2032

Шифр: 10.05.01
Направление подготовки: Компьютерная безопасность
Направленность (профиль) образовательной программы:
«Математические методы защиты информации»

Квалификация выпускника: Специалист по защите информации

Калининград
2026

Программа государственной итоговой аттестации (ГИА) разработана в соответствии с СУОС, утвержденным приказом БФУ им. И.Канта от 21.01.2026 №36 «О введении в действие образовательных стандартов высшего образования» и учебным планом по направлению подготовки базового высшего образования 10.05.01 «Компьютерная безопасность» (направленность (профиль) образовательной программы «Математические методы защиты информации»).

Составители:

1. Шпилевой Андрей Алексеевич, к.ф.-м.н., доцент, заместитель руководителя Образовательно-научного кластера «Институт высоких технологий»
2. Верещагин Михаил Дмитриевич, директор Высшей школы компьютерных наук и искусственного интеллекта
3. Ветров Игорь Анатольевич, доцент Высшей школы компьютерных наук и искусственного интеллекта
4. Савкин Дмитрий Александрович, руководитель образовательной программы 10.05.01 «Компьютерная безопасность»

СОГЛАСОВАНО:

Рабочая программа утверждена на заседании
Ученого совета ОНК «Институт высоких технологий»

Председатель Ученого совета ОНК «Институт высоких технологий»

Профессор, д.ф.-м.н.

А.В. Юров

Руководитель ОПОП ВО

Д.А. Савкин

Цели и задачи государственной итоговой аттестации

Целью государственной итоговой аттестации является определение соответствия результатов освоения обучающимся основной профессиональной образовательной программы соответствующим требованиям самостоятельно установленного образовательного стандарта (СУОС) по направлению подготовки базового высшего образования 10.05.01 «Компьютерная безопасность» направленность (профиль) образовательной программы «Математические методы защиты информации». Государственная итоговая аттестация проводится государственными экзаменационными комиссиями (ГЭК).

К государственной итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный план по своей образовательной программе.

Задачами государственной итоговой аттестации являются:

- оценка способности самостоятельно решать на современном уровне задачи из области своей профессиональной деятельности, профессионально излагать специальную информацию, правильно аргументировать и защищать свою точку зрения;
- решение вопроса о присвоении выпускнику квалификации «Специалист по защите информации» по результатам ГИА и выдаче выпускнику документа (диплома) о высшем образовании;
- разработка рекомендаций по совершенствованию подготовки выпускников по данному направлению подготовки на основании результатов работы государственной экзаменационной комиссии.

2. Компетенции, выносимые на государственную итоговую аттестацию

В ходе ГИА обучающийся должен продемонстрировать сформированность следующих компетенций.

2.1. Универсальные компетенции (УК):

- Способен к формированию собственного жизненно образовательного маршрута на основе критического мышления, целеполагания, стратегии достижения цели (в том числе в проектной деятельности) в условиях создания безопасной среды, с учетом традиционных российских духовно-нравственных ценностей и целей национального развития, в процессе социального взаимодействия (УК-1);

2.2. Общепрофессиональные компетенции (ОПК):

- Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-1);
- Способен применять программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2);
- Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности (ОПК-3);
- Способен анализировать физическую сущность явлений и процессов, лежащих в основе функционирования микроэлектронной техники, применять основные физические законы и модели для решения задач профессиональной деятельности (ОПК-4);
- Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации (ОПК-5);

- Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6);
- Способен создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ (ОПК-7);
- Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей (ОПК-8);
- Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации (ОПК-9);
- Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности (ОПК-10);
- Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации (ОПК-11);
- Способен администрировать операционные системы и выполнять работы по восстановлению работоспособности прикладного и системного программного обеспечения (ОПК-12);
- Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности (ОПК-13);
- Способен проектировать базы данных, администрировать системы управления базами данных в соответствии с требованиями по защите информации (ОПК-14);
- Способен администрировать компьютерные сети и контролировать корректность их функционирования (ОПК-15);
- Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях (ОПК-16);
- Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма (ОПК-17).

Общепрофессиональные компетенции (ОПК), соответствующие специализации (специализация № 2 «Математические методы защиты информации»):

- Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации (ОПК-2.1.);
- Способен разрабатывать и анализировать математические модели механизмов защиты информации (ОПК-2.2.);
- Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов (ОПК-2.3.).

2.3. Профессиональные компетенции (ПК):

- Способен разрабатывать программно-аппаратные средства защиты информации

компьютерных систем и сетей (ПК-1);

- Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей (ПК-2);

- Способен организовывать и проводить работы по технической защите информации (ПК-3);

- Способность осуществлять подбор, изучение и обобщение научно-технической информации, методических материалов отечественного и зарубежного опыта по проблемам компьютерной безопасности, а также нормативных правовых актов сфере профессиональной (ПК-4);

- Способность участвовать в теоретических и экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах (ПК-5);

- Способность проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности (ПК-6);

- Способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем (ПК-7).

3. Объем, структура и содержание государственной итоговой аттестации

Государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы (ВКР).

Государственная итоговая аттестация включает:

- выполнение и защиту выпускной квалификационной работы.

3.1. Выпускная квалификационная работа

Выпускная квалификационная работа (ВКР) представляет собой работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

Требования к содержанию, объему и структуре ВКР, порядок выполнения и методические рекомендации по ее выполнению устанавливаются высшей школой.

Тексты ВКР проверяются на объём заимствования и размещаются на соответствующих ресурсах. Порядок проверки ВКР на объём заимствования, в том числе содержательного, выявления неправомерных заимствований и размещения текстов ВКР регламентируются локальными актами университета.

При защите ВКР выпускники должны, опираясь на полученные знания, умения и навыки, показать способность самостоятельно решать задачи профессиональной деятельности, излагать информацию, аргументировать и защищать свою точку зрения.

3.2.1. Перечень тем выпускных квалификационных работ

1. Исследование асимптотической сложности проблемы «Скрытой информации».
2. Оптимизация алгоритма Коча с использованием искусственной нейронной сети и выбор наиболее подходящего блока для встраивания цифрового водяного знака.
3. Построение комплексной системы информационной безопасности в учреждении здравоохранения.
4. Построение кодов, ассоциированных с торическими поверхностями.
5. Исследование условий применимости атаки Винера на криптосистему Ривеста – Шамира – Адлемана.
6. Реализация метода вычисления числа рациональных точек на кривых Артина – Шрайера над конечными полями.
7. Разработка комплекса лабораторных работ по применению средств защиты информации от несанкционированного доступа.

8. Организация централизованной аутентификации пользователей для распределённых систем.
9. Анализ, оптимизация и распараллеливание алгоритма декодирования Фенга – Рао на алгебраических кривых.
10. Анализ математических оснований криптосистемы с открытым ключом, основанной на группе Судзуки.
11. Разработка системы защищенного обмена для мобильных телефонов с использованием отечественной криптографии.
12. Разработка программной системы обнаружения вторжений с возможностью анализа трафика службы доменных имен.
13. Построение политики информационной безопасности для критически важного объекта на основе формальной модели управления доступом и информационными потоками.
14. Анализ безопасности цифровых подписей Ксинмея и Алабади – Викера.
15. Сравнительный анализ процедур декодирования на эрмитовой кривой и квартике Клейна.
16. Реализация алгоритма слепой подписи на базе стандарта цифровой подписи
17. Разработка, анализ стойкости и реализация основных алгоритмов шифрования СМС-сообщений на основе решёток в мобильной системе Windows Phone 8.
18. Обеспечение устойчивости цифровых водяных знаков, используемых для защиты авторских прав.
19. Обнаружение стеговложений в графических файлах.
20. Реализация алгоритма короткой цифровой подписи на основе спариваний Вейля.
21. Реализация криптосистемы с открытым ключом на основе идентификационных данных.
22. Сравнительный анализ стеганографических методов сокрытия информации в графических файлах.
23. Анализ эффективности алгоритма сложения в якобиане кривой Пикара и его реализация для криптографии.
24. Вычисление группы автоморфизмов некоторых кодов, ассоциированных с квартикой Клейна.
25. Реализация и анализ безопасности некоторых пороговых цифровых подписей.
26. Классификация экстремальных кодов с использованием их групп автоморфизмов.
27. Сравнительный анализ параметров однолинейных и двухлинейных кодов, ассоциированных с антиканоническими поверхностями.
28. Анализ безопасности схемы компактных электронных денег.
29. Вычисление дзета-функции башни Гарсии – Штихтенота.
30. Вычисление производящей функции графа, связанного с кривой Ван дер Хеера – Ван дер Флухта.
31. Особенности межсетевого экранирования и реализация персонального межсетевого экрана для протокола IPv6.
32. Защита от атак на протоколы шифрования беспроводных сетей.
33. Разработка схемы распределения ключей для облачных систем, допускающих перешифрование.
34. Анализ и реализация расширенного протокола Джоукса для многосторонней сверки ключей.
35. Анализ и реализация алгоритмов кодирования и декодирования NXL и XNL-кодов на основе алгоритма Судана.
36. Исследование свойств алгеброгеометрических кодов, ассоциированных с кривой Пикара
37. Исследование свойств первых ступеней башни функциональных полей Гарсии – Штихтенота и свойств соответствующих алгеброгеометрических кодов.

38. Моделирование угроз информационной безопасности критически важного объекта с использованием национального Банка угроз и уязвимостей.
39. Разработка и реализация политики безопасности для защиты виртуальной инфраструктуры
40. Разработка и исследование свойств протоколов почтового обмена внутри гибридного облака с двумя перешифровываниями на основе спаривания Хесса.
41. Приложение кодов Гоппы к криптосистемам Мак-Элиса и Нидеррайтера.
42. Разработка и анализ вычислительной эффективности основных криптографических алгоритмов на суперэллиптических кривых.
43. Разработка семейства протоколов на эллиптических кривых для децентрализованных приложений в индустрии азартных игр.
44. Анализ структуры и стойкости криптосистемы «Три медведя».
45. Анализ состояния защищенности информационной системы с помощью средств тестирования на проникновение.
46. Разработка и реализация специализированного комплекса для сбора и классификации информации на основе открытых источников (OSINT).
47. Исследование структуры якобиана гиперэллиптической кривой рода 3.
48. Оптимизация вычислений в группе точек эллиптической кривой.
49. Реализация и анализ BLS-схемы на эллиптических кривых.
50. Сведение дискретного логарифма на гиперэллиптических кривых рода 2 к конечному полю с помощью билинейных спариваний.
51. Гомоморфное выполнение нейронных сетей.
52. Построение модели защиты персональных данных пользователей в социальных сетях.
53. Анализ производительности типовых операций над точками эллиптической кривой при использовании различных систем координат.

3.2.2. Критерии оценивания выпускной квалификационной работы

Основными качественными показателями оценивания ВКР являются:

- актуальность и обоснование выбора темы ВКР;
- логика работы, соответствия содержания ВКР и её темы;
- степень самостоятельности;
- достоверность и обоснованность выводов;
- качество оформления ВКР, четкость и грамотность изложения материала;
- качество доклада, наглядных материалов (презентации), умение вести полемику по теоретическим и практическим вопросам, глубина и правильность ответов на вопросы членов ГЭК и замечания рецензентов;
- список использованных источников, достаточность использования отечественной и зарубежной литературы;
- возможность внедрения.

Оценка **«отлично»** выставляется при максимальной оценке всех вышеизложенных параметров.

Оценка **«хорошо»** выставляется за погрешности в каком-либо параметре.

Оценка **«удовлетворительно»** выставляется за серьезные недостатки в одном или нескольких критериях оценки.

Оценка **«неудовлетворительно»** за полное несоответствие ВКР вышеизложенным требованиям.

Результаты защиты ВКР определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешную защиту ВКР.

4. Перечень основной и дополнительной учебной литературы, необходимой для прохождения государственной итоговой аттестации

Основная литература

1.Шкляр, М. Ф. Основы научных исследований : учебное пособие для бакалавров / М. Ф. Шкляр. - 7-е изд. — Москва: Издательско-торговая корпорация «Дашков и К°», 2019. - 208 с. - ISBN 978-5-394-03375-9. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1093533> (дата обращения: 20.01.2026). – Режим доступа: по подписке.

Дополнительная литература

1.Кузнецов, И. Н. Основы научных исследований : учебное пособие для бакалавров / И. Н. Кузнецов. - 5-е изд., пересмотр. - Москва: Издательско-торговая корпорация «Дашков и К°», 2020. - 282 с. - ISBN 978-5-394-03684-2. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1093235> (дата обращения: 20.01.2026). – Режим доступа: по подписке.

2.Лазарова, Л. Б. Выпускная квалификационная работа: бакалавриат : учебное пособие / Л. Б. Лазарова, Ф. А. Каирова. — Москва: ИНФРА-М, 2019. — 228 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-014585-3. - Текст: электронный. - URL: <https://znanium.com/catalog/product/991919> (дата обращения: 20.01.2026). – Режим доступа: по подписке.

5. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для прохождения государственной итоговой аттестации

- НЭБ Национальная электронная библиотека, диссертации и прочие издания;
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций;
- ЭБС ZNANIUM.COM;
- ЭБС Лань;
- Электронно-библиотечная система (ЭБС) Кантитана (<https://elib.kantiana.ru/>)

Информационное и ресурсное обеспечение процедур ГИА в случае его проведения с использованием средств электронного обучения и дистанционных образовательных технологий производится в электронной информационно-образовательной среде университета.

6. Программное обеспечение государственной итоговой аттестации

Программное обеспечение обучения включает в себя:

- система электронного образовательного контента БФУ им. И. Канта, обеспечивающая разработку и комплексное использование электронных образовательных ресурсов;
- серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
- установленное на рабочих местах студентов соответствующее ПО и антивирусное программное обеспечение.

7. Материально-техническое обеспечение государственной итоговой аттестации

Материально-техническая база БФУ им. И. Канта обеспечивает подготовку и проведение всех форм государственной итоговой аттестации, практической и научно-исследовательской работы обучающихся, предусмотренных основной образовательной программой и соответствует действующим санитарным и противопожарным правилам и

нормам.

Минимально-необходимый перечень для информационно-технического и материально-технического обеспечения дисциплины:

- аудитория для проведения консультаций, оснащенная рабочими местами для обучающихся и преподавателя, доской, мультимедийным оборудованием;
- библиотека с читальным залом и залом для самостоятельной работы обучающегося, оснащенная компьютером с выходом в Интернет, книжный фонд которой составляет специализированная научная, учебная и методическая литература, журналы (в печатном или электронном виде);
- компьютерный класс, оснащенный компьютерами с выходом в Интернет, лицензионным программным обеспечением.