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 киберфизических систем

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Период обучения по образовательной программе 2026-2031

Направление подготовки базового высшего образования
10.03.01 Информационная безопасность

Профиль
«Организация и технологии защиты информации»

Квалификация выпускника: инженер по информационной безопасности

Форма обучения очная

Калининград 2026

Программа государственной итоговой аттестации (ГИА) разработана в соответствии с СУОС ВО, утвержденным Ученым советом БФУ им. И. Канта от 25.12.2025 г. № 68 и учебным планом по направлению подготовки 10.03.01 Информационная безопасность (направленность (профиль) образовательной программы «Организация и технологии защиты информации»).

Разработчик(и):

Бурмистров Валерий Иванович, руководитель образовательных программ высшей школы киберфизических систем образовательно-научного кластера «Институт высоких технологий»

Ветров Игорь Анатольевич, к. т. н., доцент высшей школы киберфизических систем образовательно-научного кластера «Институт высоких технологий»

Шпилевой Андрей Алексеевич, заместитель руководителя образовательно-научного кластера «Институт высоких технологий», к. ф.-м. н., доцент высшей школы киберфизических систем образовательно-научного кластера «Институт высоких технологий»

СОГЛАСОВАНО:

Программа государственной итоговой аттестации рассмотрена и утверждена на заседании ученого совета образовательно-научного кластера «Институт высоких технологий»

Протокол № 01 от «16» января 2026 г.

Председатель ученого совета ОНК «Институт высоких технологий»
Руководитель ОНК «Институт высоких технологий», д. ф.-м. н., профессор — Юров А. В.

1. Цели и задачи государственной итоговой аттестации

Целью государственной итоговой аттестации является определение соответствия результатов освоения обучающимся основной профессиональной образовательной программы соответствующим требованиям самостоятельно устанавливаемого образовательного стандарта базового высшего образования по направлению подготовки 10.03.01 Информационная безопасность, Направленность (профиль) образовательной программы «Организация и технологии 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 «Инженер по информационной безопасности» 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 проектном типе 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 применять математические методы, физические законы и модели для

решения задач профессиональной деятельности (ОПК-1);

– способен применять информационные технологии, технологии поиска, обработки и анализа информации в профессиональной деятельности (ОПК-2);

– способен использовать языки, методы и инструментальные средства программирования, системы управления базами данных для решения задач профессиональной деятельности (ОПК-3);

– способен применять положения в области электроники и схемотехники, электротехники, оптоэлектроники для решения профессиональных задач (ОПК-4);

– способен осуществлять выбор аппаратных средств вычислительной техники для решения задач профессиональной деятельности (ОПК-5);

– способен самостоятельно проводить экспериментальные исследования и использовать основные приемы обработки и представления полученных данных (ОПК-6);

– способен разрабатывать и использовать техническую, нормативную и правовую документацию, характерную для области профессиональной деятельности (ОПК-7);

– способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства (ОПК-8);

– способен применять программные, программно-аппаратные и технические средства защиты информации на объектах информатизации (ОПК-9);

– способен проводить функциональный анализ процесса объекта защиты, разрабатывать, организовывать и управлять мероприятиями по обеспечению информационной безопасности в организации (ОПК-10).

2.3. Профессиональные компетенции (ПК):

– способен к выполнению работ по установке, настройке, обеспечению бесперебойной работы и техническому обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации (ПК-1);

– способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

– способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-3);

– способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-4);

– способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-5);

– способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-6);

– способен организовывать работу и управлять персоналом, обслуживающим программные, программно-аппаратные (в том числе криптографические) и технические средства и системы защиты информации (ПК-7);

– способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-8);

– способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-9);

– способен проводить исследования на побочные электромагнитные излучения и наводки технических средств обработки информации, защищенности акустической речевой информации от утечки по техническим каналам (ПК-10).

3. Объем, структура и содержание государственной итоговой аттестации

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

Государственная итоговая аттестация включает*:*

–подготовку к процедуре защиты 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 ученым советом образовательно-научного кластера.

Тексты ВКР проверяются на объём заимствования и размещаются на соответствующих ресурсах. Порядок проверки ВКР на объём заимствования, в том числе содержательного, выявления неправомочных 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.

3.1.1. Перечень тем выпускных квалификационных работ

1. Построение виртуальной защищённой сети с учетом требований безопасного хранения ключевой информации в организации.
2. Разработка комплекса процедур аудита информационной безопасности Scada систем.
3. Разработка методики управления инцидентами и событиями информационной безопасности.
4. Модель защиты веб ресурсов на основе CMS.
5. Модернизация системы защиты информации на предприятии.
6. Автоматическая атака Wi-Fi «Twincy».
7. Исследование ПЭМИН от видеосредств при обработке конфиденциальной информации программно-аппаратным комплексом "Навигатор-П5М".
8. Разработка подсистемы фильтрации электронных почтовых сообщений от спама и вредоносного содержимого с использованием машинного обучения.
9. Защита информации при использовании электронной почты.
10. Разработка системы защиты информации для систем видеонаблюдения.
11. Организация системы контроля и управления доступом с применением биометрических персональных данных.
12. Разработка системы защиты обмена электронными почтовыми отправлениями.
13. Разработка системы информационной безопасности для лаборатории защиты информации.
14. Разработка системы обеспечения информационной безопасности корпоративной сети.
15. Разработка системы обеспечения информационной безопасности на примере предприятия.
16. Исследование распространения виброакустических колебаний в инженерных коммуникациях АПК «Смарт».
17. Разработка системы обеспечения информационной безопасности удалённого доступа к внутренним информационным ресурсам для коммерческой организации.
18. Разработка средства обнаружения сетевой разведки.
19. Совершенствование системы защиты информации в ООО «МечелБизнессервис».

20. Разработка спам-фильтра для сервера корпоративных сетей.

21. Разработка проекта системы защиты оконных проемов и решеток специальных помещений.

22. Инструментальный аудит удаленного автоматизированного рабочего места.

23. Разработка системы защиты конфиденциальной информации от несанкционированного разглашения.

24. Разработка системы защищенного документооборота в организации с обработкой персональных данных в автоматизированных системах.

25. Организация защиты персональных данных в организации.

26. Разработка проекта комплексной защиты информации (обеспечения ИБ) хлебзавод ООО"TURON-NON".

27. Методы защиты автоматизированной системы учета оплаты проезда в муниципальной системе пассажирских перевозок города Калининграда.

28. Разработка механизмов защиты диспетчерских компонентов сетей АСУ ТП.

29. Разработка проекта системы защиты периметра корпоративный сети коммерческой организации.

30. Разработка проекта системы защиты от утечки конфиденциальной информации регионального органа исполнительной власти.

31. Разработка программного обеспечения для выявления снифинга в локальных вычислительных сетях.

32. Разработка методики измерения экранирующих свойств альтернативных измерительных площадок программно-аппаратным комплексом «Навигатор 5».

33. Разработка систем обеспечения информационной безопасности промышленного предприятия.

34. Проектирование системы центра реагирования на инциденты информационной безопасности на примере образовательного учреждения.

35. Разработка проекта защиты конфиденциальной информации помещения ситуационного центра правительства Калининградской области.

36. Разработка программного обеспечения для повышения уровня защищенности конфиденциальной информации.

37. Оценка уровня информационной безопасности предприятия и пути совершенствования комплексной системы защиты от информационных угроз.

38. Модернизация аппаратного комплекса ситуационного центра правительства Калининградской области.

39. Разработка механизмов защиты сетей компьютерных классов общеобразовательной

школы.

40. Разработка методики измерения затухания альтернативных измерительных площадок программно-аппаратным комплексом «Навигатор 5».

41. Анализ событий безопасности в Linux

42. Разработка web-приложения для обучения работников организации вопросам информационной безопасности

43. Организация защиты информации в государственной информационной системе

44. Разработка программно-технического средства контроля и управления доступом в помещения с функцией уведомления о критических событиях

45. Разработка системы защиты информации на примере коммерческой организации

46. Определение клавиатурного почерка с использованием элементов искусственного интеллекта

47. Разработка концепции формирования и развития культуры ИБ граждан в Калининградской области

48. Использование математических методов для анализа событий безопасности

49. Организация защиты распределённой системы обращений граждан Калининградской области

50. Разработка подсистемы генерации и назначения надёжных паролей пользователей информационных ресурсов корпоративной сети

51. Разработка концепции и реализация мероприятий по обеспечению ИБ детей в Калининградской области

52. Организации защиты информации в образовательном учреждении Калининградской области

53. Организация проведений контрольных мероприятий в государственных информационных системах

54. Исследование и разработка сценариев фишинговых симуляций для образовательных организаций

55. Автоматизация процесса подбора рекомендаций для повышения защищенности информационных систем

56. Разработка программного решения для анализа событий безопасность с использованием сервисных нейросетей

57. Проведение мероприятий по локализации уязвимостей web-сайтов государственного учреждения

58. Разработка web-портала планирования и учета мероприятий по защите информации в организации

59. Организация мероприятий по устранению уязвимостей веб-сайта коммерческой организации

60. Разработка web-приложения для проведения соревнований по информационной безопасности

61. Анализ и разработка инструмента обфускации в целях защиты кода приложений

62. Разработка веб-приложения для обучения и тестирования работников организации по вопросам ИБ с элементами игрофикации.

63. Разработка механизма анализа событий безопасности в операционной системе Linux

64. Разработка программного средства автоматизации проведения аудита ИБ корпоративной сети

65. Разработка средства обнаружения сетевой разведки

66. Исследование и разработка архитектуры и механизмов обеспечения ИБ сервиса учета финансов пользователя

67. Разработка программного тренажера для имитационного моделирования работы программно-аппаратного комплекса по защите информации

68. Разработка программного средства поддержки принятия решений в ходе анализа защищённости корпоративной сети

69. Анализ безопасности веб-приложений: поиск и эксплуатация уязвимостей

70. Разработка виртуального помощника (ассистента, чат-бота) по вопросам информационной безопасности

71. Разработка электронного учебного пособия по изучению программно-аппаратных средств защиты информации

72. Разработка кроссплатформенного ПО для защищённого взаимодействия с экстренными службами

73. Разработка информационной системы защиты персональных данных для проектной организации

74. Разработка модели безопасности для промышленной организации

75. Проведение мероприятий по локализации уязвимостей web-сайтов государственного учреждения

76. Разработка веб-приложения для обучающей платформы по информационной безопасности

77. Разработка механизма анализа событий безопасности в операционной системе Linux.

78. Разработка программного средства автоматизации проведения аудита ИБ корпоративной сети

79. Разработка аппаратно-программного средства контроля и управления доступом в

помещения с функцией уведомления о критических событиях

80. Разработка системы защиты персональных данных в медицинской организации

81. Контроль событий безопасности средствами мониторинга информационной системы

82. Разработка программного средства для исследования веб-сайтов на возможность проведения атак «SQL-инъекция»

83. Разработка модели угроз и инцидентов для государственных информационных систем

84. Разработка механизмов защиты от атаки "копирование модели" на нейронную сеть

85. Разработка кроссплатформенного фреймворка оркестрации командных сценариев для автоматизации задач информационной безопасности

86. Исследование методов защиты беспроводных сетей от атак типа "злой двойник".

87. Создание системы обучения персонала для защиты от атак методом социальной инженерии

88. Разработка программного средства безопасного хранения файлов в многопользовательских системах

89. Исследование уязвимостей протокола Bluetooth и методов их предотвращения

90. Поиск аномалий в трафике сервисов интернета вещей по протоколу MQTT

91. Построение защищенной локальной сети в образовательном учреждении

92. Анализ уязвимостей SQL-инъекций в системе управления базами данных PostgreSQL, методы их обнаружения и предотвращения

93. Организация автоматизированного аудита безопасности облачной инфраструктуры Яндекс

94. Разработка системы контроля доступа для предприятий агропромышленного комплекса

3.1.2. Критерии оценивания выпускной квалификационной работы

Основными качественными показателями оценивания ВКР являются:

– соответствие тематики ВКР направлению подготовки;

– 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. Белов, Е. Б. Основы информационной безопасности: Учебное пособие для вузов / Е.Б. Белов и др. - Москва : Гор. линия-Телеком, 2011. - 558 с.: ил.; . - (Специальность; Учебное пособие для высших учебных заведений). ISBN 5-93517-292-5, 100 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/405159

2. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: https://znanium.com/catalog/product/997105.

3. Краковский, Ю. М. Защита информации: Учебное пособие (ФГОС) / Краковский Ю.М. - Ростов-на-Дону :Феникс, 2016. - 347 с.ISBN 978-5-222-26911-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/908844.

Дополнительная литература

1. Скакун В. В. Защита информации в базах данных и экспертных системах: учеб. пособие для вузов / В. В. Скакун ; Белорус. гос. ун-т им. В. И. Ленина. - Минск: Изд-во БГУ, 2015. - 134, [2] с. - Библиогр.: с. 133. - ISBN 978-985-566-194-9

2. Внуков А. А. Защита информации в банковских системах: учеб. пособие для

бакалавриата и магистратуры / А. А. Внуков; Высш. шк. экономики, Нац. исслед. ун-т. - 2-е изд., испр. и доп. - Москва : Юрайт, 2017. - 246 с. - (Бакалавр и магистр. Академический курс). - Библиогр.: с. 233. - ISBN 978-5-534-01679-6

3. Гришина Н. В. Информационная безопасность предприятия: учеб. пособие для вузов / Н. В. Гришина. - 2-е изд., доп. - Москва: ФОРУМ: Инфра-М, 2017. - 238 с.: ил. - (Высшее образование - бакалавриат). - Библиогр.: с. 200-204 (60 назв.). - ISBN 978-5-00091-007-8. - ISBN 978-5-16-010494-2

4. Информационная безопасность при управлении техническими системами : учеб. пособие для вузов / С. А. Баркалов [и др.]. - Санкт-Петербург: Интермедия, 2016. - 528 с.: ил. - Библиогр.: с. 513-516 (44 названия). - ISBN 978-5-4383-0133-2

5. Ерохин В. В. Безопасность информационных систем: учеб. пособие / В. В. Ерохин, Д. А. Погонышевва, И. Г. Степченко; М-во образования и науки РФ, ФГБОУ ВПО "Брянск. гос. ун-т" им. акад. И. Г. Петровского. - 3-е изд., стер. - Москва: Флинта: Наука, 2016. - 182, [1] с.: ил. - Библиогр. в конце кн. - ISBN 978-5-9765-1904-6. - ISBN 978-5-02-038563-4

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

- ЭБС Лань - Коллекция издательства «Лань» https://e.lanbook.com/
- ЭБС Консультант студента https://www.studmedlib.ru/cgi-bin/mb4
- ЭБС ZNANIUM https://znanium.com/catalog/document?id=333215
- НЭБ Национальная электронная библиотека https://rusneb.ru/
- ЭБС IBOOKS.RU https://ibooks.ru/
- eLIBRARY.RU Научная электронная библиотека, книги, статьи, тезисы докладов конференций https://www.elibrary.ru/defaultx.asp

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. обеспечивающую 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 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).