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 физических проблем и технологий

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Период обучения по образовательной программе 2023-2027

Направление подготовки бакалавриата
10.03.01 Информационная безопасность

Профиль направления подготовки бакалавриата
«Организация и технология защиты информации»

Форма обучения очная

Калининград 2023

Программа государственной итоговой аттестации (ГИА) разработана в соответствии с ФГОС ВО, утвержденным приказом Министерства образования и науки Российской Федерации от 17.11.2020 г. № 1427 и учебным планом по направлению подготовки бакалавриата 10.03.01 Информационная безопасность (профиль «Организация и технология защиты информации»).

Разработчик(и):

Бурмистров Валерий Иванович, руководитель основных образовательных программ ОНК «Институт высоких технологий»
Ветров Игорь Анатольевич, к. т. н., доцент ОНК «Институт высоких технологий»
Шпилевой Андрей Алексеевич, заместитель руководителя ОНК «Институт высоких технологий», к. ф.-м. н., доцент ОНК «Институт высоких технологий»

СОГЛАСОВАНО:

Программа государственной итоговой аттестации рассмотрена и утверждена на заседании ученого совета ОНК «Институт высоких технологий»

Протокол № 4 от «24» января 2023 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 федерального государственного образовательного стандарта (ФГОС ВО) по направлению подготовки бакалавриата 10.03.01 Информационная безопасность (профиль «Организация и технология 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 «Бакалавр» 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 осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач (УК-1);

– способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений (УК-2);

– способен осуществлять социальное взаимодействие и реализовывать свою роль в команде (УК-3);

– способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах) (УК-4);

– способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах (УК-5);

– способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни (УК-6);

– способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности (УК-7);

– способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов (УК-8);

– способен принимать обоснованные экономические решения в различных областях жизнедеятельности (УК-9);

– способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности (УК-10).

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 информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности (ОПК-2);

– способен использовать необходимые математические методы для решения задач профессиональной деятельности (ОПК-3);

– способен применять необходимые 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 в сфере профессиональной деятельности (ОПК-5);

– способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ОПК-6);

– способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности (ОПК-7);

– способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности (ОПК-8);

– способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности (ОПК-9);

– способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты (ОПК-10);

– способен проводить эксперименты по заданной методике и обработку их результатов (ОПК-11);

– способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений (ОПК-12);

– 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-13);

– способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников угроз, их возможных целей, путей реализации и предполагаемого ущерба (ОПК-2.1);

– способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы (ОПК-2.2);

– способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности (ОПК-2.3);

– способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами (ОПК-2.4).

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 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-6);

– способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-7);

– способен проводить исследования на побочные электромагнитные излучения и наводки технических средств обработки информации, защищенности акустической речевой информации от утечки по техническим каналам (ПК-8);

– способен принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-9);

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

Выпускная квалификационная работа выполняется в виде выпускной квалификационной работы бакалавра.

Требования к содержанию, объему и структуре ВКР, порядок выполнения и методические рекомендации по ее выполнению устанавливаются учебно-методическим советом института.

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

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 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
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 (дата обращения: 13.01.2022). – Режим доступа: по подписке.
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 (дата обращения: 13.01.2022). – Режим доступа: по подписке.

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 ПРОСПЕКТ http://ebs.prospekt.org/books
– 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 IBOOS.RU https://ibooks.ru/
– 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 – https://lms.kantiana.ru/ , обеспечивающую разработку и комплексное использование электронных образовательных ресурсов;
– серверное программное обеспечение, необходимое для функционирования сервера и связи с системой электронного обучения через Интернет;
– платформа для проведения онлайн вебинаров https://webinar.ru/ ;
– установленное на рабочих местах студентов ПО: Microsoft Windows 7, Microsoft Office Standart 2010, антивирусное программное обеспечение Kaspersky Endpoint Security.

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).