Федеральное агентство по рыболовству

Балтийская государственная академия рыбопромыслового флота федерального государственного бюджетного образовательного учреждения высшего образования «Калининградский государственный технический университет»

(БГАРФ ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
И.О. Декана РТФ
_____ /В.А. Баженов/
_27_. _июня_.2018 г.

ПРОГРАММА

государственной итоговой аттестации

выпускников по специальности

10 . 05 . 03 Информационная безопасность автоматизированных систем

(код и наименование)

Специализация

«Обеспечение информационной безопасности распределённых информационных систем»

Квалификация **специалист по защите информации**

Калининград 2018

Программа государственной итоговой аттестации: / Авт.-сост. Великите Н.Я., г. Калининград: БГАРФ ФГБОУ ВО «КГТУ», 2018.

Автор:
к.ф.-м.н., доцент кафедры ИБ _____ Н.Я.Великите

Программа государственной итоговой аттестации рассмотрена и одобрена на заседании кафедры «Информационная безопасность». Протокол № 9 от 14.06 2018г.

Заведующий кафедрой ИБ_____/Великите Н.Я./

Программа государственной итоговой аттестации рассмотрена и одобрена на заседании Совета РТФ. Протокол №6 от 27.06 2018г.

Председатель методической комиссии РТФ_____/Жестовский А.Г./

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью государственной итоговой аттестации (ГИА) является установление уровня подготовки выпускников к выполнению профессиональных задач и соответствия их подготовки требованиям Федерального государственного образовательного стандарта (ФГОС) высшего образования (ВО) (от 1.12.2016 №1509). И образовательной программы (ОП) высшего образования (ВО), разработанной в Балтийской государственной академии рыбопромыслового флота федерального государственного бюджетного образовательного учреждения высшего образования «Калининградский государственный технический университет» (БГАРФ ФГБОУ ВО «КГТУ»)

Программа ГИА составлена на основании:

-Порядок проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры, утверждённый приказом Минобрнауки России от 29 июня 2015 г. № 636.

-Положения о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры ФГБОУ ВО «Калининградский государственный технический университет» QD-8.1-(03.02), версия:V.3. (от 22.11.2017).

1.1. Государственная итоговая аттестация по специальности 10.05.03 «Информационная безопасность автоматизированных систем» включает:

-государственный экзамен в устной форме;

-защиту выпускной квалификационной работы в виде дипломной работы.

1.2. Видами профессиональной деятельности выпускника по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализации «Обеспечение информационной безопасности распределенных информационных систем» являются:

-научно-исследовательская;

-проектно-конструкторская;

-контрольно-аналитическая;

-организационно-управленческая;

-эксплуатационная.

1.3. Задачами профессиональной деятельности выпускника по специальности 10.05.03 «Информационная безопасность автоматизированных систем» являются:

научно-исследовательская деятельность:

- сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности автоматизированных систем;
- подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований;
- моделирование и исследование защищенных автоматизированных систем;
- анализ защищённости информации в автоматизированных системах и безопасности реализуемых информационных технологий;
- разработка эффективных решений по обеспечению информационной безопасности автоматизированных систем;

проектно-конструкторская деятельность:

- сбор и анализ исходных данных для проектирования систем защиты информации;
- разработка политик информационной безопасности автоматизированных систем;
- разработка защищенных автоматизированных систем в сфере профессиональной деятельности, обоснование выбора способов и средств защиты информационно-технологических ресурсов автоматизированных систем;
- выполнение проектов по созданию программ, комплексов программ, программно-аппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем;
- разработка системы управления информационной безопасностью автоматизированных систем;

контрольно-аналитическая:

- контроль работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
- выполнение экспериментально-исследовательских работ при сертификации средств защиты информации и аттестации автоматизированных систем;
- проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;

организационно-управленческая деятельность:

- организация работы коллектива, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ;
- организационно-методическое обеспечение обеспечения информационной безопасности автоматизированных систем;
- организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;
- контроль реализации политики информационной безопасности;

эксплуатационная деятельность:

- реализация информационных технологий в сфере профессиональной

деятельности с использованием защищенных автоматизированных систем;
- администрирование подсистем информационной безопасности автоматизированных систем;
- мониторинг информационной безопасности автоматизированных систем;
- управление информационной безопасностью автоматизированных систем;
- обеспечение восстановления работоспособности систем защиты информации при возникновении нештатных ситуаций.

Профессиональные задачи в соответствии со специализацией № 7 **«Обеспечение информационной безопасности распределенных информационных систем»:**

- разработка и исследование моделей информационно-технологических ресурсов, модели угроз и модели нарушителей информационной безопасности в распределенных информационных системах;
- удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
- аудит защищенности информационно-технологических ресурсов;
- координация деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации.

2. ТРЕБОВАНИЯ К ВЫПУСКНИКУ, ПРОВЕРЯЕМЫЕ В ХОДЕ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА,.

На государственный экзамен выносятся дисциплины, являющиеся базовыми для профессиональной подготовки будущих специалистов:

1. Организационное и правовое обеспечение информационной безопасности.
2. Безопасность операционных систем.
3. Техническая защита информации.
4. Криптографические методы защиты информации.
5. Методы проектирования защищённых распределённых информационных систем
6. Информационная безопасность распределённых информационных систем
7. Технология построения защищённых распределённых приложений
8. Теоретические основы компьютерной безопасности.
9. Программно-аппаратные средства обеспечения информационной безопасности.

10. Комплексное обеспечение информационной безопасности автоматизированных систем.

Банк вопросов по дисциплинам, выносимым на государственный экзамен состоит из перечня теоретических вопросов и типовых практических заданий (см. приложение к программе ФОС для ГИА)

2.1 В рамках проведения государственного экзамена проверяется степень освоения выпускником следующих компетенций:

ОК-1: способность использовать основы философских знаний для формирования мировоззренческой позиции;

ОК-2: способностью использовать основы экономических знаний в различных сферах деятельности;

ОК-3: способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма;

ОК-4: способность использовать основы правовых знаний в различных сферах деятельности;

ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;

ОК-6: способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;

ОК-7: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;

ОК-8: способность к самоорганизации и самообразованию;

ОК-9: способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности;

ОПК-1: способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач;

ОПК-2: способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники;

ОПК-3: способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности;

ОПК-4: способность понимать значение информации в развитии современного общества, применять достижения современных

информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах;
ОПК-5: способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;
ОПК-6: способность применять нормативные правовые акты в профессиональной деятельности;
ОПК-7: способность применять приемы первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций;
ОПК-8: способность к освоению новых образцов программных, технических средств и информационных технологий;
ПК-1 способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;
ПК-2 способность создавать и исследовать модели автоматизированных систем;
ПК-3 способность проводить анализ защищенности автоматизированных систем;
ПК-4 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
ПК-5 способность проводить анализ рисков информационной безопасности автоматизированной системы;
ПК-6 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;
ПК-7 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;
ПК-8 способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;
ПК-9 способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
ПК-10 способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;
ПК-11 способность разрабатывать политику информационной безопасности автоматизированной системы;
ПК-12 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;

ПК-13 способность участвовать в проектировании средств защиты информации автоматизированной системы;
ПК-14 способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
ПК-15 способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем;
ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;
ПК-17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
ПК-18 способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;
ПК-19 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
ПК-20 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
ПК-21 способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
ПК-22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
ПК-23 способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;
ПК-24 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;
ПК-25 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
ПК-26 способность администрировать подсистему информационной безопасности автоматизированной системы;
ПК-27 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;

ПК-28 способность управлять информационной безопасностью автоматизированной системы;
ПСК-7.1 способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах;
ПСК-7.2 способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах;
ПСК-7.3 способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем;
ПСК-7.4 способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
ПСК – 7.5 способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации.

В рамках изучения дисциплин, вынесенных на государственный экзамен выпускник должен:

Безопасность операционных систем

Знать:

- принципы построения и функционирования, примеры реализаций современных операционных систем;
- функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами;
- критерии оценки эффективности и надежности средств защиты ОС;
- принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows.

Уметь:

- использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;
- оценивать эффективность и надежность защиты операционных систем;
- планировать политику безопасности операционных систем.

Владеть:

- навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев;
- навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности.

Криптографические методы защиты информации

Знать:

- основные задачи и понятия криптографии;
- требования к шифрам и основные характеристики шифров;

- типовые поточные и блочные шифрсистемы, асимметричные криптосистемы;
- модели шифров и математические методы их исследования;
- криптографические стандарты и их использование в информационных системах.

Уметь:

- эффективно использовать отечественные и зарубежные стандарты в области криптографических методов защиты информации в автоматизированных системах;
- применять математические методы исследования моделей шифров.

Владеть:

- криптографической терминологией;
- навыками использования типовых криптографических алгоритмов;
- навыками использования ПЭВМ при анализе простейших шифров;
- навыками математического моделирования в криптографии;
- знаниями из научно-технической литературы в области криптографической защиты.

Техническая защита информации

Знать:

- технические каналы утечки информации и их характеристики;
- возможности технических средств перехвата информации;
- способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;
- организацию защиты информации от утечки по техническим каналам на объектах информатизации;
- основы физической защиты объектов информатизации.

Уметь:

- пользоваться нормативными документами по противодействию технической разведке;
- анализировать и оценивать угрозы информационной безопасности объекта.

Владеть:

- методами и средствами технической защиты информации;
- методами расчета и инструментального контроля показателей технической защиты информации

Организационное и правовое обеспечение информационной безопасности

Знать:

- основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
- правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях;

- организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации.

Уметь:

- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации.

Владеть:

- навыками работы с нормативными правовыми актами;
- навыками организации и обеспечения режима секретности;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- методами формирования требований по защите информации.

Программно-аппаратные средства обеспечения информационной безопасности

Знать:

- методы и средства ограничения доступа к компонентам ВС;
- методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям;
- методы и средства хранения ключевой информации;
- задачи и технологию сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности;
- способы встраивания средств защиты в программное обеспечение;
- цели и задачи защиты информации в сетях передачи данных;
- основные нормативные правовые акты и методические документы по защите от НСД.

Уметь:

- организовывать защиту программ от изучения;
- производить защиту от разрушающих программных воздействий;
- производить защиту программ от изменений;
- осуществлять контроль целостности программ и построение изолированной программной среды.

Владеть:

- средствами контроля информационной целостности;
- средствами защиты автоматизированного комплекса от несанкционированного доступа;
- средствами борьбы с вирусами и вредоносными закладками

Комплексное обеспечение информационной безопасности автоматизированных систем

Знать:

- содержание основных понятий по правовому обеспечению информационной безопасности;
- основы безопасности операционных систем;
- основы безопасности вычислительных сетей;
- основы правового регулирования взаимоотношений администрации и персонала в области защиты информации;
- основные технические средства и методы защиты информации;
- основные программно-аппаратные средства обеспечения информационной безопасности.

Уметь:

- создавать необходимую информационную базу с использованием безопасных информационных технологий;
- эффективно использовать средства и способы безопасных информационных технологий в профессиональной деятельности.

Владеть:

- навыками работы со средствами защиты информации, создавать и эксплуатировать системы защищенного электронного документооборота в организации;
- иметь навыки создавать необходимую информационную базу с использованием безопасных информационных технологий;
- эффективно использовать средства и способы безопасных информационных технологий в профессиональной деятельности.

Теоретические основы компьютерной безопасности

Знать:

- методологические и технологические основы комплексного обеспечения безопасности АС;
- угрозы и методы нарушения безопасности АС;
- формальные модели, лежащие в основе систем защиты АС;
- стандарты по оценке защищенности АС и их теоретические основы;
- методы и средства реализации защищенных АС;
- методы и средства верификации и анализа надежности защищенных АС.

Уметь:

- проводить анализ АС с точки зрения обеспечения компьютерной безопасности;
- разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы;
- применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС;
- реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС.

Владеть:

- навыками работы с документацией АС;
- навыками использования критериев оценки защищенности АС;

- навыками построения формальных моделей систем защиты информации АС.

Методы проектирования защищённых распределённых информационных систем

Знать:

- общие принципы построения защищенных распределенных систем;
- принципы проектирования архитектуры, структуры и основных объектов защищенных систем;
- основные этапы процесса проектирования и методы, используемые при построении проектируемой сети

Уметь:

- формировать требования к проектируемой сети с учетом анализа угроз и несанкционированных воздействий;
- составлять функциональные схемы проектируемых распределенных систем

Владеть:

- методами построения распределенных защищенных систем;
- навыками составления проекта и пониманием содержания основных этапов процесса проектирования.

Информационная безопасность распределённых информационных систем

Знать:

- концепцию диспетчера доступа;
- методы и средства ограничения доступа к ресурсам распределенной ВС;
- методы и средства обнаружения уязвимостей распределенной ВС;
- методы и средства обнаружения атак на ресурсы распределенной ВС;
- методы и средства противодействия атакам на ресурсы распределенной ВС.

Уметь:

- организовывать защиту распределенной ВС;
- производить защиту от атак на ресурсы распределенной ВС;
- производить защиту программ от изменений в распределенной ВС;
- осуществлять контроль трафика в рамках распределенной ВС.

Владеть:

- средствами защиты в распределенной ВС от несанкционированного доступа и нарушения функциональности ее подсистем;
- средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных.
- методикой контроля информационной целостности в распределенной ВС;

Технология построения защищённых распределённых приложений

Знать:

- Основы проектирования защищенных распределённых приложений;
-Распределенные базы данных как ядро распределенного приложения.

- Способы обеспечения безопасности при создании распределенных приложений.

Уметь:

- Вводить в эксплуатацию защищенное распределенное приложение

Владеть:

- Методами отладки защищенных распределенных приложений.

2.2.Критерии оценки результатов сдачи государственного экзамена.

Результаты государственного экзамена определяются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в тот же день после оформления в установленном порядке протоколов заседания ГЭК.

Оценка знаний и практических навыков студентов в ходе экзамена определяется по частным оценкам ответов на вопросы билета (см. Приложение 1.), каждым членом экзаменационной комиссии независимо друг от друга.

Результаты государственного экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» по следующим критериям:

-«отлично» - в частных оценках не более двух оценки «хорошо», а остальные «отлично», в том числе за практические навыки, действия;

-«хорошо» - в частных оценках не более двух оценки «удовлетворительно», а остальные «хорошо» или «отлично», в том числе за практические навыки, действия;

-«удовлетворительно» - не более одной частной оценки «неудовлетворительно», за исключением оценки за практические навыки, действия;

-«неудовлетворительно» - не выполнены условия на оценку «удовлетворительно».

Интегральная оценка определяется с учётом ответов по теоретической и практической части билета:

-«**отлично**» - в соответствии с паспортом компетенции дисциплины показывает глубокое и полное знание категорий и концепций, всего содержания учебной дисциплины; проявляет высокий уровень умений применять знания и методы для решения практических задач/заданий и владеет навыками использования их в сфере профессиональной деятельности;

-«хорошо» - в соответствии с паспортом компетенции дисциплины демонстрирует знание проблем и процессов, основного содержания учебной дисциплины, но допускает неточности в их объяснении; демонстрирует определённые навыки использования приобретённых умений при решении практических задач/заданий в профессиональной деятельности;

-«удовлетворительно» - в соответствии с паспортом компетенции

дисциплины имеет представление о категориях и концепциях, находящихся в отдельных частях учебной дисциплины; испытывает сложности при выборе методов для решения практических задач/заданий и объяснения их и может с трудом показать навыки использования приобретённого знания в будущей профессиональной деятельности

-«неудовлетворительно» - В соответствии с паспортом компетенции дисциплины не имеет представление о категориях и концепциях, находящихся в содержании учебной дисциплины; не может продемонстрировать умение выбирать методы для решения практических задач/заданий и не демонстрирует навыков необходимых в будущей профессиональной деятельности.

3. ОРГАНИЗАЦИЯ И ПОРЯДОК ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОГО ЭКЗАМЕНА.

Порядок проведения государственного экзамена по специальности 10.05.03 «Информационная безопасность автоматизированных систем» определяется на основании порядка проведения государственной итоговой аттестации по образовательным программам высшего образования – программам специалитета, объявленного приказом Минобрнауки РФ от 29 июня 2015 г. № 636; Положения о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры ФГБОУ ВО «Калининградский государственный технический университет» QD-8.1-(03.02), версия:V.3. (от 22.11.2017).

Организация и проведение государственного экзамена обеспечена рекомендациями обучающимся по подготовке к государственному экзамену (см. приложение ФОСы для ГИА).

3.1.Состав ГЭК. Государственный экзамен проводится государственной экзаменационной комиссией (ГЭК). Состав ГЭК по специальности 10.05.03 «Информационная безопасность автоматизированных систем» утверждается приказом ректора ФГБОУ ВО «КГТУ» по представлению заведующего кафедрой информационной безопасности, согласованному с деканом радиотехнического факультета не менее чем за месяц до наступления срока ГИА, установленного графиком учебного процесса на текущий учебный год.

Численный состав ГЭК не может быть меньше 5 человек, из которых не менее 50% являются ведущими специалистами - представителями работодателей или их объединений в области защиты информации, остальные - лицами, относящимися к профессорско-преподавательскому составу академии, и (или) иных организаций, имеющими ученое звание и (или) ученую степень.

3.2.Процедура проведения государственного экзамена. К государственному экзамену допускаются студенты, завершившие полный

курс обучения по основной образовательной программе и успешно прошедшие все предшествующие испытания, предусмотренные учебным планом.

На проведение государственного экзамена выделяется время из расчета не менее пяти дней с учетом подготовки к его сдаче. Расписание проведения государственного экзамена (дата, время, место), а также расписание предэкзаменационных консультаций устанавливается и оформляется начальником академии, которое доводится деканом РТФ до сведения обучающихся, всех членов комиссии, включая апелляционную комиссию, секретаря, консультантов и руководителей ВКР не позднее, чем за 30 дней до дня проведения первого государственного испытания. При формировании расписания устанавливается перерыв между государственными аттестационными испытаниями продолжительностью не менее 7 календарных дней.

Кафедра информационной безопасности разрабатывает экзаменационные билеты, подготавливает перечень таблиц, справочников, макетов, которыми разрешено пользоваться студентам на экзамене.

Обучающимся и лицам, привлекаемым к ГИА, во время её проведения запрещается иметь при себе, и использовать какие-либо средства связи. Присутствие посторонних лиц на государственном экзамене не допускается.

Экзаменационные билеты для государственного экзамена рассматриваются и утверждаются на заседании кафедры информационной безопасности и подписываются деканом РТФ и заведующим кафедрой информационной безопасности. Экзаменационный билет состоит из четырёх вопросов (трех теоретических и одного практического). Теоретические вопросы в каждом отдельно взятом билете не должны принадлежать одной и той же дисциплине из банка вопросов (см. приложение ФОС).

В качестве вопросов должны формулироваться основные теоретические положения, предполагающие их развернутое обоснование при ответе. Формулировка каждого вопроса должна определять рамки и объем ответа.

Количество экзаменационных билетов должно превышать количество студентов не менее чем на 10 %. Предварительное ознакомление студентов с экзаменационными билетами запрещается.

На экзамене должны быть:

- копия приказа об утверждении состава ГЭК;
- копия приказа о допуске к государственному экзамену обучающихся, выполнивших все требования учебного плана специальности 10.05.03 «Информационной безопасности автоматизированных систем»;
- программа государственной итоговой аттестации по специальности 10.05.03 «Информационной безопасности автоматизированных систем»;
- комплект экзаменационных билетов, утвержденных установленным порядком (Приложение 1);
- книга протоколов заседания ГЭК по приему государственного экзамена;

- списки обучающихся с итогами освоения ими ОП ВО (средний балл, информация о возможности получения диплома с отличием), в количестве экземпляров по числу членов ГЭК;

- зачетные книжки обучающихся, подготовленные и заполненные в деканате РТФ;

- чистые листы бумаги формата А4 (для записей при подготовке ответа);

- перечень наглядных пособий, материалов справочного характера, нормативных документов и программно-аппаратных средств, разрешенных к использованию на экзамене.

Перед началом экзамена студенты представляются председателю ГЭК. Студентам объявляется состав ГЭК и порядок сдачи экзамена.

Прибывший для сдачи экзамена студент докладывает председателю комиссии о прибытии, по его разрешению берет билет и называет его номер, знакомится с содержанием, получает чистые, специально подготовленные, листы бумаги со штампом (печатью) и готовится к ответу. Лист бумаги студент аккуратно оформляет и подписывает. При подготовке к ответу в устной форме студенты делают необходимые записи по каждому вопросу. Время на подготовку к ответу первому студенту отводится до 60 минут, остальные сменяются и отвечают в порядке очерёдности. Время на ответ по билету не должно превышать 45 минут.

О готовности к ответу студент докладывает председателю ГЭК и, получив разрешение, отвечает на вопросы экзаменационного билета.

На практический вопрос экзаменационного билета студенты отвечают, используя программно-аппаратные средства, макеты, плакаты, схемы, таблицы. После ответа на практический вопрос студент приступает к ответу на теоретические вопросы билета. После окончания ответа экзаменуемый докладывает председателю ГЭК о том, что он закончил ответ на поставленные вопросы. Члены комиссии в целях полного выяснения знаний экзаменуемого могут задавать дополнительные вопросы в объеме программного материала.

По завершении государственного экзамена, ГЭК на закрытом заседании с обязательным присутствием председателя комиссии обсуждает характер ответов и выставляет каждому студенту согласованную итоговую оценку в соответствии с критериями оценивания (ФОС приложение к ГИА).

В случае расхождения мнения членов ГЭК по итоговой оценке на основе оценок, поставленных каждым членом комиссии в отдельности, решение ГЭК принимается простым большинством голосов ее членов, участвующих в заседании, при обязательном присутствии председателя комиссии. При равном числе голосов председатель комиссии обладает правом решающего голоса.

Итоговая оценка по экзамену объявляется студенту в день сдачи государственного экзамена, проставляется в протокол заседания и зачетную книжку студента, где расписываются председатель и члены ГЭК.

Результаты сдачи оформляются протоколами заседаний, которые подписываются председателем и секретарём, сшиваются в книги и хранятся в архиве БГАРФ ФГБОУ ВО «КГТУ» в соответствии с утверждённой номенклатурой дел.

Листы с ответами студентов на экзаменационные вопросы хранятся на кафедре в течение установленного срока.

3.3. Повторное прохождение ГИА. Повторная сдача государственного экзамена с целью повышения положительной оценки не допустима.

Студентам, не явившимся на государственный экзамен по уважительной причине (по медицинским показаниям или в других исключительных случаях, подтвержденных документально), вправе пройти её в течение 6 месяцев после завершения государственной итоговой аттестации. Обучающийся должен представить в организацию документы, подтверждающие уважительную причину его отсутствия.

Продление сроков прохождения государственных итоговых аттестационных испытаний осуществляется приказом ректора университета (уполномоченного им лица) на основании личного заявления обучающегося, раскрывающего причину переноса сроков и резолюциями заведующего кафедрой ИБ, декана радиотехнического факультета, с приложением документов, подтверждающих уважительность причин неявки.

Предварительно заявление обучающегося с резолюциями ответственных лиц и приложенными документами представляется обучающимся на рассмотрение в ГЭК. Ходатайство или отказ в продлении сроков ГЭК, подтверждённое протоколом заседания, подписанного председателем ГЭК, прилагается к заявлению обучающегося.

По заявлению обучающегося, завизированному заведующим кафедрой ИБ и деканом радиотехнического факультета, при условии неявки на государственное аттестационное испытание по уважительной причине председателем ГЭК в исключительных случаях может быть принято решение о прохождении государственного экзамена в период защиты ВКР, если ГЭК является единой для приема междисциплинарного государственного экзамена и защиты ВКР.

Обучающийся, не прошедший одно государственное аттестационное испытание по уважительной причине, допускается к сдаче следующего государственного аттестационного испытания.

Обучающиеся, в том числе обучающиеся из числа инвалидов, не прошедшие государственное аттестационное испытание в связи с неявкой по неуважительной причине или отказавшиеся от прохождения государственной аттестации, а также не допущенные к прохождению государственной аттестации, или получившие на ГИА неудовлетворительные оценки, отчисляются из учебного заведения с выдачей справки об обучении как не выполнившие обязанностей по добросовестному освоению образовательной программы и выполнению учебного плана.

Лицо, не прошедшее государственную итоговую аттестацию, может

повторно пройти ГИА не ранее чем через 1год и не позднее чем через 5 лет после срока проведения ГИА, которая не пройдена обучающимся.

Для повторного прохождения ГИА лицо, не прошедшее аттестационные испытания по неуважительной причине, или получившее на ГИА неудовлетворительную оценку, по его заявлению восстанавливается в академии на период времени не менее предусмотренного календарным учебным графиком для ГИА по образовательной программе специальности 10.05.03 «ИБАС».

При восстановлении в академии для прохождения повторной ГИА выпускнику, по его желанию и согласованию с заведующим выпускающей кафедрой, и решению вуза может быть изменена тема ВКР.

Повторное прохождение ГИА проводится в соответствии с образовательными программами, освоенными во время обучения выпускника до первого итогового государственного испытания.

Для лиц, не прошедших государственное аттестационное испытание в связи с неявкой по неуважительной причине повторное прохождение ГИА включает в себя повторение всех видов государственной аттестации, несмотря на получение положительных оценок на государственном экзамене при первичной попытке пройти государственную аттестацию.

Допуск к повторному прохождению ГИА осуществляется деканом радиотехнического факультета в случае выполнения обучающимся действующей на текущий период времени образовательной программы.

3.4. Порядок проведения ГИА обучающимся из числа инвалидов.

Для обучающихся из числа инвалидов ГИА организуется с учетом особенностей их психофизического развития, их индивидуальных возможностей и состояния здоровья (далее - индивидуальные особенности).

Обучающийся инвалид не позднее, чем за три месяца до начала проведения государственной итоговой аттестации подаёт письменное заявление о необходимости создания для него специальных условий при проведении государственных аттестационных испытаний с указанием его индивидуальных особенностей. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в Вузе).

В заявлении обучающийся инвалид указывает на необходимость (отсутствие необходимости) присутствия ассистента на государственном аттестационном испытании, необходимость (отсутствие необходимости) увеличения продолжительности сдачи государственного аттестационного испытания по отношению к установленной продолжительности (для каждого аттестационного испытания). Продолжительность подготовки обучающегося, из числа инвалидов, к ответу на государственном экзамене, проводимом в устной форме, может быть увеличена не более чем на 20 минут. Продолжительность выступления обучающегося при защите ВКР - не более чем на 15 минут.

4. ТРЕБОВАНИЯ К ВЫПУСКНИКУ, ПРОВЕРЯЕМЫЕ В ХОДЕ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ.

В ходе теоретического обучения, при прохождении учебной практики, научно-исследовательской работы и производственных практик были полностью сформированы и оценены по степени освоения все компетенции согласно ФГОС ВО 10.05.03 «Информационная безопасность автоматизированных систем»

В процессе государственной итоговой аттестации (государственный экзамен в устной форме, защита ВКР в виде дипломной работы) по данной специализации завершается формирование и оценивается степень освоения комплекса компетенций, содержащих все общекультурные компетенции и общепрофессиональные компетенции, профессиональные компетенции и специальные профессиональные компетенции, согласно выбранным видам деятельности.

4.1.По итогам выпускной квалификационной работы в виде дипломной работы специалиста проверяется степень освоения выпускником следующих компетенций:

ОК-1: способность использовать основы философских знаний для формирования мировоззренческих позиций;
ОК-2: способность использовать основы экономических знаний в различных сферах деятельности;
ОК-3: способность анализировать основные этапы и закономерности исторического развития России, её место и роль в современном мире для формирования гражданской позиции и развития патриотизма;
ОК-4: способность использовать основы правовых знаний в различных сферах деятельности;
ОК-5: способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
ОК-6: способность работать в коллективе, толерантно воспринимая социальные, культурные и иные различия;
ОК-7: способность к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности;
ОК-8: способность к самоорганизации и самообразованию;
ОК-9: способность использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности;

ОПК-1: способность анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач;
ОПК-2: способность корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники;
ОПК-3: способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности;
ОПК-4: способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах;
ОПК-5: способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;
ОПК-6: способность применять нормативные правовые акты в профессиональной деятельности;
ОПК-7: способность применять приемы первой помощи, методы защиты производственного персонала и населения в условиях чрезвычайных ситуаций;
ОПК-8: способность к освоению новых образцов программных, технических средств и информационных технологий;
ПК-1 способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке;
ПК-2 способность создавать и исследовать модели автоматизированных систем;
ПК-3 способность проводить анализ защищенности автоматизированных систем;
ПК-4 способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;
ПК-5 способность проводить анализ рисков информационной безопасности автоматизированной системы;
ПК-6 способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;
ПК-7 способность разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;
ПК-8 способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем;

ПК-9 способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности;
ПК-10 способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности;
ПК-11 способность разрабатывать политику информационной безопасности автоматизированной системы;
ПК-12 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы;
ПК-13 способность участвовать в проектировании средств защиты информации автоматизированной системы;
ПК-14 способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
ПК-15 способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем;
ПК-16 способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных требований по защите информации;
ПК-17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;
ПК-18 способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности;
ПК-19 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы;
ПК-20 способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности;
ПК-21 способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем;
ПК-22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации;
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа;
ПК-24 способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности;

ПК-25 способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций;
ПК-26 способность администрировать подсистему информационной безопасности автоматизированной системы;
ПК-27 способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы;
ПК-28 способность управлять информационной безопасностью автоматизированной системы;
ПСК-7.1 способность разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах;
ПСК-7.2 способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах;
ПСК-7.3 способность проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем;
ПСК-7.4 способность проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах;
ПСК – 7.5 способность координировать деятельность подразделений и специалистов по защите информации на предприятии, в учреждении, организации.

4.2. Структура выпускной квалификационной работы и требования к её содержанию. Выпускная квалификационная работа (ВКР) для специальности 10.05.03 «ИБАС» в соответствии с уровнем ОП ВО выполняется в виде дипломной работы. Дипломная работа – самостоятельная исследовательская работа студента, которая связана с решением определённых производственных, организационно-управленческих, экономических задач, результатом которой является формулировка выявленных закономерностей, инструктивных материалов, технических или методических рекомендаций. ВКР представляет собой выполненную обучающимся (несколькими обучающимися совместно) работу, демонстрирующую уровень подготовленности выпускника к самостоятельной профессиональной деятельности.

Требования к структуре, рубрикации, содержанию и оформлению дипломных работ специалистов должны быть аналогичны требованиям к структуре, содержанию и оформлению отчетов по НИР, изложенным в ГОСТ 7.32-2017 «Отчет о научно-исследовательской работе. Структура и правила оформления».

ВКР состоит из пояснительной записки и графического материала.

Пояснительная записка включает в себя титульный лист (см. Приложение 2), задание на ВКР (см. Приложение 3), содержание, введение, обзор и анализ научно-технической и патентной информации, задачи ВКР, обоснование выбора темы, основную часть, заключение, список использованных источников, приложения. ВКР обязательно содержит пояснительную записку и другие материалы в электронном виде (CD-диск). Состав основной части пояснительной записки может изменяться руководителем ВКР с учетом специфики темы ВКР и должен указываться в задании на ВКР. В пояснительную записку вкладываются (не подшиваются) отзывы руководителя и рецензента.

Объем пояснительной записки рекомендуется не менее 60 страниц и не более 80 страниц.

Основная часть пояснительной записки делится на разделы, подразделы, пункты и подпункты. Каждый элемент основной части должен представлять собой законченный в смысловом отношении фрагмент ВКР.

В приложении оформляется материал, дополняющий содержание ВКР. В приложении или приложениях могут быть: графические материалы; таблицы большого формата; тексты программ и/или результаты расчета на ЭВМ; описания аппаратуры и приборов; схемы, чертежи и т.п.

Пояснительная записка ВКР должна в краткой и чёткой форме раскрывать сущность решаемой задачи, содержать обоснование принятого метода его решения и используемые средства, основные результаты работы, результаты эксперимента или моделирования и их анализ.

Электронная версия ПЗ, презентации и иных демонстрационных материалов при их наличии и возможности представления в электронном виде (фильмы, отдельные фотографии, чертежи, схемы и т.п. Прилагается к ПЗ на CD – диске. Если ВКР посвящена разработке программного обеспечения (ПО), электронная версия должна содержать полный набор компонентов ПО, необходимый для воспроизведения программы, включая исходный текст, исполняемые модули и библиотеки, набор драйверов, утилит, библиотек API и фреймворков, инструментальных сред разработки. Исключение составляют проприетарные среды, являющиеся собственностью заказчика ВКР, а также универсальные среды широкого применения, лицензия на которые имеется в вузе. После успешной защиты тексты ВКР размещаются в электронной библиотечной среде (ЭБС) академии секретарём ГЭК и ответственным за проверку на объём заимствований в течение недели после последнего дня защиты ВКР.

Доступ лиц к текстам ВКР должен быть обеспечен в соответствии с законодательством Российской Федерации, с учётом изъятия руководителем ВКР по решению правообладателя производственных, технических, экономических, организационных и других сведений, в том числе о результатах интеллектуальной деятельности в научно-технической сфере, о способах осуществления профессиональной деятельности, которые имеют

действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам.

4.3. Порядок утверждения тем выпускной квалификационной работы, выполнения её и представления в государственную экзаменационную комиссию. Темы ВКР разрабатываются выпускающей кафедрой информационной безопасности, утверждаются деканом РТФ, обновляются не реже одного раза в год и доводятся до сведения обучающихся не позднее, чем за 6 месяцев до начала государственной итоговой аттестации.

Темы ВКР должны быть актуальными, соответствовать современному состоянию и перспективам развития науки и техники, учитывать специфику специальности 10.05.03 «Информационная безопасность автоматизированных систем». При формулировке тем рекомендуется учитывать реальные задачи в области защиты информации в автоматизированных системах. Тематика ВКР определяется выпускающей кафедрой «Информационная безопасность», в соответствии с перечнем типовых тем выпускных квалификационных работ (см. Приложение ФОС ГИА.). По письменному заявлению обучающегося ему может быть предоставлена возможность подготовки и защиты ВКР по теме им предложенной, в случае обоснованности целесообразности её разработки для практического применения в области профессиональной деятельности по специальности 10.05.03 «ИБАС» или на конкретном объекте профессиональной деятельности. Решение об утверждении, предложенной обучающимся тематики, принимается на заседании выпускающей кафедры ИБ и утверждается деканом РТФ. Закрепление тем ВКР, руководителей, рецензентов и, при необходимости, консультантов осуществляется приказом начальника академии. Проект приказа подготавливается заведующим кафедрой ИБ, согласовывается с деканом радиотехнического факультета и заместителем начальника академии по УМР. Закрепление тем ВКР и руководителей ВКР специалистов осуществляется приказом начальника академии не позднее, чем за две недели до начала преддипломной практики по личному заявлению студента.

В исключительных случаях допускается корректировка темы ВКР по согласованию с руководителем ВКР и выпускающей кафедрой ИБ не позднее месяца до начала защиты ВКР, оформляемой приказом начальника академии, на основании мотивированного заключения заведующего кафедрой на имя заместителя начальника академии по учебно-методической работе, которое оформляется приказом начальника академии издаваемым не позднее, чем за неделю до окончания преддипломной практики.

Расписание государственных аттестационных испытаний (дата, время и место проведения защиты ВКР) устанавливается и оформляется распорядительным актом начальника академии, которое доводится до сведения обучающихся, всех членов комиссий, секретаря комиссии, руководителей и консультантов ВКР не позднее, чем за 30 дней до дня проведения государственного аттестационного испытания.

Для подготовки ВКР студенту назначается руководитель ВКР из числа преподавателей выпускающей кафедры, либо работодатель – специалист в области информационной безопасности. В случае необходимости, кафедре предоставляется право приглашать в качестве руководителей ВКР сотрудников других кафедр университета, ведущих специалистов и высококвалифицированных работников предприятий, научно-исследовательских и проектных институтов и других организаций, давших предварительное согласие на руководство. А также в случае необходимости могут назначаться консультанты по специальным разделам ВКР. Консультанты могут назначаться из числа специалистов предприятия, при выполнении ВКР по заявкам предприятий; либо из числа преподавателей соответствующих кафедр. Консультанты по этим разделам выдают задание и проверяют их выполнение. Отметки о выдачи задания консультанты делают на бланке задания на ВКР.

В обязанности руководителя входит:

- составление задания по сбору необходимого для выполнения ВКР материала в период прохождения обучающимся преддипломной практики;
- разработка совместно с обучающимся задания на ВКР (см.Приложение 3)
- оказание необходимой помощи обучающемуся при составлении календарного плана выполнения ВКР (см. Приложение 3), при подборе литературы и фактического материала в ходе преддипломной практики;
- консультирование обучающегося по вопросам ВКР согласно установленному графику;
- постоянный контроль за сроками выполнения ВКР, своевременностью и качеством написания отдельных глав и разделов работы;
- оформление отзыва на выполненную ВКР (см. Приложение 4);
- практическая помощь обучающемуся в подготовке текста доклада и презентационного материала к защите;
- присутствие на заседании ГЭК при защите обучающимся ВКР.

На первой неделе выполнения ВКР кафедра информационной безопасности проводит организационно-методическое собрание дипломников. На этом собрании освещаются основные вопросы, возникающие при выполнении ВКР, а именно: контрольные сроки проверки выполнения ВКР; сроки предзащиты ВКР на кафедре (отдельный график); график консультаций с научным руководителем по теме ВКР утверждается заведующим кафедрой информационная безопасность. На заседаниях кафедры регулярно выслушиваются доклады руководителей ВКР, который определяет степень выполнения ВКР.

Ответственность за содержание ВКР и за достоверность всех приведённых в ВКР данных несёт обучающийся.

Завершённая ВКР, сдаётся руководителю на проверку. Руководитель подписывает задание на ВКР, подтверждающее выполнение дипломной работы в указанные сроки и оформляет письменный отзыв. В отзыве

руководителя отмечается: актуальность темы, практическая ценность выполненного проекта, возможность внедрения результатов работы, уровень теоретической и практической подготовки студента, способность студента самостоятельно решать инженерные задачи, умение студента работать с научно-технической и учебной литературой, оценка работы студента над ВКР, возможность представления данной работы для защиты на заседании ГЭК.

Решение о допуске ВКР к защите принимается комиссией в составе сотрудников кафедры ИБ во время предварительной защиты. Цель предзащиты - оценка завершенности ВКР, качества ее выполнения и оформления, соответствия требованиям ФГОС ВО и ОП ВО по специальности 10.05.03 «ИБАС» и выпускающей кафедры (на основании данной программы ГИА), наличия реально полученных результатов, а также оценки готовности самого студента к защите.

Предзащиту ВКР выпускающая кафедра проводит не позднее, чем за 10 дней до защиты. Для этого составляется график заседания комиссий по проведению предзащит. При разработке графика для установления очередности может учитываться степень готовых к защите работ на основании сведений, поступающих от руководителей. На каждом заседании комиссии по предзащите должно присутствовать не менее двух членов комиссии из числа ведущих преподавателей выпускающей кафедры. Желательно (но не обязательно), чтобы на предзащите присутствовал и руководитель ВКР. Предзащита состоит из двух этапов: демонстрации реально полученных студентом результатов (работающий программный продукт, устройство или программно-технический комплекс, разработанный проект или результаты моделирования, экспериментальных или теоретических исследований) и оценки степени готовности к защите пояснительной записки ВКР, презентации, иных материалов и самого доклада выпускника.

Для предварительной защиты студент должен подготовить:

- результаты своей деятельности для демонстрации их комиссии;

-полностью оформленную пояснительную записку в несброшюрованном виде и её текст в электронном виде на CD-диске;

- согласованные с руководителем доклад и презентацию.

- справку по объёму неправомочных заимствований.

Проверки на объем заимствования осуществляются на выпускающих кафедрах на основании соответствующего распоряжения по назначению ответственного лица на выпускающей кафедре.

За две недели до даты защиты завершённая ВКР, в бумажном и электронном варианте, представляется обучающимся сотруднику выпускающей кафедры ИБ радиотехнического факультета, ответственному за проверку на объём заимствований, который в течение двух дней проводит проверку, выдаёт студенту справку о результатах проверки ВКР в системе «Антиплагиат» на объём заимствования, в том числе содержательного,

выявления неправомочных заимствований (Приложение №5) и бумажный вариант ВКР с отметкой об идентичности электронного и бумажного вариантов. Ответственность за проверку на идентичность бумажного и электронного варианта несёт назначенный на проведение данной процедуры сотрудник кафедры ИБ.

Итоговая оценка оригинальности текста ВКР определяется в системе «Антиплагиат. ВУЗ» и закрепляется на уровне не менее 40 % - для работ, выполненных обучающимися по программам подготовки специалистов.

Бумажный вариант ВКР вместе со справкой о результатах проверки ВКР в системе «Антиплагиат» на объём заимствования, представляется обучающимся руководителю, который оформляет письменный отзыв о работе, подписывает его и передаёт на проверку заведующему кафедрой, который проводит нормоконтроль. После положительного прохождения нормоконтроля заведующий ставит свою подпись на титульном листе в соответствующей графе.

В случае выполнения ВКР несколькими обучающимися руководитель представляет отзыв об их совместной работе в период подготовки ВКР.

Для проведения рецензирования ВКР направляется заведующим кафедрой рецензенту из числа лиц, не являющихся работниками кафедры, на которой выполнена ВКР согласно списка рецензентов по ранее оформленному приказу начальника академии.

Если ВКР имеет междисциплинарный характер, она направляется нескольким рецензентам. В этом случае число рецензентов устанавливается кафедрой. Рецензент проводит анализ ВКР и представляет на кафедру письменную рецензию на указанную работу. Рецензия составляется в соответствии с памяткой рецензента (см. Приложение 6)

ВКР, отзыв и рецензия (рецензии), справка по объёму заимствования обучающимся передаются секретарю ГЭК не позднее, чем за 2 календарных дня до дня защиты ВКР.

Конкретный вид предоставляемых для демонстрации практической реализации сведений и материалов зависит от тематической направленности ВКР и характера полученного в ходе ее выполнения результата.

На основании просмотренной записки, сделанного студентом доклада, презентации, качества ответов на заданные вопросы, и оценки продемонстрированных результатов, полученных в ходе проведения ВКР, комиссия принимает решение о допуске к защите или необходимости повторения процедуры предзащиты, если устранить замечания в срок представляется возможным.

На ближайшем заседании кафедры принимается решение о допуске ВКР к защите, на основании результатов предзащиты и отзыва руководителя.

Обучающийся должен быть ознакомлен руководителем и рецензентом ВКР с отзывом и рецензией не позднее, чем за 5 календарных дней до дня защиты ВКР.

Допуск обучающихся к ГИА по специальности 10.05.03. «Информационная безопасность автоматизированных систем» оформляется приказом начальника академии, проект которого подготавливает декан радиотехнического факультета не позднее, чем за день до наступления срока ГИА, установленного графиком учебного процесса на текущий учебный год. В проект приказа вносятся фамилии выпускников, в полном объеме успешно усвоивших ОП ВО по специальности 10.05.03 «ИБАС». На каждого из выпускников, не включенных в проект приказа о допуске к ГИА, должны быть приложены выписки из протокола заседания выпускающей кафедры с обоснованием причин их не допуска.

Допуск обучающегося к защите ВКР оформляется подписью заведующего выпускающей кафедрой информационной безопасности и декана радиотехнического факультета на титульном листе ВКР.

Обучающийся вправе выйти на защиту ВКР с отрицательной оценкой рецензента и отрицательным результатом проверки на объем неправомочных заимствований. В этих случаях окончательное решение принимает ГЭК по результатам защиты.

Ответственность за качество и своевременность выполнения ВКР полностью несёт обучающийся.

4.4. Порядок защиты ВКР. Защита выпускной квалификационной работы является обязательной частью ГИА. Заседания комиссий (состав ГЭК см. пункт 3.1.) правомочны, если в них участвуют не менее двух третей от числа членов комиссий.

Решения ГЭК принимаются на закрытых заседаниях простым большинством голосов членов комиссий, участвующих в заседании, при обязательном присутствии председателя комиссии. При равном числе голосов председатель комиссии обладает правом решающего голоса.

На защиту ВКР секретарем ГЭК представляются следующие материалы:

- в обязательном порядке:

- копию приказа об утверждении состава ГЭК;
- копия приказа о допуске к ГИА обучающихся;
- книга протоколов заседаний ГЭК по защите ВКР;
- списки обучающихся с итогами освоения ими ОП ВО (средний балл, информация о возможности получения диплома с отличием), в количестве экземпляров по числу членов ГЭК;
- оригинал ВКР (с визами руководителя, консультантов по разделам (при наличии), заведующего кафедрой, декана факультета;
- справка по объему неправомочных заимствований;
- отзыв руководителя;
- рецензия на ВКР;
- зачетная книжка обучающегося;

- в инициативном порядке:

- материалы, подтверждающие качество выполненного исследования (справку или акт о внедрении, публикации и т.д.);

- другие материалы в соответствии с требованиями внутренних нормативных документов выпускающей кафедры ИБ радиотехнического факультета по защите ВКР.

Продолжительность защиты ВКР не должна превышать 30 минут, а продолжительность заседания ГЭК - 6 часов в день.

В начале заседания председатель ГЭК объявляет о начале защит и предоставляет слово секретарю. Секретарь оглашает название, автора и руководителя ВКР, место ее выполнения, после чего предоставляет слово выпускнику для доклада. На доклад отводится не более 15 минут.

По окончании доклада председатель предлагает сначала членам ГЭК, а затем и всем присутствующим задать вопросы студенту. После окончания ответов на вопросы секретарь ГЭК зачитывает перечень дополнительных документов, представленных на защиту (например, акты о внедрении, дипломы, грамоты, свидетельства об участии в выставках и конкурсах, и т.п.) и отзывы руководителя, рецензента. Далее председатель дает возможность докладчику ответить на замечания при их наличии, предоставляя ему заключительное слово. После заключительного слова высказать свое мнение о работе могут все присутствующие на защите. Если у присутствующих не появилось вопросов, и нет желающих высказать свое мнение о работе, председатель объявляет окончание защиты, и начинается процедура защиты очередной работы. По итогам каждой защиты каждый член ГЭК проставляет оценку ВКР в баллах и заносит ее в оценочный лист. После последней защиты объявляется закрытое совещание ГЭК, на котором членами ГЭК обсуждаются результаты защит, подводятся общие итоги работы комиссии. По окончании закрытого заседания выпускники приглашаются в аудиторию, и председатель ГЭК объявляет результаты защиты.

ГЭК наряду с присвоением квалификации специалист по защите информации принимает решение о выдаче диплома установленного образца о высшем образовании, в том числе, диплома с отличием. Обучающийся, достигший особых успехов в освоении ОП ВО, имеет право на получение диплома с отличием при соблюдении следующих условий:

- наличие оценки "отлично" по всем государственным аттестационным испытаниям;

- не менее 75 % оценок "отлично" из числа оценок, вносимых в приложение к диплому, включая оценки по дисциплинам, курсовым работам (проектам), практикам и государственным аттестационным испытаниям, (остальные – «хорошо»);

- отсутствие перерывов в учебе, вызванных отчислением за академическую неуспеваемость и невыполнение студентом обязанностей, предусмотренных уставом университета.

В случае, когда в рамках промежуточной аттестации по одной дисциплине предусмотрено несколько экзаменов, итоговая оценка по

дисциплине, вносимая в приложение к диплому, определяется как последняя оценка по времени. Среднюю оценку выводить не допускается.

В целях получения диплома с отличием обучающемуся предоставляется возможность до начала государственных аттестационных испытаний пересдать не более трёх экзаменов (за исключением государственного).

Повторная сдача промежуточных экзаменов с целью повышения оценки производится с разрешения начальника академии (зам. начальника академии по учебно-методической работе) по письменному заявлению студента, в котором выражено мнение декана РТФ по вопросу возможной пересдачи.

В случае удовлетворения просьбы обучающегося и успешной повторной сдачи экзамена заявление прикладывается к личной карточке обучающегося, затем передаётся в его личное дело.

Двойная пересдача по одной дисциплине (с оценки «удовлетворительно» на «хорошо», затем с оценки «хорошо» на «отлично») не допускается.

ГЭК также принимает решение о рекомендации к внедрению результатов ВКР, представлению ВКР на конкурсы университетского и всероссийского уровней, по продолжению обучения выпускника на следующем уровне высшего образования (аспирантура) по специальности.

Повторное прохождение ГИА, порядок проведения ГИА обучающимся из числа инвалидов и апелляция результатов государственных аттестационных испытаний прописаны в пунктах 3.3; 3.4; 3.5 настоящей программы согласно положения о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры ФГБОУ ВО «Калининградский государственный технический университет» QD-8.1-(03.02), версия:V.3. (от 22.11.2017).

4.5.Показатели и критерии выставления оценок ВКР. Критерии выставления оценок (соответствия уровня подготовки выпускника требованиям ОП ВО на основе выполнения и защиты ВКР), с учётом степени освоения выпускником всех компетенций. В качестве критериев для оценки ВКР члены ГЭК должны учесть:

- актуальность темы ВКР. Степень её изученности и сложности исследования;
- теоретическая и практическая ценность ВКР. Обоснованность результатов проведённого исследования и сформулированных по его итогам выводов и предложений, а также степень новизны этих результатов;
- содержание работы. Степень самостоятельности студента при написании работы;
- использование источников;
- возможности практического использования полученных результатов.

- качество защиты ВКР. Уровень устного доклада и качество ответов на вопросы членов комиссии;
- оценку руководителя и рецензента;
- качество пояснительной записки и иллюстративного материала.
- соответствие оформления работы установленным требованиям и качество иллюстративного материала к докладу.

Оценка **«отлично»** выставляется студенту, являющемуся автором ВКР, соответствующей всем предъявляемым требованиям, при этом работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, глубокий анализ проблемы, критический разбор деятельности предприятия (организации), характеризуется логичным, последовательным изложением материала с соответствующими выводами и обоснованными предложениями; имеет положительные отзывы руководителя и рецензента; при защите работы студент показывает глубокие знания вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения по улучшению положения предприятия (организации) с точки зрения защиты информации, эффективному использованию имеющихся ресурсов, а во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, легко отвечает на поставленные вопросы.

Оценка **«хорошо»** выставляется студенту, являющемуся автором ВКР, соответствующей всем предъявляемым требованиям, при этом работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, достаточно подробный анализ проблемы и критический разбор деятельности предприятия (организации) с точки зрения защиты информации, характеризуется последовательным изложением материала с соответствующими выводами, однако с не вполне обоснованными предложениями; имеет положительный отзыв руководителя и рецензента; при защите студент показывает знания вопросов темы, оперирует данными исследования, вносит предложения по улучшению деятельности предприятия (организации), эффективному использованию ресурсов, во время доклада использует наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, без особых затруднений отвечает на поставленные вопросы.

Оценка **«удовлетворительно»** выставляется студенту, являющемуся автором ВКР, соответствующей всем предъявляемым требованиям, при этом работа носит исследовательский характер, содержит теоретическую главу, базируется на практическом материале, но отличается поверхностным анализом и недостаточно критическим разбором деятельности предприятия (организации) с точки зрения защиты информации, в ней просматривается непоследовательность изложения материала, представлены необоснованные предложения; в отзывах руководителя и рецензента имеются замечания по содержанию работы и методике анализа; при защите студент проявляет

неуверенность, показывает слабое знание вопросов темы, не дает полного, аргументированного ответа на заданные вопросы.

Оценка **«неудовлетворительно»** выставляется студенту, являющемуся автором ВКР, не соответствующей всем предъявляемым требованиям, а также, если работа не носит исследовательского характера, не содержит анализа и практического разбора деятельности предприятия (организации) в части защиты информации; не имеет выводов либо они носят декларативный характер; в отзывах руководителя и рецензента имеются существенные критические замечания; при защите студент затрудняется отвечать на поставленные вопросы по теме, не знает теории вопроса, при ответе допускает существенные ошибки, к защите не подготовлены наглядные пособия или раздаточный материал.

Оценка **«неудовлетворительно»** также выставляется студенту, если во время защиты у членов комиссии возникли обоснованные сомнения в том, что студент является автором представленной к защите выпускной квалификационной работы, то есть не ориентируется в тексте работы, не может дать ответы на уточняющие вопросы касающиеся сформулированных в работе теоретических и практических предложений. Такое решение принимается и в том случае, если работа соответствует всем предъявляемым требованиям.

Если оценка рецензента является «неудовлетворительной» и (или) неудовлетворительными являются результаты проверки на объём неправомочных заимствований, то окончательное решение принимает ГЭК по результатам защиты.

Приложение 1

Образец оформления
экзаменационного билета на государственный экзамен

Федеральное агентство по рыболовству (шрифт 14)
ФГБОУ ВО «Калининградский государственный технический университет»

Балтийская государственная академия рыбопромыслового флота

Экзаменационный билет № 1

Государственный экзамен по специальности 10.05.03. Информационная безопасность автоматизированных систем			
Семестр:	**10**		
Кафедра:	Информационная безопасность		
№ вопроса	Вопрос		
1	Информационная сфера и информационная среда. Субъекты и объекты правоотношений в области информационной безопасности.		
2	Раскрыть принципы построения модели Белла-ЛаПадулы и основной теоремы безопасности.		
3	Объекты и классы. Определение класса. Данные класса. Методы класса. Определение объектов.		
4	Расшифровать последовательность, зашифрованную шифром Цезаря: ZPTWSFJVKL, при условии что ключ k=3.		
И.о. декана РТФ			**В.А. Баженов**
Заведующий кафедрой ИБ			**Н.Я. Великите**

Приложение 2

Пример оформления титульного листа ВКР

Федеральное агентство по рыболовству (шрифт 14)
ФГБОУ ВО «Калининградский государственный технический университет»

Балтийская государственная академия рыбопромыслового флота

радиотехнический факультет (шрифт 14)

Кафедра информационной безопасности (шрифт 14)

Допустить к защите (ШРИФТ 14)

Декан факультета _____ /_____/_____
(подпись) (фамилия, инициалы) (дата)

Заведующий кафедрой _____/_____/_____
(подпись) (фамилия, инициалы) (дата)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (шрифт 16)

по _____
код и наименование специальности (направления подготовки)
_____

на тему _____ (шрифт 20)
наименование темы

Пояснительная записка (шрифт 14)
(ДР.БГАРФ.10.05.03.ИБ51.18 ПЗ)[1] (шрифт 14)

Разработал курсант/студент гр.___	_____	/ П.П.Петров /	01.06.2018
Руководитель к.т.н., доцент (шрифт 14)	_____	/ И.И.Иванов /	10.06.2018
Нормоконтролер к.т.н., доцент (шрифт 14)	_____ (подпись)	/С.М.Смирнов / (фамилия, инициалы)	15.06.2018 (дата)

Калининград – 2018 (шрифт 14)

[1] код пояснительной записки состоит из набора цифровых и буквенных сочетаний, которые означают:
ДР – форма работы (ДП – дипломный проект; ДР – дипломная работа; БР – ВКР бакалавра; МД – ВКР магистра);
БГАРФ – учебное заведение, где проходит обучение выпускник;
10.05.03 – код специальности (направления подготовки бакалавра, магистра) согласно ФГОС ВО;
ИБ51 – номер учебной группы;
18 – год выпуска из ВУЗа;
ПЗ – пояснительная записка (для инженерных специальностей)

Приложение 3

Задание на выпускную квалификационную работу

Федеральное агентство по рыболовству (шрифт 14)
ФГБОУ ВО «Калининградский государственный технический университет»

Балтийская государственная академия рыбопромыслового флота

Радиотехнический факультет факультет

Кафедра информационной безопасности

Специальность 10.05.03 – «Информационная безопасность автоматизированных систем»

(код и наименование специальности)

УТВЕРЖДАЮ

Заведующий кафедрой

_____
(название кафедры)
_____/_____/
(подпись) (фамилия и инициалы)

«_____»_____20___г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

студенту _____
(фамилия, имя, отчество)

1. Тема ВКР:_____
_____
_____

утверждена приказом начальника академии от «____»_____20___г. №_____

2. Цель работы: _____
_____
_____

3. Исходные данные: _____
_____
_____

4. Перечень вопросов, подлежащих разработке:

_____
_____
_____
_____
_____

5. Перечень графического материала _____

_____

6. Рекомендуемая литература: _____

_____

Календарный план
разработки выпускной квалификационной работы

№ п/п	Наименование этапов разработки ВКР	Срок выполнения	Примечание
1	2	3	4
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

7. Дата выдачи задания_____

8. Срок сдачи законченной ВКР _____

Руководитель ВКР _____/_____/
(подпись) (фамилия, инициалы)

Задание принял к исполнению студент

_____/_____/
(подпись) (фамилия, инициалы)

Приложение 4

Пример оформления отзыва на ВКР

О Т З Ы В

на выпускную квалификационную работу

Студента БГАРФ_____(Ф.И.О.)_____

Специальность: 10.05.03 – Информационная безопасность автоматизированных систем

Тема:_____
_____
_____

Объём ВКР: пояснительной записки____; количество листов приложений___
Заключение об актуальности и о степени соответствия выполненной ВКР заданию на ВКР и специальности_____
_____
_____

Проявленная при выполнении ВКР дипломником самостоятельность, умение планировать, дисциплинированность, соблюдение графика работы.
Индивидуальные особенности_____
_____
_____

Положительные стороны ВКР_____
_____
_____

Недостатки_____
_____
_____

Характеристика общетехнической и специальной подготовки студента – дипломника_____
_____
_____

Оценка качества выполнения пояснительной записки_____
_____
_____

Общая оценка за выполненную ВКР «____(по четырёх-бальной системе)__»
Выпускник __(ФИО)_____заслуживает присвоения квалификации «специалист по защите информации» по специальности 10.05.03 «Информационное обеспечение автоматизированных систем»
Руководитель____(звание, степень)_____ _____/_____(ФИО)__/
Место работы и должность_____

«_____»_____20__г.

Приложение 5

Образец справки о результатах проверки ВКР в системе «Антиплагиат»

Федеральное агентство по рыболовству
ФГБОУ ВО «Калининградский государственный технический университет»

Балтийская государственная академия рыбопромыслового флота

Деканат радиотехнического факультета
Кафедра информационной безопасности

СПРАВКА
О РЕЗУЛЬТАТАХ ПРОВЕРКИ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ В СИСТЕМЕ «АНТИПЛАГИАТ» НА НАЛИЧИЕ НЕПРАВОМЕРНЫХ ЗАИМСТВОВАНИЙ

В соответствии с положением о порядке проведения государственной итоговой аттестации по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры ФГБОУ ВО «Калининградский государственный технический университет» была проведена проверка текста выпускной квалификационной работы.

Тема ВКР_____
_____
_____
_____

ВКР выполнена студентом группы _____
_____
(шифр группы, Ф.И.О. студента, выполнившего работу)

Руководитель ВКР_____
_____
(ФИО, ученая степень, ученое звание)

Согласно проведенному анализу выявлено:
- полная идентичность электронного и бумажного варианта ВКР / не полная идентичность электронного и бумажного варианта ВКР (нужное подчеркнуть);
- в обозначенной работе оригинальный текст составляет _____ процентов.

Распечатка результатов проверки прилагается.

Проверку выполнил_____/_____/
Личная подпись И.О.Фамилия

____._____.20____

Приложение 6

Памятка рецензенту

1. В рецензии необходимо отразить: актуальность темы и её соответствие направлению подготовки; соответствие содержания ВКР заданию на её выполнение; полноту раскрытия вопросов, поставленных в задании; степень опоры дипломника на использование специальных и общеинженерных знаний (компетенций) при решении профессиональных задач; достаточность обращения к литературе по теме работы; элементы творчества дипломника; обоснованность выводов; новизну и практическую значимость результатов; недостатки ВКР с указанием конкретного раздела пояснительной записки, где выявлен данный недостаток.
2. Рецензент оценивает ВКР по четырёх бальной системе на: «неудовлетворительно», «удовлетворительно», «хорошо», «отлично», в соответствии с критериями приведёнными в приложении к программе ГИА (см. ФОС для ГИА) и пункта 1 данной памятки.
3. Рецензию оформлять в печатном виде. Ваша подпись должна быть заверена печатью организации, в которой Вы работаете.