МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

БАЛТИЙСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ ИММАНУИЛА КАНТА

Институт физико-математических наук и информационных технологий

«Согласовано»
Ведущий менеджер ООП ИФМНиИТ
_____ В.И.Бурмистров
«22» марта 2021 г.

«Утверждаю»
Директор ИФМНиИТ
_____ А.В.Юров
«22» марта 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Процедура защиты выпускной квалификационной работы»

для студентов 4 курса
очной формы обучения

направления подготовки 10.03.01.
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

профиль подготовки **«ОРГАНИЗАЦИЯ И ТЕХНОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ»**

уровень высшего образования – бакалавриат

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 34219E685EE8D891F77F96F99B3B8407
Владелец: Федоров Александр Александрович
Действителен: с 28.12.2022 до 22.03.2024

Калининград, 2021 г.

Лист согласования

Составители: доцент ИФМНиИТ, к. т. н., доцент Ветров И. А.

Программа обсуждена и утверждена на заседании учебно–методического совета института физико-математических наук и информационных технологий.

Протокол № __/__ от «__» _____ 20__ г.

Председатель учебно-методического совета _____первый заместитель директора института, к.ф.-м.н., доцент, Шпилевой А. А.

Программа пересмотрена на заседании учебно-методического совета института физико-математических наук и информационных технологий. Внесены следующие изменения (или изменений не внесено) _____

Протокол №____ от «___ »_____20_ г.

Ведущий менеджер ООП _____Бурмистров В. И.

СОДЕРЖАНИЕ
ПРОГРАММЫ ПРОЦЕДУРЫ ЗАЩИТЫ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

1. Общая характеристика процедуры государственной итоговой аттестации выпускника по направлению подготовки 10.03.01 «Информационная безопасность», уровень высшего образования – бакалавриат

1.1. Общие положения

Программа ГИА является частью основной профессиональной образовательной программы в соответствии с ФГОС ВО в части государственных требований к минимуму содержания и уровню подготовки выпускников по направлению подготовки 10.03.01 «Информационная безопасность».

К ГИА допускаются лица, выполнившие требования, предусмотренные курсом обучения по основной образовательной программе по направлению подготовки 10.03.01 «Информационная безопасность» и успешно прошедшие все промежуточные аттестационные испытания по теоретическому и практическому этапам обучения, предусмотренные утвержденным учебным планом направления подготовки 10.03.01 «Информационная безопасность».

Видом ГИА в соответствии с п. 2.7 ФГОС ВО и учебным планом является защита выпускной квалификационной работы.

Аттестацию проводит Государственная Экзаменационная Комиссия (ГЭК). Председатель ГЭК и состав ГЭК утверждаются в установленном порядке.

Выпускная квалификационная работа выполняется в обязательном порядке, в установленные сроки, проходит рецензирование (в необязательном порядке) и защищается в ГЭК.

Государственная итоговая аттестация (ГИА) включает в себя два основных этапа - этап подготовки к процедуре защиты выпускной квалификационной работы (Б3.01(Д)) и процедуру защиты выпускной квалификационной работы Б3.02(Д).

Наименование дисциплины (модуля) - «Процедура защиты выпускной квалификационной работы».

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Целью освоения дисциплины «Процедура защиты выпускной квалификационной работы» является защита выпускной квалификационной работы.

В ходе защиты выпускной квалификационной работы, обучающиеся должны показать свою способность и умение, опираясь на полученные углубленные знания, умения и сформированные универсальные и профессиональные компетенции, профессионально презентовать результаты своей работы, научно аргументировать и защищать свою точку зрения в ходе презентации.

Выпускник направления подготовки 10.03.01 «Информационная безопасность», профиль подготовки «Организация и технология защиты информации» в соответствии с целями основной образовательной программы и типами задач профессиональной деятельности в результате освоения данной дисциплины должен обладать компетенциями, представленными в таблице

Код компетенции	Результаты освоения ООП	Перечень планируемых результатов обучения по дисциплине
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	**Знать**: определения базовых понятий и категорий теориикоммуникации; формы, уровни и виды коммуникации; структуру коммуникационного процесса; специфику массовой коммуникации; основные положения теорий взаимодействия иаудитории **Уметь:** дифференцировать, характеризовать и оцениватьформы, уровни и виды коммуникации; выстраивать (моделировать) коммуникацию позаданным моделям и видам; отличать массовую коммуникацию от других видовкоммуникации по основным параметрам – адресант, адресат, сообщение, каналы, код, эффект;

		дифференцировать, характеризовать и оценивать отдельные компоненты, составляющие структуру коммуникационного процесса; дифференцировать, характеризовать и оценивать основные положения теорий взаимодействия СМК и аудитории; использовать и при необходимости трансформировать теоретические модели в соответствии с конкретной (реальной) коммуникативной ситуацией; оценивать особенности аудитории, удерживать и активировать ее внимание **Владеть**: навыками деловой коммуникации; способностью к обобщению, анализу, восприятию информации; базовыми навыками, составляющими коммуникативную компетентность личности, включая навык оценивания коммуникативной компетентности коммуникатора и коммуниканта, в том числе и в отношении собственной личности
ОПК-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	**Знать**: организационные формы и их применение для реализации информационных процессов; системное и прикладное программное обеспечение компьютера организационные формы и их применение для реализации информационных процессов; основные стандарты, нормы и правила, связанные со своей профессиональной деятельностью **Уметь:** создавать сложные документы с таблицами, формулами и рисунками; осуществлять поиск информации в сети интернет создавать документы, соответсвующие технической документации; читать конструкторские схемы и чертежи **Владеть**: техническими и программными средствами защиты информации при работе с компьютерными системами, включая приемы антивирусной защиты программным обеспечением, необходимым для создания документов, связанных со своей профессиональной деятельностью
ПК-1	Способен к выполнению работ по установке,	**Знать**: основные понятия теории

	настройке, обеспечению бесперебойной работы и техническому обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты информации	инфокоммуникационных технологий и методы построения моделей систем связи, основные стандарты построения многоканальных телекоммуникационных систем, принципы устройства станционных систем связи, построения и функционирования систем передачи информации, современные тенденции развития в области техники и технологий основ цифровых систем передачи (ЦСП), принципы построения многоканальных телекоммуникационных систем, методики и алгоритмы расчета основных разновидностей сетей, сооружений и средств инфокоммуникаций, средства автоматизации расчетов, приемы монтажа и настройки инфокоммуникационного оборудования для организации обмена трафиком на сетях связи **Уметь:** рассчитывать основные характеристики телекоммуникационных систем, учитывать тенденции развития основ цифровых систем передачи (ЦСП), собирать, анализировать исходные данные и квалифицированно проводить расчеты наиболее важных параметров многоканальных телекоммуникационных систем, применять стратегии и сценарии построения и модернизации многоканальных телекоммуникационных систем, проводить типовые расчеты основных разновидностей сетей, сооружений и средств инфокоммуникаций, определять системные принципы развития перечня услуг, сигнализации, нумерации и технического обслуживания, собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов, организовать монтаж и настройку инфокоммуникационного оборудования для организации информационного обмена на сетях связи **Владеть**: способностью использовать нормативную документацию при технической эксплуатации инфокоммуникационных систем, навыками работы с Российской и зарубежной научно-исследовательской литературой по тематике основ цифровых систем передачи (ЦСП), навыками работы с научно-технической информацией для применения отечественного и зарубежного опыта по

		тематике проекта, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникации, теоретическими и экспериментальными методами исследования с целью освоения новых перспективных технологий передачи цифровых сигналов, сравнительной оценкой различных способов построения многоканальных телекоммуникационных систем, оценкой влияния различных факторов на основные параметры каналов и трактов, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникаций
ПК-2	Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	**Знать**: базовые принципы, лежащие в основе наиболее распространённых формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; инструменты в операционных системах, посредством которых в данной системе можно реализовать ту или иную политику безопасности; отечественные и зарубежные стандарты для оценки эффективности систем защиты информации в операционных системах; основные этапы при проведении анализа безопасности компьютерной системы; наиболее популярные на сегодняшний день программно-аппаратные средства защиты информации; принципы функционирования различных программно-аппаратных средств защиты информации **Уметь:** строить теоретические модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учётом различных факторов; анализировать параметры компьютерной системы на соответствие стандартам безопасности; применять специализированные программные и аппаратные средства для оценки надёжности компьютерной системы; настраивать различные программно-аппаратные средства защиты информации в соответствии с рекомендациями производителя;

		разрабатывать собственные программные средства защиты информации наподобие имеющихся аналогов **Владеть**: навыками по реализации формальных моделей безопасности на практике; приёмами по выявлению «слабых» мест в системе безопасности различных компьютерных систем; навыками по анализу отчётов, которые предоставляют в ходе своей работы автоматизированные средства, предназначенные для проверки системы безопасности; навыками по использованию программно-аппаратных средств защиты информации для решения различных практических задач; навыками работы в команде
ПК-3	Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	**Знать**: методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности; этапы и процедуры аудита информационной безопасности автоматизированных систем управления **Уметь:** разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления **Владеть**: способами контроля эффективности реализации политики информационной безопасности организации; анализом недостатков в функционировании системы защиты информации автоматизированной системы;

		способами оценки защищённости автоматизированной системы; методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации
ПК-4	Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	**Знать**: архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры; принципы построения и работы ПЭВМ **Уметь:** определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования
ПК-5	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать**: принципы метрологического обеспечения, стандартизации и сертификации; способы и приёмы наладки, настройки, регулировки и испытания оборудования, тестирование, настройка и обслуживание аппаратно-программных средств; методы и способы проведение всех видов измерений параметров оборудования и сквозных каналов и трактов (настроечных, приёмосдаточных, эксплуатационных и аварийных); принципы оформления и делопроизводства в области метрологического обеспечения, стандартизации и сертификации

		телекоммуникаций **Уметь:** самостоятельно работать на компьютере и в компьютерных сетях, моделировать на компьютере устройства, системы и процессы с использованием универсальных пакетов прикладных компьютерных программ; применять принципы метрологического обеспечения и способы инструментальных измерений, используемых в области инфокоммуникационных технологий и систем связи; организовать и осуществить проверку технического состояния и ресурса оборудования; применять современные методы их обслуживания и ремонта **Владеть**: основными приёмами технической эксплуатации и метрологического обеспечения аппаратуры и систем телекоммуникаций

1.3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Процедура защиты выпускной квалификационной работы» составляет 3 зачетных единиц и 108 академических часов. Контактная работа обучающихся с преподавателем (по видам учебных занятий) 1 час, Самостоятельная работа обучающихся 107 академических часов

Место и время проведения государственной итоговой аттестации

Порядок и сроки проведения аттестационных испытаний устанавливаются в соответствии с графиком учебного процесса по направлению подготовки 10.03.01 «Информационная безопасность» профиль подготовки «Организация и технология защиты информации» на основании положения об организации выполнения и защиты выпускной квалификационной работы обучающимися (студентами) от 15.05.2014 г., утвержденного Ученым советом БФУ (протокол № 10 от 12 мая 2014 г.).

2. Процедура защиты выпускной квалификационной работы в Государственной экзаменационной комиссии

Защита выпускной квалификационной работы проводится в установленное время на заседании экзаменационной комиссии по соответствующему направлению подготовки ГЭК БФУ им. И. Канта. Кроме членов комиссии на защите необходимо присутствие научного руководителя или рецензента, а также возможно присутствие других студентов, преподавателей и администрации БФУ им. И. Канта.

2.1. Порядок защиты выпускной квалификационной работы на заседании ГЭК

1. Защита начинается с доклада студента по теме выпускной квалификационной работы. На доклад по выпускной квалификационной работе отводится до 8 минут.

Доклад следует начинать с обоснования актуальности избранной темы, описания научной проблемы и формулировки цели работы (не более 2 мин), а затем в последовательности, установленной логикой проведенного исследования, по главам раскрывать основное содержание работы, обращая особое внимание на наиболее важные разделы и интересные результаты, критические сопоставления и оценки (около 5 мин). Заключительная часть доклада строится по тексту заключения выпускной квалификационной работы, перечисляются общие выводы из её текста без повторения частных обобщений, сделанных при характеристике глав основной части, собираются воедино основные рекомендации (примерно 1 мин). Студент должен излагать основное содержание своей выпускной квалификационной работы свободно, не читая письменного текста.

Рекомендуется в процессе доклада использовать заранее подготовленный наглядный графический материал (таблицы, схемы), иллюстрирующий основные положения работы. Все материалы, выносимые на наглядную графику, должны быть оформлены так, чтобы студент мог демонстрировать их без особых затруднений, и они были видны всем присутствующим в аудитории.

В среднем насыщенность одного плаката (слайда) информацией должна быть эквивалентна 10-15 строкам текста, не более. Плакаты (слайды) нумеруются в первом верхнем углу. Весь плакат (слайд) или его части должны иметь заголовок-название: Постановка задачи, Структурная схема системы и т.д. Обычно плакаты (слайды) соответствуют разделам или подразделам работы.

2. После завершения доклада члены ГЭК задают студенту вопросы, как непосредственно связанные с темой ВКР, так и близко к ней относящиеся. При ответах на вопросы студент имеет право пользоваться своей работой.

3. После ответов студента на вопросы слово предоставляется научному руководителю. В конце своего выступления научный руководитель даёт свою оценку выпускной квалификационной работе.

4. При защите выпускной квалификационной работы после выступления научного руководителя слово предоставляется рецензенту. В случае отсутствия последнего на заседании ГЭК его отзыв зачитывает секретарь ГЭК. В конце своего выступления рецензент даёт свою оценку работе.

5. После выступления рецензента начинается обсуждение работы или дискуссия. В дискуссии могут принять участие как члены ГЭК, так и присутствующие заинтересованные лица.

6. После окончания дискуссии студенту предоставляется заключительное слово. В своём заключительном слове студент должен ответить на замечания рецензента, соглашаясь с ними или давая обоснованные возражения. Признаком хорошего тона являются слова благодарности в адрес членов ГЭК, научного руководителя и рецензента.

Решение ГЭК об итоговой оценке основывается на:

- оценке научного руководителя за работу, включая текущую работу в семестре;
- оценке рецензента за работу в целом;
- оценке членов ГЭК за содержание работы, её защиту, включая доклад, ответы на вопросы и замечания рецензента.

2.2. Описание показателей и критериев оценивания компетенций

Степень сформированности компетенций в результате защиты выпускной квалификационной работы осуществляется комиссией в ходе доклада по теме ВКР и ответах студента на вопросы в дискуссии.

1. В качестве критериев для оценки ВКР научные руководители и члены ГЭК должны иметь в виду:

- актуальность темы и задач работы;
- соответствие тематики направлению подготовки «Информационная безопасность»;
- обоснованность результатов и выводов;
- определенную оригинальность и новизну полученных данных;
- самостоятельность (личный вклад студента);
- возможности практического использования полученных результатов.

2. Обоснованность результатов и выводов определяются с позиций:

- соответствия известным научным положениям и фактам;
- логичности в изложении и обсуждении собственных данных;
- корректности постановки опыта, эксперимента;
- корректности использования математических методов.

При этом должны учитываться:

- уровень устного доклада на защите;
- соответствие оформления работы установленным требованиям;
- качество иллюстративного материала к докладу.

3. Оригинальность и новизна полученных данных определяется как:

- установление нового научного факта или подтверждение известного факта для новых условий;
- получение сведений, приводящих к формулировке проверяемых гипотез, которые требуют дальнейшей проверки;
- разработка оригинального метода решения известной задачи;
- применение известных методик для решения новых задач;

- введение в научный оборот новых данных;
- обоснованное решение поставленной задачи.

4. Личный вклад студента определяется: степенью самостоятельности в выборе темы, постановке задач, планировании и организации исследования, обработке и осмыслении полученных результатов.

5. Возможность практического использования данных, полученных в ВКР, определяется в отношении НИР, выполняемых в университете или в других организациях; задачами совершенствования учебного процесса; возможностью публикации в печати.

2.3. Шкала оценивания степени сформированности компетенций

Выпускная квалификационная работа оценивается по четырёхбалльной шкале: 5 – «отлично», 4 – «хорошо», 3 – «удовлетворительно», 2 – «неудовлетворительно».

Выпускная квалификационная работа оценивается членами ГЭК на основании доклада студента и выступления рецензента. Члены ГЭК оценивают уровень работы не только на основе перечисленных критериев (см. предшествующий раздел), а также обязательно принимают во внимание умение выпускника представить свою работу и правильно ответить на вопросы членов ГЭК.

Оценка **«ОТЛИЧНО»** ставится за реализацию всех необходимых компетенций в ходе доклада по теме ВКР и ответах на вопросы в дискуссии (высокий уровень сформированных компетенций): выпускная квалификационная работа имеет исследовательский характер, грамотно изложена теоретическая часть, логичное, последовательное изложение материала с соответствующими выводами и обоснованными предложениями. При её защите студент показывает глубокие знания вопросов темы. Выпускная квалификационная работа имеет положительные отзывы научного руководителя и рецензента.

Оценка **«ХОРОШО»** ставится за частичную реализацию всех необходимых

компетенций в ходе доклада по теме ВКР и ответах на вопросы в дискуссии (уровень освоения компетенций достаточный): выпускная квалификационная работа содержит элементы научного исследования, грамотно изложена теоретическая часть, логичное, последовательное изложение материала с соответствующими выводами, однако с не вполне обоснованными предложениями. При её защите студент показывает знания вопросов темы, оперирует данными исследования, во время доклада использует наглядные пособия, без особых затруднений отвечает на поставленные вопросы. Выпускная квалификационная работа имеет положительные отзывы научного руководителя и рецензента.

Оценка **«УДОВЛЕТВОРИТЕЛЬНО»** ставится в том случае, если студент демонстрирует частичную сформированность компетенций (средний уровень), предусмотренных ФГОС: выпускная квалификационная работа имеет технический характер, базируется на практическом материале, но анализ выполнен поверхностно, в ней просматривается непоследовательность изложения материала. Представлены необоснованные предложения. При её защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не дает полных аргументированных ответов на заданные вопросы. В отзывах научного руководителя и рецензента имеются замечания по содержанию работы и методике анализа.

Оценка **«НЕУДОВЛЕТВОРИТЕЛЬНО»** выставляется, если демонстрируется несформированность (низкий уровень сформированности) соответствующих компетенций, предусмотренных ФГОС ВО: выпускная квалификационная работа не носит исследовательского характера, не отвечает требованиям, изложенным в методических рекомендациях. В работе нет выводов, либо они носят декларативный характер. При защите работы студент затрудняется отвечать на поставленные вопросы, при ответе допускает существенные ошибки. В отзывах научного руководителя и рецензента имеются серьезные критические замечания.

Итоговая оценка ГЭК выводится по принципу учета оценок большинства

членов ГЭК, а также руководителя. Оцениваемые компетенции и оценочный лист приведены в приложениях 1 и 2, соответственно.

Итоговая оценка за защиту ВКР складывается из оценок:

- демонстрационных материалов (презентации результатов работы);
- доклада на защите;
- ответов на вопросы членов комиссии.

Руководитель ВКР и члены ГЭК по итогам защиты ВКР оценивают уровень сформированности компетенций по:

- качеству демонстрационного материала,
- содержательности и логичности представленного доклада,
- ответам на заданные вопросы.

По результатам группового обсуждения всех присутствующих членов ГЭК председатель заполняет оценочный лист (приложение 2).

3. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература

1. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс]: учеб. и практикум для бакалавриата и магистратуры/ [Т. А. Полякова [и др.] ; под ред.: Т. А. Поляковой, А. А. Стрельцова. - Москва: Юрайт, 2019. - 1 on-line, 325 с.: рис.. - (Бакалавр и магистр. Академический курс)
2. Титов, А. А. Инженерно-техническая защита информации : учебное пособие / А. А. Титов. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2010. — 197 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/13931.html

Дополнительная литература

1. Мельников, В. П. Информационная безопасность [Электронный ресурс]: [учеб. пособие]/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 8-е изд., испр.. - Москва: Академия, 2013. - 1 эл. опт. диск (CD-ROM), 336 с.: рис., табл.). - - Библиогр.: с. 327-328 (37 назв.)
2. Шейдаков, Н. Е. Физические основы защиты информации: учеб. пособие для вузов/ Н.Е. Шейдаков, О.В. Серпенинов, Е.Н. Тищенко. - Москва: РИОР; Москва: Инфра-М, 2017. - 202, [1] с.: ил. - (Высшее образование). - Библиогр.: с. 195-198. - ISBN 978-5-369-01603-9. - ISBN 978-5-16-012372-1: 485.89, 485.89, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
3. Сагдеев, К. М. Физические основы защиты информации: учеб. пособие для вузов/ К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. - 2-е изд., испр. и доп.. - Санкт-Петербург: Интермедия, 2017. - 408 с.: ил. - Библиография: с. 405-406 (22 названия). - ISBN 978-5-4383-0141-7: 780.00, 780.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
4. Рагозин, Ю. Н. Инженерно-техническая защита информации: учеб. пособие по физ. основам образования техн. каналов утечки информации по практикуму оценки их опасности/ Ю. Н. Рагозин. - Санкт-Петербург: Интермедия, 2018. - 165 с.: ил.. - Библиогр.: с. 164-165 (31 назв.). - ISBN 978-5-4383-0161-5: 680.00, 680.00, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
5. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам/ Г. А. Бузов. - Москва: Горячая линия-Телеком, 2014. - 585, [4] л. вкл. с.: ил.. - Библиогр.: с. 574-581 (126 назв.). - ISBN 978-5-9912-0424-8: 712.80, 712.80, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
6. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации/

В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп.. - Москва: Форум; Москва: ИНФРА-М, 2014. - 255 с. - (Высшее образование - бакалавриат). - Библиогр.: с. 251-253. - ISBN 978-5-91134-856-4. - ISBN 978-5-16-009578-3: 349.69, 349.69, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)

7. Бузов, Г. А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации/ Г. А. Бузов. - М.: Горячая линия-Телеком, 2013. - 239 с.: ил. - Библиогр.: с. 230-235. - ISBN 978-5-9912-0121-6: 303.60, 303.60, р. Имеются экземпляры в отделах /There are copies in departments: ч.з.N3(1)
8. Технические средства и методы защиты информации: учеб. пособие для вузов/ А. П. Зайцев [и др.]; под ред. А. П. Зайцева, А. А. Шелупанова. - [4-е изд., испр. и доп.]. - М.: Горячая линия-Телеком, 2012. - 615 с.: ил. - (Учебное пособие для высших учебных заведений. Специальность). - Библиогр.: с. 608-609 (34 назв.). - ISBN 978-5-9912-0084-4: 699.60, 699.60, р. Имеются экземпляры в отделах /There are copies in departments: всего /all 15: УБ(14), ч.з.N3(1)

Перечень интернет-источников

1. «Национальная электронная библиотека» (http://xn--90ax2c.xn--p1ai/).
2. ЭБС Кантиана (https://elib.kantiana.ru/).
3. ЭБС IPR BOOKS (https://www.iprbookshop.ru/78574.html).
4. ЭБС Znanium (https://znanium.com/catalog/document?id=333215).

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕДЕНИИ ПРАКТИКИ

1. Использование системы электронного образовательного контента БФУ им. И. Канта http://lms-3.kantiana.ru/.
2. Использование электронной образовательной среды БФУ им. И. Канта https://teams.microsoft.com/

4. Фонд оценочных средств для проведения ГИА

Компетенция	Перечень планируемых результатов	Диагностический инструмент	Критерии оценки
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	1. Актуальность тематики работы и её соответствие профилю ОП 2. Степень полноты обзора состояния вопроса и корректность постановки задачи. 3. Уровень и корректность использования в работе методов исследований, математического моделирования, расчетов.	Глубокое раскрытие темы, качественное оформление работы, обоснованность сделанных выводов и их аргументированность, оригинальность и новизна полученных результатов.

ОПК-2 Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	**Знать**: организационные формы и их применение для реализации информационных процессов; системное и прикладное программное обеспечение компьютера организационные формы и их применение для реализации информационных процессов; основные стандарты, нормы и правила, связанные со своей профессиональной деятельностью **Уметь:** создавать сложные документы с таблицами, формулами и рисунками; осуществлять поиск информации в сети интернет создавать документы, соответсвующие технической документации; читать конструкторские схемы и чертежи **Владеть**: техническими и программными средствами защиты информации при работе с компьютерными системами, включая приемы антивирусной защиты программным обеспечением, необходимым для создания документов, связанных со своей профессиональной деятельностью	3. Степень комплексности работы, применение в ней знаний общепрофессиональных и специальных дисциплин. 5. Ясность, четкость, последовательность и обоснованность изложения. 6. Применение современного математического и программного обеспечения, компьютерных технологий в работе. 7. Качество оформления (общий уровень грамотности, стиль изложения, качество иллюстраций, соответствие требованиям стандартов). 8. Объем и качество выполнения графического материала, его соответствие тексту. 9. Обоснованность и доказательность выводов работы. 10. Оригинальность и новизна полученных результатов, научно-исследовательских, технических или методических решений.	

ПК-1 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	**Знать**: основные понятия теории инфокоммуникационных технологий и методы построения моделей систем связи, основные стандарты построения многоканальных телекоммуникационных систем, принципы устройства станционных систем связи, построения и функционирования систем передачи информации, современные тенденции развития в области техники и технологий основ цифровых систем передачи (ЦСП), принципы построения многоканальных телекоммуникационных систем, методики и алгоритмы расчета основных разновидностей сетей, сооружений и средств инфокоммуникаций, средства автоматизации расчетов, приемы монтажа и настройки инфокоммуникационного оборудования для организации обмена трафиком на сетях связи **Уметь:** рассчитывать основные характеристики телекоммуникационных систем, учитывать тенденции развития основ цифровых систем передачи (ЦСП), собирать, анализировать исходные данные и квалифицированно проводить расчеты наиболее важных параметров многоканальных телекоммуникационных систем, применять стратегии и сценарии построения и модернизации многоканальных телекоммуникационных систем, проводить типовые расчеты основных разновидностей сетей, сооружений и средств инфокоммуникаций, определять системные принципы развития перечня услуг, сигнализации, нумерации и технического обслуживания, собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов, организовать монтаж и настройку инфокоммуникационного оборудования для организации информационного обмена на		

	сетях связи **Владеть**: способностью использовать нормативную документацию при технической эксплуатации инфокоммуникационных систем, навыками работы с Российской и зарубежной научно-исследовательской литературой по тематике основ цифровых систем передачи (ЦСП), навыками работы с научно-технической информацией для применения отечественного и зарубежного опыта по тематике проекта, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникации, теоретическими и экспериментальными методами исследования с целью освоения новых перспективных технологий передачи цифровых сигналов, сравнительной оценкой различных способов построения многоканальных телекоммуникационных систем, оценкой влияния различных факторов на основные параметры каналов и трактов, первичными навыками типовых расчетов основных разновидностей сетей, сооружений и средств инфокоммуникаций		
ПК-2 Способен применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения	**Знать**: базовые принципы, лежащие в основе наиболее распространённых формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах; инструменты в операционных системах, посредством которых в данной системе можно реализовать ту или иную политику безопасности; отечественные и зарубежные стандарты для оценки эффективности систем защиты информации в операционных системах; основные этапы при проведении анализа безопасности компьютерной системы; наиболее популярные на сегодняшний день программно-		

профессиональных задач	аппаратные средства защиты информации; принципы функционирования различных программно-аппаратных средств защиты информации **Уметь:** строить теоретические модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учётом различных факторов; анализировать параметры компьютерной системы на соответствие стандартам безопасности; применять специализированные программные и аппаратные средства для оценки надёжности компьютерной системы; настраивать различные программно-аппаратные средства защиты информации в соответствии с рекомендациями производителя; разрабатывать собственные программные средства защиты информации наподобие имеющихся аналогов **Владеть**: навыками по реализации формальных моделей безопасности на практике; приёмами по выявлению «слабых» мест в системе безопасности различных компьютерных систем; навыками по анализу отчётов, которые предоставляют в ходе своей работы автоматизированные средства, предназначенные для проверки системы безопасности; навыками по использованию программно-аппаратных средств защиты информации для решения различных практических задач; навыками работы в команде		
ПК-3 Способен принимать участие в организации и проведении	**Знать**: методы анализа и оценки защищённости автоматизированных систем; национальные и международные стандарты в области аудита и оценки информационной безопасности;		

контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	этапы и процедуры аудита информационной безопасности автоматизированных систем управления **Уметь:** разрабатывать методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять разработанные методики оценки защищённости программно-аппаратных средств защиты информации автоматизированных систем; применять национальные и международные стандарты в области защиты информации для оценки защищённости автоматизированной системы; проводить проверку организаций на соответствие требованиям нормативных правовых актов в области информационной безопасности защищённых автоматизированных систем управления **Владеть**: способами контроля эффективности реализации политики информационной безопасности организации; анализом недостатков в функционировании системы защиты информации автоматизированной системы; способами оценки защищённости автоматизированной системы; методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем управления нормативным требованиям по защите информации		
ПК-4 Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения	**Знать**: архитектуру основных типов современных компьютерных систем; структуру и принципы работы современных и перспективных микропроцессоров; принципы работы элементов и функциональных узлов электронной аппаратуры;		

информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	принципы построения и работы ПЭВМ **Уметь:** определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств; работать с современной элементной базой электронной аппаратуры. определять направления использования ЭВМ определенного класса для решения служебных задач **Владеть**: навыками применения технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности; навыками устранения неисправностей и технического обслуживания ПЭВМ и периферийного оборудования; навыками формирования структуры СВТ и выбора режимов их функционирования		

ПК-5 Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	**Знать**: принципы метрологического обеспечения, стандартизации и сертификации; способы и приёмы наладки, настройки, регулировки и испытания оборудования, тестирование, настройка и обслуживание аппаратно-программных средств; методы и способы проведение всех видов измерений параметров оборудования и сквозных каналов и трактов (настроечных, приёмосдаточных, эксплуатационных и аварийных); принципы оформления и делопроизводства в области метрологического обеспечения, стандартизации и сертификации телекоммуникаций **Уметь:** самостоятельно работать на компьютере и в компьютерных сетях, моделировать на компьютере устройства, системы и процессы с использованием универсальных пакетов прикладных компьютерных программ; применять принципы метрологического обеспечения и способы инструментальных измерений, используемых в области инфокоммуникационных технологий и систем связи; организовать и осуществить проверку технического состояния и ресурса оборудования; применять современные методы их обслуживания и ремонта **Владеть**: основными приёмами технической эксплуатации и метрологического обеспечения аппаратуры и систем телекоммуникаций		

4.1. Примерная тематика выпускных квалификационных работ по направлению подготовки 10.01.01 «Информационная безопасность» (профиль подготовки «Организация и технология защиты информации»).

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»

4.2. Примеры формулировки тем и содержания выпускных квалификационных работ

Тема: Разработка механизма защиты диспетчерских компонентов сетей АСУ ТП

Введение

Глава 1. Теоретическая часть.

1.1 Особенности построения и функционирования распределенной многоуровневой АСУ ТП

1.2 Структура многоуровневой АСУ ТП на базе MasterSCADA

1.3 SCADA-система и особенности ее защиты

Глава 2 Повышение защищенности подсистем диспетчерского уровня АСУ ТП.

2.1 Определение архитектуры разрабатываемых механизмов выявления и

блокирования программ.

2.2 Разработка алгоритмов выявления и блокирования вредоносных программ.

2.3 Определение особенностей эксплуатации разработанных механизмов.

Глава 3. Определение эффективности разработанных механизмов защиты.

Заключение.

Список использованных источников

1. ГОСТ Р МЭК 61131-3-2016 Национальный стандарт Российской Федерации. Контроллеры программируемые. Часть 3. Языки программирования" (утв. и введен в действие Приказом Росстандарта от 13.05.2016 N 313-ст) из информационного банка "Отраслевые технические нормы" «КонсультантПлюс» [Электронный ресурс] – URL:http://consultant.ru
2. Приказ ФСТЭК России от 14.03.2014 N 31 (ред. от 09.08.2018) "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" (Зарегистрировано в Минюсте России 30.06.2014 N 32919)
3. Байрс Э. IT-безопасность в промышленности. Глубокий анализ пакетов данных для SCADA-систем // Современные технологии автоматизации. - 2013.-№4. – с.12-16.
4. Единое окно доступа к образовательным ресурсам [Электронный ресурс] – URL:http://window.edu.ru/
5. Антивирусная утилита [Электронный ресурс] – URL:http://z-oleg.com/
6. Втюрин В.А. Автоматизированные системы управления технологическими процессами. Основы АСУ ТП: учебное пособие для студентов высшего учебного заведений // -СПб.: Санкт-Петербургская Государственная Лесотехническая Академия имени С.М. Кирова, 2006. -152
7. «КонсультантПлюс» [Электронный ресурс] – URL:http://consultant.ru

8. Зайцев О. В. ROOTKITS, SPYWARE/ADWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. – СПб.: БХВ-Петербург, 2006. – 304 с.
9. Котенко И. В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях // Новости искусственного интеллекта. – 2004. – № 1. – с. 56–72.
10. MasterSCADA-система для АСУ ТП [Электронный ресурс] – URL:https://masterscada.insat.ru/
11. Определение эффективности [Электронный ресурс] – URL:https://dsec.ru/
12. Подтопельный В. В. Особенности информационной защиты систем управления на промышленных объектах // III БАЛТИЙСКИЙ МОРСКОЙ ФОРУМ: материалы Международного морского форума. – Калининград: Изд-во БГАРФ,2015 г., с. 74-78.
13. Подтопельный В. В. Уязвимости системы информационного сопровождения судов // II БАЛТИЙСКИЙ МОРСКОЙ ФОРУМ: материалы Международного морского форума. – Калининград: Изд-во БГАРФ,2014 г., с. 70-74.
14. Фаулер, М. UML. Основы. Учебное пособие [Текст] / М. Фаулер. – Символ-Плюс, 2007. – 192 с.: ил. – 2000 экз. – ISBN: 5-93286-060-5
15. Щербаков А. Сеть CAN: популярные прикладные протоколы // ChipNews,1999, №5.

ПРИЛОЖЕНИЯ

Приложение 1

Оценочный лист сформированности компетенций для руководителя ВКР и членов ГЭК

Коды проверяемых компетенций	Текст ВКР	Этап подготовки к процедуре защиты ВКР
УК-4	+	+
ОПК-2	+	+
ПК-1	+	+
ПК-2	+	+
ПК-3	+	+
ПК-4	+	+
ПК-5	+	+

Приложение 2

Оценочный лист членов ГЭК

Оценка уровня сформированности компетенций студента _____ направления подготовки 10.03.01 «Информационная безопасность» профиль подготовки «Организация и технология защиты информации защиты информации» в процессе защиты выпускной квалификационной работы, выполненной на тему

_____

_____

Коды проверяемых компетенций	**Показатели оценки результата**	**Показатели уровня сформированности компетенций**			
		2 – низкий	**3 – средний**	**4 – достаточный**	**5 – высокий**
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)				
ОПК-2	Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности				
ПК-1	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-2	Способен применять				

	программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач				
ПК-3	Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации				
ПК-4	Способен проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений				
ПК-5	Способен оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов				
ПК-6	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				