МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
_____ А.Г. Жуковский
«_29_» ____08_____ 2022 г.

Б3.01 Государственная итоговая аттестация
Подготовка к процедуре защиты и защита выпускной квалификационной работы

рабочая программа

Кафедра **«Информатика и вычислительная техника»**

Направление подготовки **10.03.01 Информационная безопасность**
Профиль **Безопасность компьютерных систем**
Формы обучения **очная**

Объем и структура подготовки к процедуре защиты и защиты выпускной квалификационной работы				
Вид учебной работы	ОФ		ЗФ	
	ЗЕ	часов	ЗЕ	часов
Общая трудоемкость государственной итоговой аттестации	6	216		
Самостоятельная работа	6	216		

Программу составил:
зав. кафедрой ИВТ д.т.н. профессор Соколов С.В.

Рецензенты:
Ведущий научный сотрудник РНИИРС д.т.н. доцент Погорелов В.А.

Рабочая программа
Государственная итоговая аттестация
Подготовка к процедуре защиты и защита выпускной квалификационной работы

Разработана в соответствии с ФГОС ВО
направления подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства образования и науки Российской Федерации от 17 ноября 2020г. №1427.

Составлена на основании учебного плана
направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 25.04.2022, и утвержденного директором СКФ МТУСИ 25.04.2022 г.

Одобрена на заседании кафедры
"Информатика и вычислительная техника "

Протокол от 29.08. 2022 г. № 1
Зав. кафедрой _____/ Соколов С.В./

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры **"Информатика и вычислительная техника "**

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____/ Соколов С.В./

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры **"Информатика и вычислительная техника "**

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____/ Соколов С.В./

Визирование для использования в 20__/20__ уч. году

Утверждаю
Зам. директора по УВР
__ _____ 20__ г.
Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры **"Информатика и вычислительная техника "**

Протокол от _ _____ 20__ г. № _
Зав. кафедрой _____/ Соколов С.В./

1. Цели подготовки к процедуре защиты и защиты выпускной квалификационной работы

Целями подготовки к процедуре защиты и защиты выпускной квалификационной работы являются получение профессиональных умений и навыков в области профессиональной деятельности.

2. Планируемые результаты обучения

Подготовка к процедуре защиты и защита выпускной квалификационной работы направлены на формирование у выпускника способности решать профессиональные задачи в соответствии с ***эксплуатационным*** видом деятельности**.**

Результатом подготовки к процедуре защиты и защиты выпускной квалификационной работы являются сформированные у выпускника следующие компетенции.

ПК-1: Администрирование подсистем защиты информации в операционных системах
Знать:
- архитектуру и принципы построения операционных систем; - программные интерфейсы операционных систем; - виды политик управления доступом и информационными потоками применительно к операционным системам; - архитектуру подсистем защиты информации в операционных системах; - принципы функционирования средств защиты информации в операционных системах, в том числе использующих криптографические алгоритмы; - состав типовых конфигураций программно-аппаратных средств защиты информации; - требования по составу и характеристикам подсистем защиты информации применительно к операционным системам; - порядок реализации методов и средств антивирусной защиты в операционных системах; - программно-аппаратные средства и методы защиты информации в операционных системах; - принципы работы и правила эксплуатации программно-аппаратных средств защиты информации; - нормативные правовые акты в области защиты информации; - руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; - организационные меры по защите информации.
Уметь:

- формулировать политики безопасности операционных систем;

- настраивать политики безопасности операционных систем;

- оценивать угрозы безопасности информации операционных систем;

- противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем;

- выбирать режимы работы программно-аппаратных средств защиты информации в операционных системах;

- настраивать антивирусные средства защиты информации в операционных системах;

- устанавливать обновления программного обеспечения и средств антивирусной защиты;

- проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах;

- производить анализ эффективности программно-аппаратных средств защиты информации в операционных системах;

- оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в операционных системах.

Владеть:

- определением состава применяемых программно-аппаратных средств защиты информации в операционных системах;

- разработкой порядка применения программно-аппаратных средств защиты информации в операционных системах;

- формированием шаблонов установки программно-аппаратных средств защиты информации в операционных системах;

- установкой программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации;

- конфигурированием программно-аппаратных средств защиты информации в операционных системах;

- контролем корректности функционирования программно-аппаратных средств защиты информации в операционных системах;

- управлением антивирусной защитой операционных систем в соответствии с действующими требованиями.

ПК-2: Администрирование программно-аппаратных средств защиты информации в компьютерных сетях

Знать:

- принципы построения компьютерных сетей;

- стек сетевых протоколов операционных систем;

- стек протоколов сетевого оборудования;

- порядок реализации методов и средств межсетевого экранирования;

- принципы функционирования сетевых протоколов, включающих криптографические алгоритмы;

- виды политик управления доступом и информационными потоками в компьютерных сетях;

-источники угроз информационной безопасности в компьютерных сетях и меры по их предотвращению;

- состав типовых конфигураций программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях;

- методы измерений, контроля и технических расчетов характеристик программно-аппаратных средств защиты информации;

- принципы работы и правила эксплуатации эксплуатируемых программно-аппаратных средств защиты информации;

- программно-аппаратные средства и методы защиты информации в компьютерных сетях;

- нормативные правовые акты в области защиты информации;

- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

- организационные меры по защите информации.

Уметь:

- оценивать угрозы безопасности информации в компьютерных сетях;

- настраивать правила фильтрации пакетов в компьютерных сетях;

- обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях;

- конфигурировать и контролировать корректность настройки программно-аппаратных средств защиты информации в компьютерных сетях;

- выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных сетях;

- проводить мониторинг функционирования программно-аппаратных средств защиты информации в компьютерных сетях;

- производить анализ эффективности программно-аппаратных средств защиты информации в компьютерных сетях;

- оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях.

Владеть:

- определением состава применяемых программно-аппаратных средств защиты информации в компьютерных сетях;

- разработкой порядка применения программно-аппаратных средств защиты информации в компьютерных сетях;

- формированием шаблонов конфигурации программно-аппаратных средств защиты информации в компьютерных сетях;

- настройкой программных и аппаратных средств построения компьютерных сетей, использующих криптографическую защиту информации;

- управлением функционированием программно-аппаратных средств защиты информации в компьютерных сетях;

- контролем корректности функционирования программно-аппаратных средств защиты информации в компьютерных сетях;

- управлением средствами межсетевого экранирования в компьютерных сетях в соответствии с действующими требованиями

ПК-3: Администрирование средств защиты информации прикладного и системного программного обеспечения

Знать:

- архитектуру подсистем защиты информации в операционных системах;

- принципы построения систем управления базами данных;

- основные средства и методы анализа программных реализаций;

- принципы построения антивирусного программного обеспечения;

- виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению;

- источники угроз информационной безопасности программного обеспечения и меры по их предотвращению;

- уязвимости используемого программного обеспечения и методы их эксплуатации;

- виды и формы функционирования вредоносного программного обеспечения;

- характерные признаки наличия вредоносного программного обеспечения;

- средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения;

- принципы функционирования программных средств криптографической защиты информации;

- порядок обеспечения безопасности информации при эксплуатации программного обеспечения;

- нормативные правовые акты в области защиты информации;

- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

- организационные меры по защите информации.

Уметь:

- анализировать угрозы безопасности информации программного обеспечения;

- формулировать правила безопасной эксплуатации программного обеспечения;

- обосновывать правила безопасной эксплуатации программного обеспечения;

- анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия;

- производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации;

- осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения;

- определять порядок функционирования программного обеспечения с целью обеспечения защиты информации;

- анализировать эффективность сформулированных требований к встроенным средствам защиты информации программного обеспечения.

Владеть:

- определением порядка установки программного обеспечения с целью соблюдения требований по защите информации;

- контролем над соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение;

- формулированием требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения;

- выполнением работ по обнаружению вредоносного программного обеспечения;

- ликвидацией обнаруженного вредоносного программного обеспечения и последствий его функционирования;

- формулированием требований к встроенным средствам защиты информации программного обеспечения.

3. Место подготовки к процедуре защиты и защиты выпускной квалификационной работы в структуре образовательной программы

Требования к предварительной подготовке обучающегося (предшествующие дисциплины)
Подготовка к процедуре защиты и защита выпускной квалификационной работы являются логическим продолжением изучения всех дисциплин направления 10.03.01, знание которых в объеме требований образовательной программы является необходимым.

4. Содержание подготовки к процедуре защиты и защиты выпускной квалификационной работы (ВКР)

Требования к ВКР и порядку их выполнения

4.1. К видам аттестационных испытаний ГИА для выпускников СКФ МТУСИ по направлению подготовки 10.03.01. «Информационная безопасность», профиль «Безопасность компьютерных систем» относится защита выпускной квалификационной работы (ВКР).

4.2. ВКР выполняются в форме бакалаврской работы объемом 50-80 страниц в соответствии с требованиями ГОСТ 2.105-95, ЕСКД, ЕСПД .

4.3. Сроки выполнения выпускных квалификационных работ в обязательном порядке доводятся до сведения студентов не позднее, чем за полгода до начала ГИА.

4.4. Завершенные ВКР подлежат внешнему или межкафедральному рецензированию.

5. Перечень тем ВКР, предлагаемых выпускникам

1. Разработка системы технической защиты информационной системы войсковой части
2. Разработка системы защиты информации ЛВС Руднянского ЛТЦ Волгоградского филиала МРФ «Юг» ПАО «Ростелеком»
3. Модернизация системы защиты локальной вычислительной сети типографии
4. Разработка защиты локальной вычислительной сети ООО «Шахтоуправление «Садкинское» г. Белая Калитва
5. Разработка системы защиты персональных данных в информационной системе фонда ОСПО ГУ МВД по Ростовской области
6. Усиление информационной безопасности офиса контактного центра Теле2-Ростов за счет инженерно-технической защиты
7. Модернизация защиты локальной вычислительной сети ООО «Вилмари»
8. Разработка защиты сети беспроводного доступа на основе технологии LTE в Крыловском районе Краснодарского края силами ЛТЦ Крыловского района ПАО «Ростелеком»
9. Разработка системы защиты от несанкционированного доступа в ЛВС ООО «Престиж-Интернет»
10. Разработка программно-технического комплекса защиты информационной системы отделений ПАО «Сбербанк РФ» от несанкционированного доступа
11. Разработка системы защиты видеообмена в локальной вычислительной сети МБУЗ КДЦ «Здоровье» для проведения видеоконференций
12. Развертывание WIMAX-сетей в сельских районах
13. Программа мониторинга действий пользователей в компьютерной сети
14. Разработка сайта «Молодежное самоуправление ВУЗа»

15. Программно-аппаратный комплекс архитектуры Advanced RISC Machine домашнего медиа-сервера с низким энергопотреблением

16. Разработка модулей лабораторного практикума и тестов электронного пособия по дисциплине «Технологии программирования»

17. Разработка интерактивного компьютерного лабораторного практикума по дисциплине «Инженерная и компьютерная графика»

18. Проектирование защиты проводной локальной вычислительной сети для филиала №3 государственного учреждения Ростовского регионального отделения фонда социального страхования РФ

19. Разработка программного обеспечения для имитозащиты и контроля целостности информации с использованием криптографической хеш-функции

20. Разработка электронной системы тестирования знаний об элементах памяти цифровых устройств

21. Разработка управляющего и лекционного модулей электронного пособия по дисциплине «Технологии программирования»

22. Разработка лабораторного практикума по дисциплине «ЭВМ и периферийные устройства»

23. Разработка электронного пособия по объектно-ориентированному программированию

6. Образец задания на ВКР

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
СЕВЕРО-КАВКАЗСКИЙ ФИЛИАЛ
ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО
БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ»

Кафедра «Информатика и вычислительная техника » (ИВТ)

Утверждаю
Зав. кафедрой ИВТ СКФ МТУСИ
_____ С.В. Соколов
«____» _____ 20____ г.

ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Студенту Боренкову Алексею Сергеевичу группы _Д-41

Направление подготовки **–10.03.01 Информационная безопасность**
Профиль **Безопасность компьютерных систем**

Тема выпускной квалификационной работы: **Модернизация системы защиты локальной вычислительной сети ООО «Современный Образ», г. Воронеж**

утверждена приказом директора филиала_____

№	Содержание	Объём работы и срок исполнения
1.	Исходные данные к ВКР 1.1. Основные виды деятельности ООО «Современный Образ». 1.2. Организационная и техническая защита структуры ЛВС ООО «Современный Образ». 1.3. План размещения аппаратуры и рабочих мест ЛВС в помещениях офиса ООО «Современный Образ».	
2.	Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов): 2.1. Введение. 2.2. Технология построения и функционирования системы защиты ЛВС ООО «Современный Образ». 2.2.1. Организационно-штатная структура ООО «Современный Образ» и особенности системы защиты его ЛВС. 2..2.1.1. Основные цели модернизации системы защиты ЛВС ООО «Современный Образ» 2.2.2. Анализ существующих методов проектирования систем защиты ЛВС. 2.3. Выбор сетевой архитектуры и топологии модернизированной ЛВС ООО «Современный Образ». 2.3.1. Анализ современных методов построения ЛВС. 2.3.1.1. Ethernet. 2.3.1.2. Fast Ethernet 100 Мбит/с. 2.3.1.3. Wi-Fi-сети. 2.3.1.4. WiMAX-сеть. 2.3.2. Понятие виртуальной локальной сети. 2.3.2.1. Обзор технологии виртуальных локальных сетей в ЛВС. 2.3.3. Паспортизация рабочих мест и серверов ЛВС. 2.3.4. Выбор топологии, сетевой технологии, архитектуры и	1%, 7.05.23 33%, 20.05.23 33%, 5.06.23

	структуры системы защиты ЛВС. 2.4. Разработка проекта модернизации системы защиты ЛВС ООО «Современный Образ». 2.4.1. Выбор оборудования. 2.4.1.1. Выбор рабочих станций. 2.4.1.2. Выбор точки доступа. 2.4.1.3. Выбор коммутатора. 2.4.1.4. Выбор сетевой операционной системы. 2.4.1.5. Выбор антивирусной программы. 2.4.1.6. Выбор программы резервного архивирования данных. 2.4.2. Организационная и техническая структура ООО «Современный Образ» и системы защиты его ЛВС после модернизации. 2.4.3. Построение математической модели модернизированной системы защиты ЛВС. 2.4.4. Построение имитационной модели системы защиты модернизированной ЛВС.	32%, 23.06.23
3 4	Вопросы конструктивных разработок – не запланированы Заключение.	1%, 25.06.23

2. Перечень графического материала, выносимого на защиту:

1. Организационно-штатная структура предприятия ООО «Современный Образ».

2. Обобщенная структура существующей системы защиты ЛВС до модернизации.
3. Размещение аппаратуры системы защиты ЛВС в помещениях офиса ООО «Современный Образ».

4. Примеры построения различных видов систем защиты ЛВС.
5. Организационно-штатная структура предприятия ООО «Современный Образ» после модернизации.

6. Обобщенная структура системы защиты ЛВС ООО «Современный Образ» после модернизации.

3. Срок сдачи студентом законченной ВКР ___25 июня 2023 г.

4. Дата выдачи задания ____25 января 2023 г.

Руководитель

Чикалов А.Н., доцент кафедры ИВТ, к. т. н. _____

(фамилия и инициалы, должность, ученая степень) (подпись руководителя)

Задание принял к исполнению _____

(дата и подпись студента)

Примечание. Настоящее задание прилагается к пояснительной записке законченной бакалаврской работы и представляется в ГАК.

7. Требования к ВКР

7.1 Выпускная квалификационная работа бакалавра должна представлять собой самостоятельную и логически завершенную проектную работу, связанную с разработкой теоретических вопросов, с экспериментальными исследованиями или с решением задач прикладного характера, являющихся, по возможности, частью научно-исследовательских работ, выполняемых выпускающей кафедрой.

7.2 Выпускная работа бакалавра выполняется на базе теоретических знаний и практических навыков, полученных студентом в период обучения.

7.3 Темы выпускных работ бакалавров разрабатываются выпускающей кафедрой и утверждаются приказом директора филиала. Темы бакалаврских работ должны по проблематике соответствовать профилям, реализуемым в филиале по направлению 10.03.01. "Информационная безопасность".

7.4 Для руководства выпускной работой по представлению выпускающей кафедры назначается руководитель, как правило, из числа преподавателей кафедры. По предложению руководителя выпускной работы кафедре, в случае необходимости, предоставляется право приглашать консультантов по отдельным разделам выпускной работы из числа сотрудников других кафедр. Руководителями выпускной работы могут быть также специалисты из других профильных учреждений и предприятий.

7.5 Содержание выпускной квалификационной работы бакалавра должно учитывать требования ФГОС ВО к профессиональной подготовленности студента и включать в себя:

- обоснование выбора объекта и постановку задачи проектирования, выполненные на основе обзора научно-технической литературы, в том числе с учетом периодических научных и технических изданий;

- обоснование инфокоммуникационных технологий и технологий информационной безопасности, на базе которых предполагается реализация ВКР;

- расчет параметров проектируемой системы защиты сети или средства;

- схемы проектируемой системы защиты сети или инфокоммуникационной системы;

- вопросы конструктивных разработок (при необходимости);

- выводы и рекомендации;

- список использованных источников.

7.6 Законченная и оформленная выпускная квалификационная бакалаврская работа должна соответствовать следующим требованиям:

- общий объем пояснительной записки должен быть не менее 50 страниц текста, сама записка оформлена в соответствии с требованиями, предъявляемыми к технической документации;

- цифровые, табличные и прочие иллюстративные материалы могут быть вынесены в приложения;

- титульный лист ВКР и задание на работу должны иметь подписи студента, руководителя работы, заведующего выпускающей кафедрой и рецензента.

7.7 Завершенная работа представляется на рецензирование. Список рецензентов представляется выпускающей кафедрой и утверждается директором филиала.

7.8 Законченная ВКР с отзывом и рецензией представляется на допуск к защите заведующему выпускающей кафедрой.

8. Критерии оценки государственной итоговой аттестации бакалавров

8.1. Конечными результатами обучения, выявляемыми в ходе защиты ВКР, являются сформированные компетенции, оцениваемые по когнитивным дескрипторам: «знать», «уметь», «владеть». Формирование этих дескрипторов происходит в течение всего периода овладения ОП поэтапно в рамках различного вида занятий и самостоятельной работы.

Оценка когнитивных дескрипторов осуществляется по трем уровням: уровень 1 – соответствует традиционной оценке «удовлетворительно»; уровень 2 — «хорошо» и уровень 3 — «отлично».

8.2. Сформированные дескрипторы оцениваются по единой форме контроля: итоговый контроль.

8.3. Итоговый контроль осуществляется на защите выпускной квалификационной работы. По результатам контроля выставляются оценки по четырехбалльной системе: «неудовлетворительно», «удовлетворительно», «хорошо» и «отлично».

8.4. Итоговая оценка складывается из трех составляющих – оценки выполнения задания на

ВКР, оценки рецензента и оценки качества защиты.

8.5. Критерии и оценки выполнения задания по ВКР приведены в таблице 8.1.

Таблица 8.1

Уровень	**Критерии выполнения задания на ВКР**	**Оценка**
Недостаточный	Имеет представление о содержании ВКР, но не знает основные методы, к которым относится задание, не способен выполнить задание с очевидным решением, не владеет навыками оформления полученных результатов	Неудовлетворительно
Пороговый	Знает и воспроизводит основные положения ВКР в соответствии с заданием, применяет стандартные методы для выполнения всех пунктов задания	Удовлетворительно
Базовый	Знает, понимает основные положения ВКР, демонстрирует умение применять свои знания для выполнения пунктов задания, в которых нет явно указанных способов решения. Анализирует полученные результаты, делает правильные выводы	Хорошо
Высокий	Знает, понимает основные положения ВКР, демонстрирует умение применять свои знания для выполнения пунктов задания, в котором нет явно указанных способов решения. Анализирует полученные результаты, делает правильные выводы, сводит их в единую систему, способен выдвинуть идею, способен создавать проектные решения с использованием инновационных и нестандартных методов	Отлично

8.6. Критерии и оценки рецензирования ВКР.

Рецензент должен чётко формулировать замечания и вопросы, желательно со ссылками на работу (можно на конкретные страницы работы), на исследования и фактические данные, которые не учёл автор. Кроме того, рецензент оценивает:

- соответствие работы заданию на ВКР;
- соответствие тематики работы студента направлению подготовки 10.03.01 "Информационная безопасность", профиль "Безопасность компьютерных систем";
- актуальность тематики работы;
- соответствие оформления работы установленным требованиям;
- возможность реализации результатов работы;
- умение студента решать практические задачи по проектированию систем защиты вычислительных машин, комплексов, систем и сетей;
- достоинства и недостатки работы;

- общую оценку работы и возможность присвоения выпускнику квалификации «бакалавр» по направлению подготовки 10.03.01 "Информационная безопасность", профиль "Безопасность компьютерных систем".

Оценка 5 ставится, если выполнены все требования к подготовке и оформлению ВКР, корректно сформулирована задача и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую задачу и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, корректно рассчитаны технические параметры проектируемой сети, комплекса или системы.

Оценка 4 – основные требования к ВКР выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём ВКР; имеются упущения в оформлении.

Оценка 3 – имеются существенные отступления от требований к ВКР. В частности: тема освещена лишь частично; допущены незначительные ошибки в содержании ВКР или при выполнении расчетов; отсутствуют выводы.

Оценка 2 – тема ВКР не раскрыта, обнаруживается существенное непонимание задачи.

8.7. Критерии и оценки качества защиты ВКР приведены в таблице 8.2

Таблица 8.2

№п/п	**Оцениваемые параметры**	**Оценка в баллах**
1.	Качество презентации и доклада: - содержит достаточный объем иллюстративного материала, соответствует заданию на ВКР; - четко выстроен; - рассказывается технически грамотным языком; - зачитывается.	 1 2 2 0
2.	Использование демонстрационного материала: - разнообразный демонстрационный материал, четкие комментарии; - демонстрационный материал хорошо оформлен, но есть неточности в комментариях; - представленный демонстрационный материал подобран или оформлен плохо, неграмотно прокомментирован.	 3 2 0
3.	Качество ответов на вопросы: - отвечает на вопросы; - не может ответить на большинство вопросов; - не может четко ответить на вопросы.	 3 2 0

4.	Владение научным и специальным аппаратом: - владеет специальным аппаратом; - использованы общенаучные и специальные термины; - владеет базовым аппаратом.	 3 2 0
5.	Наличие выводов: - четкие, аргументированные; - нечеткие; - имеются, но не доказаны.	 3 2 0

8.8. Комплексная оценка ВКР

Комплексная оценка ВКР формируется из трех оценок – оценки выполнения задания, оценки качества защиты и оценки рецензента, как среднее арифметическое, округленное в большую сторону. Оценка выполнения задания указывается в отзыве руководителя, но может быть скорректирована с учетом мнения государственной экзаменационной комиссии. Оценка качества защиты формируется голосами членов ГЭК, при этом голос председателя ГЭК является решающим при возникновении спорных вопросов.

9. Оценочные материалы для проведения государственной итоговой аттестации

Оценочные материалы : ВКР, контрольные вопросы при защите ВКР.

Контрольные вопросы:

1. Нормативная и правовая документация в области ИБ (ПК-2, ПК-3)

1) Перечислить основные руководящие документы по организации деятельности IT-предприятия.
2) Что определяет федеральный закон "О персональных данных"?
3) Что определяют основные руководящие документы в области IT-технологий?

2. Требования по правилам и мерам безопасности (ПК-2, ПК-3)

1) Перечислите основные опасные факторы при эксплуатации IT-оборудования.
2) Перечислите общие требования безопасности.
3) Перечислите опасные факторы воздействия электрического тока.
4) Перечислите основные документы, в которых определены требования безопасности.

3. Состав оборудования и правила эксплуатации (ПК-1)

1) Охарактеризовать надёжность используемого в ВКР оборудования.
2) Основные технические характеристики систем защиты инфокоммуникационного оборудования.

3) Информационные принципы функционирования систем защиты IT-оборудования.

4) Пояснить общую структурную схему системы защиты инфокоммуникационной сети IT-предприятия.
5) Охарактеризовать используемую для построения системы защиты инфокоммуникационной сети IT-предприятия технологию передачи данных.
6) Охарактеризовать возможные технологии для построения альтернативной системы защиты сети.
7) Описать перспективы развития систем защиты инфокоммуникационных сетей IT-предприятия.
8) Оценить возможность масштабирования и расширения существующих систем защиты инфокоммуникационных сетей IT-предприятия.
9) Охарактеризовать надёжность системы защиты сетевой структуры, используемой в ВКР.

4. Организация рабочего места (ПК-1,ПК-2)
1) Опишите состав типового рабочего места IT-предприятия.
2) Требования к освещённости рабочего помещения.
3) Требования к вентиляции помещения.
4) Требования к размещению средств вычислительной техники на рабочем месте.

5. Правила размещения инфокоммуникационного оборудования (ПК-2, ПК-3)
1) Влияние на размещение инфокоммуникационного оборудования системы отопления.
2) Влияние на размещение инфокоммуникационного оборудования системы водоснабжения.
3) Влияние на размещение инфокоммуникационного оборудования системы электропитания.
4) Влияние на размещение инфокоммуникационного оборудования конфигурации сооружения.
5) Какие средства могут быть применены для защиты инфокоммуникационных устройств при их размещении в помещениях организации?
6) Возможна ли установка инфокоммуникационного оборудования в помещениях организации без дополнительных средств защиты?

6. Правила проведения технического обслуживания и устранения неисправностей (ПК-1, ПК-3)
1) Виды технического обслуживания, предусмотренные для системы защиты инфокоммуникационного оборудования.
2) Пояснить состав и правила выполнения сезонного технического обслуживания.
3) Пояснить порядок проведения внешнего осмотра системы защиты IT-оборудования.
4) Для чего необходимо проводить техническое обслуживание?
5) Перечислить средства для проведения технического обслуживания.
6) Какие существуют методы поиска неисправностей для IT-оборудования?
7) Какие существуют методы устранения неисправностей?
8) Какие методы устранения неисправностей применяются для системы защиты IT-оборудования?
9) Каким образом организуется проведение текущего ремонта IT-оборудования?
10) Какие методы организации текущего ремонта Вам известны?

11) На основании каких документов производится техническое обслуживание системы защиты?
12) Какие негативные последствия может вызвать неправильное проведение технического обслуживания системы защиты IT-оборудования?
13) Влияет ли качество проведения технического обслуживания на гарантийные обязательства производителя?
14) Как осуществляется проверка соответствия параметров среды в местах эксплуатации IT-оборудования и какова её периодичность?

7. Ведение учётно-отчётной документации (ПК-2, ПК-3)
1) Перечислите виды учетно-отчётной документации, ведущейся в организации.
2) В каких документах отражается учёт IT-оборудования?
3) Какие документы оформляются при проведении технического обслуживания?
4) Какие документы оформляются при выявлении неисправности в негарантийный период эксплуатации IT-оборудования?
5) Какие документы оформляются при возникновении неисправности в гарантийный период эксплуатации?
6) Какие документы оформляются при необходимости закупки нового IT-оборудования?
7) Какие документы оформляются при необходимости закупки комплектующих и запасных частей для ремонта системы защиты IT-оборудования?

10. Учебно-методическое и информационное обеспечение ВКР

10.1. Рекомендуемая литература				
10.1.1. Основная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л1.1		Эксплуатационная документация на используемое оборудование системы защиты компьютерной системы.	Производитель оборудования	
Л1.2		Нормативные документы по организации и контролю обеспечения безопасной эксплуатации оборудования системы защиты компьютерной системы	Производитель оборудования	
Л1.3		Нормативные документы по организации и техническому обслуживанию оборудования системы защиты компьютерной системы	Производитель оборудования	
10.1.2. Дополнительная литература				
Код	**Авторы, составители**	**Заглавие**	**Издательство, год**	**Кол.**
Л2.1		Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015)		Э1
Л2.2		Федеральный закон от 06.04.2011 N 63-ФЗ		Э2

		(ред. от 30.12.2015) "Об электронной подписи"		
Л2.3		Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 13.07.2015) "О связи" (с изм. и доп., вступ. в силу с 10.01.2016)		Э3
Л2.4		Федеральный закон от 17 июля 1999 г. N 176-ФЗ "О почтовой связи" (7 июля 2003 г., 22 августа, 29 декабря 2004 г., 26 июня 2007 г., 14, 23 июля 2008 г., 28 июня 2009 г., 6 декабря 2011 г., 2 марта 2016 г.)		Э4
Л2.5		Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 10.01.2016)		Э5
Л2.6		Закон РФ от 21 июля 1993 г. N 5485-I "О государственной тайне" (с изменениями и дополнениями от 6 октября 1997 г., 30 июня, 11 ноября 2003 г., 29 июня, 22 августа 2004 г., 1 декабря 2007 г., 18 июля 2009 г., 15 ноября 2010 г., 18, 19 июля, 8 ноября 2011 г., 21 декабря 2013 г., 8 марта 2015 г.)		Э6
Л2.7		Указ Президента РФ от 17 марта 2008 г. N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" (с изменениями и дополнениями от 21 октября 2008 г., 14 января 2011 г., 1, 25 июля 2014 г., 22 мая 2015 г.		Э7
Л2.8		Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"		Э8
Л2.9		ГОСТ 34.936-91 Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом к среде		Э9
Л2.10		ГОСТ Р 53724-2009 Качество услуг связи. Общие положения		Э10
10.1.3. Учебно-методическое обеспечение для самостоятельной работы обучающихся				

Код	Авторы, составители	Заглавие	Издатель-ство, год	Кол.
Л3.1	Жуковский А.Г., Манин А.А.	Руководство по подготовке курсовых работ (проектов) и выпускных квалификационных работ	РнД: СКФ МТУСИ, 2017	70
10.2. Электронные образовательные ресурсы				
Э1	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=178749			
Э2	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=191956			
Э3	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=201564			
Э4	http://www.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=201192			
Э5	http://ivo.garant.ru/#/document/12148555/paragraph/3471:2			
Э6	http://ivo.garant.ru/#/document/10102673/paragraph/51952:4			
Э7	http://ivo.garant.ru/#/document/192944/paragraph/8911:2			
Э8	http://ivo.garant.ru/#/document/70391358/paragraph/1:4			
Э9	http://www.infosait.ru/Pages_gost/19099.htm			
Э10	http://docs.cntd.ru/document/gost-r-53724-2009			
10.3. Программное обеспечение				
П.1	OS Windows XP - 7			
П.2	Пакет Microsoft Office			
П.3	Специализированное ПО для моделирования систем защиты компьютерных и инфокоммуникационных систем			

10.4 Перечень информационных технологий, используемых при проведении Государственной итоговой аттестации

Проведение Государственной итоговой аттестации неразрывно связано с применением информационных технологий. К таким технологиям можно отнести:

- использование средств компьютерной техники и программного обеспечения для поиска необходимой технической, научно-технической и правовой информации;
- использование средств вычислительной техники и офисного программного обеспечения для составления и оформления ВКР;
- использование специализированных программ для ЭВМ, применяемых при выполнении ВКР.

11. Методические указания по проведению ГИА

11.1. Сроки проведения ГИА определяются учебным планом направления подготовки 10.03.01 "Информационная безопасность", профиль "Безопасность компьютерных систем". Расписание работы государственных экзаменационных комиссий (ГЭК) в процессе ГИА составляется деканом факультета, утверждается директором СКФ МТУСИ и доводится до сведения студентов не позднее, чем за две недели до ее начала.

В расписании указываются - дата, время начала работы ГЭК, аудитория, состав ГЭК и список студентов с распределением их по дням защиты.

11.2. В соответствии со сроками проведения ГИА выпускникам создаются условия для подготовки: организуются консультации, обзорные лекции, предусмотренные учебной нагрузкой.

11.3. Результаты ГИА выражаются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в день проведения защиты ВКР после оформления протоколов заседания ГЭК.

11.4. Защиты выпускных квалификационных работ проводятся на открытых заседаниях ГЭК с участием не менее четырех членов комиссии, включая председателя. Решения принимаются на закрытых заседаниях простым большинством голосов, голос председателя в спорных случаях является решающим. Отзывы руководителя и рецензента учитываются при обсуждении оценок.

11.5. Решение о присвоении квалификации и выдаче диплома государственного образца о высшем образовании выпускнику СКФ МТУСИ принимает ГЭК при условии успешного прохождения всех видов аттестационных испытаний, включенных в ГИА по направлению подготовки 10.03.01 "Информационная безопасность", профиль "Безопасность компьютерных систем" и оформленных протоколами ГЭК.

11.6. Студенты, получившие неудовлетворительную оценку в ходе аттестационных испытаний, отчисляются из СКФ МТУСИ с выдачей им справки об обучении.

11.7. По окончании ГИА председатель ГЭК составляет отчет о работе ГЭК, в котором указываются:

- номер и дата приказа ректора МТУСИ об утверждении ГЭК;
- состав ГЭК в соответствии с приказом ректора;
- результаты защиты выпускных квалификационных работ;
- характеристика уровня подготовки выпускников, соответствие объема и глубины подготовки требованиям ФГОС ВО направления подготовки 10.03.01 "Информационная безопасность", профиль "Безопасность компьютерных систем";
- общая комплексная оценка качества знаний выпускников;
- замечания и предложения по оптимизации процедуры и содержания ГИА, по совершенствованию качества подготовки выпускников.

11.8. Отчет о работе ГЭК в течение 10 дней представляется заместителю директора по учебно-воспитательной работе СКФ МТУСИ.

11.9. Результаты ГИА обсуждаются на заседании Ученого совета СКФ МТУСИ и не позднее, чем через 2 месяца после завершения ГИА, отчет о работе ГЭК по направлению подготовки 10.03.01 "Информационная безопасность", профиль "Безопасность компьютерных систем" направляется ректору МТУСИ.

11.10. Протоколы аттестационных испытаний ГИА выпускников хранятся в архиве СКФ МТУСИ.

Форма протокола заседания ГЭК

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени
федерального государственного бюджетного образовательного учреждения
высшего образования
«Московский технический университет связи и информатики»

ПРОТОКОЛ №

Заседания государственной экзаменационной комиссии (ГЭК)

по защите выпускной квалификационной работы

Выпускник _____
(Фамилия, имя и отчество)

На тему _____
_____
_____

Форма выполнения выпускной квалификационной работы _____
_____
(ВКР бакалавра, дипломный проект, дипломная работа, магистерская диссертация)

Специальность (направление) _____
(Шифр специальности, направления)

_____

Присутствовали:

Председатель ГЭК _____
Члены ГЭК
_____
_____

Приказ ректора МТУСИ № 15 - 0 от 22.01.2023г.

Выпускная квалификационная работа выполнена

Под руководством _____
(Фамилия и инициалы руководителя)

В государственную экзаменационную комиссию представлены следующие материалы:

1. Справка деканата заочного факультета от _____ 2023
   о сданных обучающимся _____ экзаменах и зачетах
   и о выполнении им требований учебного плана.
2. Расчетно – пояснительная записка на _____ страницах.
3. Отзыв руководителя _____

(Фамилия, имя и отчество)

4. Рецензия _____

(Фамилия, имя и отчество)

5. Протокол № от заседания ГЭК по приему государственного экзамена

После сообщения о выполненной выпускной квалификационной работе
(в течение _____ минут) студенту (ке) заданы следующие вопросы:

1. _____

(Фамилия и инициалы лица, задавшего вопрос, содержание вопроса)

_____

2. _____

_____

3. _____

_____

Общая характеристика ответов студента на заданные вопросы и замечания рецензента

_____

_____

Оценка руководителя ВКР _____

Оценка рецензента ВКР _____

Решение государственной экзаменационной комиссии

1. Признать, что студент (ка) _____

(Фамилия, имя и отчество)

защитил (а) выпускную квалификационную работу с оценкой _____

2. Отметить, что _____

_____

_____

3. Присвоить _____

квалификацию (степень) _____

по специальности (направлению)_____

профиль _____

4. Выдать диплом _____

(с указанием диплома с отличием)

5. Мнение членов государственной экзаменационной комиссии:

об уровне подготовленности обучающегося _____

_____

недостатки в теоретической и практической подготовке _____

_____

Председатель государственной экзаменационной комиссии

_____ _____

(Ф.И.О.) (подпись)

Секретарь государственной экзаменационной комиссии

_____ _____

(Ф.И..О.) (подпись)

Примерный календарный график выполнения и защиты ВКР

СОГЛАСОВАНО
Зам. директора по УВР
_____ А.Г. Жуковский
« ___ » « _____ » 2023 г.

УТВЕРЖДАЮ
Директор СКФ МТУСИ
_____ Д.Н.Карасев
«_____» «_____» 2023 г.

График подготовки защиты ВКР
выпускников филиала 2023 года и сроки вручения дипломов
выпускникам очного и заочного факультетов

Этапы	Сроки	Мероприятия	Контингент
1	до 11.02.2023	Ознакомление под роспись выпускников филиала с черновым вариантом приложения на начало последней сессии	все 4 курсы ОФ, специалисты ФИК по УМР
2	до 18.02.2023	Окончательное заполнение приложений к дипломам бакалавров	все 4 курсы ОФ, специалисты ФИК по УМР
3	до 21.02.23	Получение бланков дипломов и приложений к дипломам бакалавров	отдел кадров СКФ
4	до 25.02.2023	Подготовка шаблонов 4 типовых приложений к дипломам бакалавров в электронном виде с помощью программы Кибер ДИПЛОМ 2014	все 4 курсы ОФ, вспомогательный персонал, зам. декана ФИК
5	до 29.02.2023	Получение приказов по составам председателей ГЭК и членов ГЭК, приглашение членов ГЭК для участия в заседаниях комиссий	директор СКФ, декан ФИК, зав. выпускающими кафедрами СКФ
6	до 04.03.23	Направление приглашений иногородним членам ГЭК для участия в проведении защит выпускников филиала в марте	зав. кафедрами, декан ФИК
7	до 05.03.2023	Контроль представления ВКР дипломниками	зав. кафедрами, деканат ФИК
8	до 05.03.2023	Заполнение приложений к дипломам бакалавров	все 4 курсы ОФ,

		в электронном виде (без итогов защит)	вспомогательный персонал
9	до 14.03.2023	Распечатка и проверка набранных приложений к дипломам бакалавров	вспомогательный персонал, специалисты ФИК по УМР, зам. декана ФИК
10	до 20.03.2023	Ознакомление под роспись выпускников филиала с черновым вариантом приложения на начало последней сессии	вспомогательный персонал, зам. декана ФИК
11	14.03 – 18.03. 29.03 – 31.03.23	Проведение защит выпускников-бакалавров 5 курсов	зав. выпускающими кафедрами СКФ, деканат ФИК
12	21.03 – 31.03.23 02.04. – 08.04.23	Подготовка и передача результатов защит и учебных дел бакалавров 5 курсов в отдел кадров СКФ	специалисты ФИК по УМР, декан ФИК
13	до 01.04.2023	Подготовка приказов об отчислении с 21.04.2023 выпускников 5 курсов и передача их в ОК СКФ	специалисты ФИК по УМР, декан ФИК
14	04.04 – 08.04.23	Занесение результатов защит в программу и печать дипломов	ОК
15	11.04 – 14.04.23	Подготовка копий дипломов, заполнение журналов и актов	ОК
16	до 14.04.2023	Корректировка, распечатка приложений к дипломам бакалавров	специалисты ФИК по УМР, зам. декана ФИК, вспомогательный персонал
17	до 16.04.2023	Оформление приложений к дипломам бакалавров и передача их в отдел кадров СКФ	вспомогательный персонал, специалисты ФИК по УМР, зам. декана ФИК
18	до 22.04.2023	Направление приглашений иногородним членам ГЭК для участия в проведении вручения дипломов выпускников филиала	зав. кафедрами, декан ФИК
19	15.04 – 19.04.23	Подписание дипломов и их копий у председателей ГЭК. Прием приложений к дипломам от деканата и внесение данных в журнал выдачи дипломов	ОК
20	до 21.04.2023	Подготовка шаблонов направлений в электронном виде с помощью программы Кибер ДИПЛОМ 2014	вспомогательный персонал, зам. декана ФИК
21	19.04 – 28.04.23	Подписание дипломов бакалавров в МТУСИ	ОК
22	до 23.04.2023	Подготовка к торжественному вручению дипломов выпускникам, аренда помещения и подготовка его к встрече, приглашение гостей	ОК, зам. директора по УВР, ФИК
23	до 29.04.23	Набор и распечатка черновиков приложений к дипломам бакалавров	вспомогательный персонал, зам. декана ФИК

24	до 29.04.23	Контроль представления ВКР дипломниками ОФ	зав. кафедрами, деканат ФИК
25	30.04.23	Вручение дипломов бакалавров выпускникам 5 курсов	ОК
26	до 16.05.23	Контроль представления выпускниками законченных ВКР	зав. кафедрами, деканат ФИК
27	до 20.05.23	Работа с выпускниками по завершению выполнения ими ВКР и подготовке их к защите	зав. кафедрами, деканат ФИК
28	до 20.05.23	Направление приглашений иногородним членам ГЭК для участия в проведении защит выпускников филиала в мае-июне	зав. кафедрами, деканат ФИК
29	до 23.05.23	Заполнение приложений к дипломам бакалавров в электронном виде (без итогов защит)	вспомогательный персонал, зам. декана ФИК
30	до 28.05.23	Распечатка и проверка набранных приложений к дипломам бакалавров	вспомогательный персонал, зам. декана ФИК
31	до 31.05.23	Проведение междисциплинарного тестирования и сдачи государственного экзамена	зав. кафедрами, деканат ФИК
32	26.05 – 18.06.23	Размещение и организация пребывания в г. Ростове-на-Дону иногородних членов ГЭК	зав. кафедрами, декан ФИК
33	20.06.- 30.06.23	Организация и проведение защиты ВКР выпускниками ОФ филиала	зав. кафедрами, деканат ФИК
34	до 11.07.23	Передача в отдел кадров СКФ приложений к дипломам выпускников-бакалавров ОФ	деканат и декан ФИК
35	с 03.06. по 30.06. с 04.07. по 11.07.23	Внесение данных по результатам защит в программу печати дипломов.	ОК
36	С 12.07. по 15.07.23	Подготовка копий дипломов, заполнение журналов и актов	ОК
37	до 16.07.23	Передача в отдел кадров СКФ приложений к дипломам выпускников ОФ	деканат и декан ФИК
38	до 16.07.23	Направление приглашений иногородним членам ГЭК для участия во вручении дипломов выпускников филиала в июле	зав. кафедрами, декан ФИК
39	с 15. 07. по 18.07.23	Подписание дипломов и копий у председателей ГЭК. Приём документов деканата, внесение последних данных с вкладышей в журнал выдачи дипломов	ОК

40	до 18.07.2023.	Прошивка всех дел	ОК
41	22. – 23.07.23	Организация доставки и размещения на арендуемой территории имущества и документации филиала, необходимой для проведения торжественного собрания	зам. директора по АХР, отдел кадров, деканат ФИК
42	23.07.23	Торжественное собрание с выпускниками филиала 2023 года и вручение им дипломов бакалавров	приглашенные гости, администрация, преподаватели и сотрудники СКФ
43	23.07.2023	Организация возвращения всего имущества и документации филиала после торжественного собрания в СКФ	зам. директора по АХР, отдел кадров, деканат ФИК

Декан факультета ИК Ефимов С.В.

Начальник ОК Шустова В.В.

Зам. директора по АХР Гуринович С.М.

Председатель профкома СКФ Янкина Н.А.

Зав. кафедрой ИТСС Юхнов В.И.

Зав. кафедрой ИВТ Соколов С.В.

12. Методика проверки ВКР на оригинальность

12.1. Проверка текста пояснительной записки ВКР на оригинальность выполняется посредством СПО Etxt Антиплагиат.

12.2. Отчет о проверке в формате PDF в электронном виде прилагается к PDF – файлу пояснительной записки ВКР.

13. Материально-техническое обеспечение ГИА

13.1 МТО выполнения ВКР
Аудитории СКФ МТУСИ с измерительно-экспериментальным оборудованием и рабочими местами, оборудованными ПК, ноутбуками, интерактивными досками и мультимедийными проекторами
13.2 МТО защиты ВКР
Аудитория СКФ МТУСИ, оборудованная ПК, ноутбуками и мультимедийными проекторами

Дополнения и изменения в рабочей программе