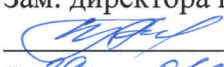


МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ
И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
Северо-Кавказский филиал
ордена Трудового Красного Знамени федерального государственного
бюджетного образовательного учреждения высшего образования
«Московский технический университет связи и информатики»

Утверждаю
Зам. директора по УВР
 Н.А. Андреева
« 29 » 04 2024 г.

**Подготовка к процедуре защиты и защита
выпускной квалификационной работы Б3.01
рабочая программа дисциплины**

Кафедра: **Информационной безопасности**

Направление подготовки: **10.03.01 Информационная безопасность**

Профиль: **Безопасность компьютерных систем (по отрасли или в сфере профессиональ-
ной деятельности)**

Формы обучения: **очная**

Распределение часов дисциплины по семестрам (для очной формы обучения (ОФО))

Объем и структура государственной итоговой аттестации		
Вид учебной работы	ОФО	
	ЗЕ	часов
Общая трудоемкость государственной итоговой аттестации	6	216
Самостоятельная работа		196
Контактная работа		20

Программу составил:

заведующий кафедрой ИБ, к.т.н., доцент Маршаков Д.В.

Рецензенты:

*ведущий научный сотрудник «Ростовский-на-Дону НИИ радиосвязи»,
д.т.н., доцент Погорелов В.А.*

Рабочая программа дисциплины

«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 2020 г. N 1427.

Составлена на основании учебного плана

направления 10.03.01 «Информационная безопасность», профиля «Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)», одобренного Учёным советом СКФ МТУСИ, протокол № 9 от 22.04.2024, и утвержденного директором СКФ МТУСИ 22.04.2024 г.

Рассмотрена и одобрена на заседании кафедры

«Информационная безопасность»

Протокол от «24» апреля 2024 г. № 9

Зав. кафедрой _____  Д.В. Маршаков

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

Утверждаю

Зам. директора по УВР _____

- _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _____ 20__ г. № _

Зав. кафедрой _____

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

Утверждаю

Зам. директора по УВР _____

- _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _____ 20__ г. № _

Зав. кафедрой _____

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

Утверждаю

Зам. директора по УВР _____

- _____ 20__ г.

Рабочая программа пересмотрена, обсуждена и одобрена на заседании кафедры
"Информационная безопасность"

Протокол от _____ 20__ г. № _

Зав. кафедрой _____

1. Цели изучения дисциплины

Целями изучения дисциплины "*Подготовка к процедуре защиты и защита выпускной квалификационной работы*" является получение профессиональных умений и навыков в области профессиональной деятельности.

2. Планируемые результаты обучения

Изучение дисциплины направлено на формирование у выпускника способности решать профессиональные задачи в соответствии со *всеми типами задач профессиональной деятельности*.

Результатом освоения дисциплины являются сформированные у выпускника следующие компетенции:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	<p>Знать:</p> <ul style="list-style-type: none">- способы осуществления поиска, критического анализа и синтеза информации;- предмет философии и специфику философского способа осмысления мира;- варианты решения задачи, оценивая их достоинства и недостатки. <p>Уметь:</p> <ul style="list-style-type: none">- применять методики поиска, сбора, обработки информации и осуществлять критический анализ и синтез информации, полученной из различных источников;- анализировать мировоззренческие, социально и лично-стно значимые философские проблемы;- осмысливать возможные варианты решения задачи, оценивая их достоинства и недостатки. <p>Владеть:</p> <ul style="list-style-type: none">- методами поиска, сбора и обработки, критического анализа и синтеза информации, для решения поставленных задач;- базовыми принципами и приемами философского познания, способностью формирования собственных суждений на основе осмысленной информации;- методикой поиска возможных вариантов решения задачи, оценивая их достоинства и недостатки.
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	<p>Знать:</p> <ul style="list-style-type: none">- способы и подходы формулирования задач, обеспечивающих достижение поставленной цели;- необходимые этапы для осуществления жизненного цикла проекта;- порядок решения конкретных задач проекта заявленного качества за установленное время, исходя из имеющихся ресурсов и ограничений. <p>Уметь:</p> <ul style="list-style-type: none">- определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить

	<p>главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности;</p> <ul style="list-style-type: none"> - выделять проблему и планировать пути ее реализации; - решать конкретные задачи проекта заявленного качества за установленное время при имеющихся ресурсах и ограничениях. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками решения поставленных задач, обеспечивающих достижение поставленной цели; - навыками решения задач в области избранных видов профессиональной деятельности; - навыками решения конкретных задач проекта заявленного качества за установленное время при имеющихся ресурсах и ограничениях.
<p>УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основные приемы и нормы социального взаимодействия, понятия и методы конфликтологии, технологии межличностной и групповой коммуникации в деловом взаимодействии; - различные приемы и способы социализации личности и социального взаимодействия. <p>Уметь:</p> <ul style="list-style-type: none"> - устанавливать и поддерживать контакты, обеспечивающие успешную работу в коллективе, применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды; - строить отношения с окружающими людьми, с коллегами. <p>Владеть:</p> <ul style="list-style-type: none"> - простейшими методами и приемами социального взаимодействия и работы в команде; - навыками командной работы, в социальных проектах, распределения ролей в условиях командного взаимодействия.
<p>УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)</p>	<p>Знать:</p> <ul style="list-style-type: none"> - функциональные стили родного языка, требования к деловой коммуникации; - основы устной и письменной коммуникации на иностранном языке. <p>Уметь:</p> <ul style="list-style-type: none"> - выражать свои мысли на государственном, родном языке в ситуации деловой коммуникации; - выражать свои мысли на иностранном языке в ситуации деловой коммуникации. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками составления текстов на государственном и родном языках, говорения на государственном; - навыками перевода текстов с иностранного языка на родной, коммуникаций в устной и письменной форме на ино-

<p>УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах</p>	<p>странном языках.</p> <p>Знать:</p> <ul style="list-style-type: none"> - особенности представлений культур друг о друге с учетом наличия общего ценностного контекста, этностереотипов и гетеростереотипов, формируемых информационной средой (история, философия, художественная культура, мультимедиа, личный опыт); - закономерности и особенности социально-исторического развития различных культур в этическом и философском контексте. <p>Уметь:</p> <ul style="list-style-type: none"> - преодолевать культурный барьер, воспринимая межкультурные различия избегать предубеждений и настраиваться на совместные действия с представителями других культур; - понимать и воспринимать разнообразие общества в социально-историческом, этическом и философском контекстах. <p>Владеть:</p> <ul style="list-style-type: none"> - простейшими методами адекватного восприятия межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах, общения в мире культурного многообразия с использованием этических норм поведения; - навыками нахождения и использования необходимой для взаимодействия с другими информацией о культурных особенностях и традициях различных социальных групп.
<p>УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основные методы и принципы эффективного планирования собственного времени; - основные принципы самовоспитания и самообразования, профессионального и личностного развития, исходя из этапов карьерного роста и требований рынка труда; - особенности профессиональной карьеры и стратегии профессионального развития. <p>Уметь:</p> <ul style="list-style-type: none"> - использовать инструменты и методы управления временем при выполнении конкретных задач, проектов, при достижении поставленных целей; - планировать время для саморазвития, формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, индивидуально-личностных особенностей; - планировать профессиональную карьеру с учетом требований рынка труда. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками определения эффективного направления действий в области профессиональной деятельности; - навыками принятия решений на уровне собственной

	<p>профессиональной деятельности и планирования собственной профессиональной деятельности;</p> <ul style="list-style-type: none"> - способностью определять стратегию профессионального развития с учетом требований рынка труда и предлагаемых образовательных услуг.
<p>УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основы физического воспитания и здорового образа жизни; - правила и способы планирования системы индивидуальных занятий физическими упражнениями различной подготовленности; - влияние оздоровительных систем физического воспитания на укрепление здоровья. <p>Уметь:</p> <ul style="list-style-type: none"> - индивидуально подбирать комплексы упражнений физической культуры для поддержания должного уровня физической подготовленности; - проводить самоконтроль при занятиях физическими упражнениями; - составлять комплексы физических упражнений для поддержания должностного уровня работоспособности. <p>Владеть:</p> <ul style="list-style-type: none"> - анализом уровней и показателей собственного здоровья; - методами составления и выполнения индивидуальных занятий с учетом физиологических особенностей организма; - способностью поддерживать должный уровень физической подготовленности с использованием средств и методов физической культуры и спорта.
<p>УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основные факторы вредного влияния на жизнедеятельность элементов среды обитания, основы безопасности жизнедеятельности; - правила техники безопасности на рабочем месте, методы контроля и определения опасных и вредных факторов в рамках осуществляемой деятельности - основные и правовые нормативные и правовые документы, касающиеся охраны окружающей среды и охраны труда на рабочем месте, телефоны служб спасения <p>Уметь:</p> <ul style="list-style-type: none"> - выделять неблагоприятные факторы, влияющие на жизнь и здоровье человека - идентифицировать опасные и вредные факторы в рамках осуществляемой деятельности, в том числе отравляющие и высокотоксичные вещества, биологические средства и радиоактивные вещества - выявлять и решать проблемы, связанные с нарушениями техники безопасности и участвует в мероприятиях по предотвращению чрезвычайных ситуаций на рабочем месте <p>Владеть:</p>

	<ul style="list-style-type: none"> - требованиями безопасности технических регламентов в сфере профессиональной деятельности - методами контроля и определения опасных и вредных факторов в рамках осуществляемой деятельности - методами обеспечения соблюдения правил охраны труда, техники безопасности и трудового законодательства, приемами оказания первой помощи
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	<p>Знать:</p> <ul style="list-style-type: none"> - основные законы и закономерности функционирования экономики; - основные законы экономики и принципы финансового планирования. - <p>Уметь:</p> <ul style="list-style-type: none"> - использовать основы экономической теории, необходимые для решения профессиональных и социальных задач; - применять экономические знания при выполнении практических задач; принимать обоснованные экономические решения для достижения текущих и долгосрочных финансовых целей. <p>Владеть:</p> <ul style="list-style-type: none"> - аналитическими и прикладными методами при решении экономических задач; - способностью использовать основные положения и методы экономических наук при решении социальных и профессиональных задач.
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	<p>Знать:</p> <ul style="list-style-type: none"> - формы проявления экстремизма, терроризма, коррупционного поведения в различных сферах общественной жизни, антикоррупционные законодательные акты; - сущность коррупционного поведения и его взаимосвязь с социальными, экономическими, политическими и иными условиями. <p>Уметь:</p> <ul style="list-style-type: none"> - применять правовые нормы противодействия экстремизму, терроризму и коррупционному поведению; - анализировать, толковать и правильно применять правовые нормы о противодействии экстремизму, терроризму и коррупционному поведению. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками работы с антикоррупционными нормативами; - навыками работы с законодательными и другими нормативными правовыми актами
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей	<p>Знать:</p> <ul style="list-style-type: none"> - основные понятия информатики и информационных, компьютерных и сетевых технологий, форматы применения информационных, компьютерных и сетевых технологий в современном обществе; - социальную значимость своей будущей профессии, основы профессиональной деятельности в области обеспечения информационной безопасности.

<p>личности, общества и государства</p>	<p>Уметь:</p> <ul style="list-style-type: none"> - осуществлять поиск, хранение и обработку информации из различных источников и баз данных, используя возможности вычислительной техники; - применять основы профессиональной деятельности в области обеспечения информационной безопасности. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками анализа и представления обработанной информации в требуемом формате с использованием информационных, компьютерных и сетевых технологий; - навыками применения основ обеспечения информационной безопасности и защиты интересов личности, общества и государства, норм профессиональной этики.
<p>ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе, отечественного производства, для решения задач профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основы организации современной вычислительной техники и её общие характеристики, тенденции развития устройств компьютера и компьютерных сетей, принципы организации использования средств вычислительной техники; - современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности. <p>Уметь:</p> <ul style="list-style-type: none"> - решать задачи профессиональной деятельности с применением информационно-коммуникационных технологий; - выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками эксплуатации средств управления информационными потоками, применения сетевого компьютерного оборудования, управления базами данных; - навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
<p>ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - современные математические методы, используемые для решения задач профессиональной деятельности; - основные понятия дискретной математики и свойства математических объектов, используемых в этих областях, формулировки утверждений, методы их доказательства, возможные сферы их приложений, основы построения компьютерных дискретно-математических моделей; - методы работы с данными и их анализа с позиции требований информационной безопасности. <p>Уметь:</p> <ul style="list-style-type: none"> - использовать математический аппарат при анализе и раз-

	<p>работке алгоритмов и методов решения задач профессиональной деятельности;</p> <ul style="list-style-type: none"> - решать задачи теоретического и прикладного характера из различных разделов дискретной математики и математической логики, доказывать утверждения, строить модели объектов и понятий; - использовать средства поиска и обработки данных для решения задач профессиональной деятельности. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками корректного применения математических методов и анализа их эффективности при решении задач профессиональной деятельности; - навыками алгоритмизации основных задач, применения математического аппарата дискретной математики, методов доказательства утверждений в этой области; - навыками разработки процедур решения теоретических и практических задач профессиональной деятельности.
<p>ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основные физические явления, фундаментальные понятия, законы классической и современной физики, современную научную аппаратуру, основные математические методы, используемые при решении физических задач; - методы моделирования, основанные на естественнонаучных и инженерных знаниях, методологию теоретического и экспериментального исследования в профессиональной деятельности. <p>Уметь:</p> <ul style="list-style-type: none"> - применять на практике основные физические модели, решать типовые задачи по физике, представлять результаты экспериментальных и теоретических исследований в графическом виде, в том числе с использованием программных средств, делать качественные оценки; - решать профессиональные задачи с применением методов моделирования, проводить теоретические и экспериментальные исследования в профессиональной деятельности. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками самостоятельного решения типовых задач по физике, самостоятельного планирования и проведения экспериментальных исследований; - навыками моделирования в профессиональной сфере на основе естественнонаучных и инженерных знаний, проведения теоретических и экспериментальных исследований объектов профессиональной деятельности.
<p>ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - особенности применения нормативных и правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации; - требования нормативных правовых актов и нормативных и методических документов, регламентирующих деятельность по защите информации.

	<p>Уметь:</p> <ul style="list-style-type: none"> - решать задачи профессиональной деятельности на основе применения нормативных и правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации; - анализировать нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками решения конкретных задач по защите информации на основе применения нормативных и правовых актов, нормативных и методических документов; - навыками выделения основной содержательной информации в нормативных и правовых актах.
<p>ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю</p>	<p>Знать:</p> <ul style="list-style-type: none"> - нормативные и правовые акты, регулирующие деятельность по обеспечению защиты информации от утечки и несанкционированных действий; - требования нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при организации защиты информации ограниченного доступа в компьютерных сетях. <p>Уметь:</p> <ul style="list-style-type: none"> - определять ресурсы, необходимые для обеспечения безопасности автоматизированных систем; - осуществлять подбор средств, соответствующих требованиям нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, при организации защиты информации ограниченного доступа в компьютерных сетях. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками анализа требований по защите средств вычислительной техники и автоматизированных систем на основе показателей защищенности; - навыками организации защиты информации ограниченного доступа в компьютерных сетях, соответствующей требованиям нормативных правовых актов и нормативных методических документов.
<p>ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основные принципы разработки программ на языках высокого и низкого уровня; - современные инструменты программирования и способы организации программ. <p>Уметь:</p> <ul style="list-style-type: none"> - применять современные методы программирования на языках высокого и низкого уровня;

	<p>- использовать современные инструменты программирования.</p> <p>Владеть:</p> <ul style="list-style-type: none"> - навыками разработки качественных программных приложений, удовлетворяющих требованиям стандартов, технических заданий и др.; - навыками разработки приложений для решения задач обеспечения компьютерной безопасности.
<p>ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - нормативные и методические материалы по вопросам оценки уровня защищенности объекта защиты информации; - перечень необходимых вопросов по выбору справочной литературы по вопросам обеспечения информационной безопасности. <p>Уметь:</p> <ul style="list-style-type: none"> - осуществлять подбор нормативных и методических материалов по вопросам применения средств защиты информации; - осуществлять изучение и обобщение научно-технической литературы, составлять обзор по вопросам обеспечения информационной безопасности. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками работы с нормативными и методическими материалами по вопросам применения средств защиты информации; - навыками работы со справочной и научно-технической литературой по вопросам обеспечения информационной безопасности.
<p>ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности</p>	<p>Знать:</p> <ul style="list-style-type: none"> - принципы использования средств криптографической защиты информации при решении задач профессиональной деятельности; - методики использования технических средств защиты информации для решения практических задач обеспечения информационной безопасности. <p>Уметь:</p> <ul style="list-style-type: none"> - использовать программно-аппаратные средства криптографической защиты информации для решения практических задач; - решать задачи защиты информации от утечки по техническим каналам, сетей и систем передачи информации. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками установки и настройки программно-аппаратных средств криптографической защиты информации для решения практических задач; - навыками использования специальных технических средств при защите информации от утечки по техническим каналам, сетей и систем передачи информации.

<p>ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты</p>	<p>Знать:</p> <ul style="list-style-type: none"> - угрозы информационной безопасности, меры защиты и противодействия; - принципы разработки политики безопасности; - основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты, требования и рекомендации по защите информации и требования по технической защите информации; - принципы управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации. <p>Уметь:</p> <ul style="list-style-type: none"> - строить концептуальные модели информационной безопасности объекта защиты; - разрабатывать политики безопасности с учетом угроз безопасности информации и требований по защите информации; - использовать нормативно-правовую базу в решении задач обеспечения информационной безопасности и комплексной защиты информации на предприятии и в организации; - разрабатывать организационные и технические мероприятия управления доступом и информационными потоками в компьютерных системах с учетом особенностей конкретного предприятия. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками выявления угроз информационной безопасности на объекте защиты; - навыками разработки, правильного оформления, презентации и внедрения разрабатываемых политик безопасности; - навыками работы с нормативно-правовыми и организационно-распорядительными документами в сфере информационной безопасности, вопросами технологии подбора сотрудников и работы с кадрами с точки зрения обеспечения информационной безопасности, основами организации внутриобъектового режима; - навыками проведения организационных и технических мероприятий по управлению доступом и информационными потоками в компьютерных системах.
<p>ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов</p>	<p>Знать:</p> <ul style="list-style-type: none"> - методику проведения эксперимента, обработку, оценку погрешности и достоверности их результатов; - основные понятия теории информации и кодирования, методы оптимального кодирования источников информации и помехоустойчивого кодирования в каналах связи. <p>Уметь:</p> <ul style="list-style-type: none"> - проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов; - решать типовые задачи теории информации и кодирования, вычислять информационные характеристики источников сообщений и каналов связи.

	<p>Владеть:</p> <ul style="list-style-type: none"> - навыками проведения экспериментов по заданной методике, обработку, оценку погрешности и достоверности их результатов; - основами построения математических моделей систем передачи информации.
<p>ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основную номенклатуру и характеристики аппаратуры, используемой для обеспечения защиты информации; - механизмы, используемые для защиты информации, циркулирующей в различных системах. <p>Уметь:</p> <ul style="list-style-type: none"> - выбирать и обосновывать критерии эффективности функционирования средств обеспечения защиты информации; - формулировать и решать задачи проектирования профессионально-ориентированных подсистем и средств обеспечения защиты информации с использованием различных методов и решений. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками подготовки технического задания на разработку подсистем защиты информации; - навыками применения современных методов и средств проектирования функциональных узлов различных подсистем.
<p>ОПК-13. Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма</p>	<p>Знать:</p> <ul style="list-style-type: none"> - основные этапы и закономерности исторического развития России; - особенности истории России в контексте всеобщей истории, миротворческую роль России в истории человечества; - основные направления развития ключевых регионов мира на рубеже XX – XXI вв., сущность и причины локальных, региональных, межгосударственных конфликтов в конце XX – начале XXI вв. <p>Уметь:</p> <ul style="list-style-type: none"> - выявлять закономерности исторического развития России, пролонгировать на современный и будущий этапы; - использовать научные методы анализа исторических событий, позволяющих проявить непредвзятую объективную оценку различных исторических этапов, позволяющую сформировать убежденную гражданскую позицию и патриотическое отношение к своей стране; - выявлять взаимосвязь отечественных, региональных, мировых социально-экономических, политических и культурных проблем. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками системного анализа исторических событий, выявления тенденций и закономерностей; - навыками поиска систематизации, оценки достоверности информации для анализа исторических событий;

	<p>- навыками ориентирования в современной экономической, политической, культурной ситуации в России и мире.</p>
<p>ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах</p>	<p>Знать:</p> <ul style="list-style-type: none"> - принципы организации современных операционных систем и их администрирования; - принципы разработки политики управления доступом в компьютерных системах; <p>Уметь:</p> <ul style="list-style-type: none"> - устанавливать, настраивать, вводить в эксплуатацию, следить за правильной эксплуатацией различных операционных систем; - разрабатывать политики управления доступом в компьютерных системах; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками установки, настройки, администрирования операционных систем - навыками разработки, правильного оформления, презентации и внедрения разрабатываемых политик управления доступом в компьютерных системах.
<p>ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях</p>	<p>Знать:</p> <ul style="list-style-type: none"> - принципы администрирования средства защиты информации в компьютерных сетях; - защищенные протоколы передачи данных в сети Интернет. <p>Уметь:</p> <ul style="list-style-type: none"> - использовать средства администрирования компьютерных сетей и информационных систем. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками настройки и управления конфигурацией устройств коммутации и маршрутизации, - навыками обеспечения безопасности веб-ресурсов.
<p>ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям</p>	<p>Знать:</p> <ul style="list-style-type: none"> - принципы администрирования средств защиты информации при работе с базами данных в соответствии с требованиями по защите информации. <p>Уметь:</p> <ul style="list-style-type: none"> - использовать средства администрирования различных баз данных, web-ресурсов и проводить оценку угроз их информационной безопасности; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками администрирования различных систем управления базами данных в соответствии с требованиями по защите информации, создания защищенных баз данных для получения, обработки, хранения и использования информации веб-ресурсов.
<p>ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соот-</p>	<p>Знать:</p> <ul style="list-style-type: none"> - базовые понятия и принципы применения современных методов оценки безопасности компьютерных систем.

<p>ветствии с нормативными и корпоративными требованиями</p>	<p>Уметь:</p> <ul style="list-style-type: none"> - выявлять угрозы и определять их актуальность для современных компьютерных систем; - описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем. <p>Владеть:</p> <ul style="list-style-type: none"> - практическими навыками применения методов обеспечения безопасности компьютерных систем.
<p>ПК-1. Способен применять средства защиты информации прикладного и системного программного обеспечения для решения профессиональных задач</p>	<p>Знать:</p> <ul style="list-style-type: none"> - принципы построения систем управления базами данных; - принципы построения антивирусного программного обеспечения; - уязвимости используемого программного обеспечения и методы их устранения; - виды и формы функционирования вредоносного программного обеспечения; - характерные признаки наличия вредоносного программного обеспечения. <p>Уметь:</p> <ul style="list-style-type: none"> - применять средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения; - осуществлять мероприятия по противодействию угрозам безопасности информации, возникающим при эксплуатации программного обеспечения. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками по обнаружению вредоносного программного обеспечения и ликвидации последствий его функционирования; - навыками применения средств и методов анализа программных реализаций.
<p>ПК-2. Способен участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты</p>	<p>Знать:</p> <ul style="list-style-type: none"> - виды политик безопасности компьютерных систем и сетей; - модели безопасности компьютерных систем; - организационные меры по обеспечению информационной безопасности объекта защиты. <p>Уметь:</p> <ul style="list-style-type: none"> - анализировать объект защиты информации с целью определения необходимого уровня защищенности и доверия; - формулировать задания по обеспечению информационной безопасности объекта защиты. <p>Владеть:</p> <ul style="list-style-type: none"> - навыками формирования политики безопасности компьютерных систем и сетей; - навыками разработки профилей защиты компьютерных систем.
<p>ПК-3. Способен проводить контроль безопасности и экспериментальные исследова-</p>	<p>Знать:</p> <ul style="list-style-type: none"> - виды политик управления доступом и информационными потоками применительно к компьютерным системам;

<p>дования компьютерных систем с целью выявления уязвимостей</p>	<p>- архитектура подсистем защиты информации в компьютерных системах и сетях; - уязвимости компьютерных систем и сетей и методы их устранения.</p> <p>Уметь: - выполнять контроль корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях; - оценивать угрозы безопасности информации компьютерных систем.</p> <p>Владеть: - навыками мониторинга функционирования безопасности информации в компьютерных системах и сетях; - навыками выявления уязвимостей в компьютерных системах и сетях.</p>
<p>ПК-4. Способен организовать безопасную эксплуатацию и выполнять администрирование общего и специального программного обеспечения</p>	<p>Знать: - состав типовых конфигураций программно-аппаратных средств защиты информации и режимов их функционирования в компьютерных системах и сетях; - источники угроз информационной безопасности в компьютерных системах и сетях и меры по их предотвращению.</p> <p>Уметь: - обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных системах и сетях; - выбирать режимы работы программно-аппаратных средств защиты информации в компьютерных системах и сетях.</p> <p>Владеть: - навыками конфигурирования и контроля корректности настройки программно-аппаратных средств защиты информации в компьютерных системах и сетях; - навыками мониторинга функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.</p>

3. Место дисциплины в структуре образовательной программы

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

Рабочая программа дисциплины для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

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 «Информационная безопасность» (ИБ)

Утверждаю

Зав. кафедрой ИБ СКФ МТУСИ

«____» _____ 20__ г.

ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Студенту Иванову Ивану Ивановичу группы Б-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.	<p><i>Исходные данные к ВКР</i></p> <p>1.1. Основные виды деятельности ООО «Современный Образ».</p> <p>1.2. Организационная и техническая защита структуры ЛВС ООО «Современный Образ».</p> <p>1.3. План размещения аппаратуры и рабочих мест ЛВС в помещениях офиса ООО «Современный Образ».</p>	
2.	<p>Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов):</p> <p>2.1. Введение.</p> <p>2.2. Технология построения и функционирования системы защиты ЛВС ООО «Современный Образ».</p> <p>2.2.1. Организационно-штатная структура ООО «Современный Образ» и особенности системы защиты его ЛВС.</p> <p>2.2.1.1. Основные цели модернизации системы защиты ЛВС ООО «Современный Образ»</p> <p>2.2.2. Анализ существующих методов проектирования систем защиты ЛВС.</p> <p>2.3. Выбор сетевой архитектуры и топологии модернизированной ЛВС ООО «Современный Образ».</p> <p>2.3.1. Анализ современных методов построения ЛВС.</p> <p>2.3.1.1. Ethernet.</p> <p>2.3.1.2. Fast Ethernet 100 Мбит/с.</p> <p>2.3.1.3. Wi-Fi-сети.</p> <p>2.3.1.4. WiMAX-сеть.</p> <p>2.3.2. Понятие виртуальной локальной сети.</p> <p>2.3.2.1. Обзор технологии виртуальных локальных сетей в ЛВС.</p> <p>2.3.3. Паспортизация рабочих мест и серверов ЛВС.</p> <p>2.3.4. Выбор топологии, сетевой технологии, архитектуры и структуры системы защиты ЛВС.</p> <p>2.4. Разработка проекта модернизации системы защиты ЛВС ООО «Современный Образ».</p> <p>2.4.1. Выбор оборудования.</p> <p>2.4.1.1. Выбор рабочих станций.</p> <p>2.4.1.2. Выбор точки доступа.</p> <p>2.4.1.3. Выбор коммутатора.</p> <p>2.4.1.4. Выбор сетевой операционной системы.</p> <p>2.4.1.5. Выбор антивирусной программы.</p> <p>2.4.1.6. Выбор программы резервного архивирования данных.</p> <p>2.4.2. Организационная и техническая структура ООО «Современный Образ» и системы защиты его ЛВС после модернизации.</p> <p>2.4.3. Построение математической модели модернизированной системы защиты ЛВС.</p> <p>2.4.4. Построение имитационной модели системы защиты модернизированной ЛВС.</p> <p>Вопросы конструктивных разработок – не запланированы</p> <p>Заключение.</p>	<p>1%, 7.05.23</p> <p>33%, 20.05.23</p> <p>33%, 5.06.23</p> <p>32%, 23.06.23</p> <p>1%, 25.06.23</p>

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 2024 г.
 4. Дата выдачи задания 25 января 2024 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 руководите-

ля 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: <ul style="list-style-type: none"> - содержит достаточный объем иллюстративного материала, соответствует заданию на ВКР; - четко выстроен; - рассказывается технически грамотным языком; - зачитывается. 	1 2 2 0
2.	Использование демонстрационного материала: <ul style="list-style-type: none"> - 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.	<p>Качество ответов на вопросы:</p> <ul style="list-style-type: none"> - отвечает на вопросы; 3 - не может ответить на большинство вопросов; 2 - не может четко ответить на вопросы. 0 	
4.	<p>Владение научным и специальным аппаратом:</p> <ul style="list-style-type: none"> - владеет специальным аппаратом; 3 - использованы общенаучные и специальные термины; 2 - владеет базовым аппаратом. 0 	
5.	<p>Наличие выводов:</p> <ul style="list-style-type: none"> - четкие, аргументированные; 3 - нечеткие; 2 - имеются, но не доказаны. 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 ИТ-предприятия.
- 2) Что определяет федеральный закон "О персональных данных"?
- 3) Что определяют основные руководящие документы в области ИТ-технологий?

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

- 1) Перечислите основные опасные факторы при эксплуатации ИТ-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 ИТ-оборудования.
- 4) Пояснить общую структурную схему системы защиты инфокоммуникационной сети ИТ-предприятия.
- 5) Охарактеризовать используемую для построения системы защиты инфокоммуникационной сети ИТ-предприятия технологию передачи данных.
- 6) Охарактеризовать возможные технологии для построения альтернативной системы защиты сети.
- 7) Описать перспективы развития систем защиты инфокоммуникационных сетей ИТ-предприятия.
- 8) Оценить возможность масштабирования и расширения существующих систем защиты инфокоммуникационных сетей ИТ-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 ИТ-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 ИТ-оборудования.
- 4) Для чего необходимо проводить техническое обслуживание?
- 5) Перечислить средства для проведения технического обслуживания.
- 6) Какие существуют методы поиска неисправностей для ИТ-оборудования?
- 7) Какие существуют методы устранения неисправностей?
- 8) Какие методы устранения неисправностей применяются для системы защиты ИТ-оборудования?
- 9) Каким образом организуется проведение текущего ремонта ИТ-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 ИТ-оборудования?
- 13) Влияет ли качество проведения технического обслуживания на гарантийные обязательства производителя?
- 14) Как осуществляется проверка соответствия параметров среды в местах эксплуатации ИТ-оборудования и какова её периодичность?

7. Ведение учётно-отчётной документации (ПК-2, ПК-3)

- 1) Перечислите виды учётно-отчётной документации, ведущейся в организации.
- 2) В каких документах отражается учёт ИТ-оборудования?
- 3) Какие документы оформляются при проведении технического обслуживания?
- 4) Какие документы оформляются при выявлении неисправности в негарантийный период эксплуатации ИТ-оборудования?
- 5) Какие документы оформляются при возникновении неисправности в гарантийный период эксплуатации?
- 6) Какие документы оформляются при необходимости закупки нового ИТ-оборудования?
- 7) Какие документы оформляются при необходимости закупки комплектующих и запасных частей для ремонта системы защиты ИТ-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 (ред. от 30.12.2015) "Об электронной подписи"		Э2

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 5485-1 "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	Издательство, год	Кол.

ЛЗ.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	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			
П.3	Kaspersky Endpoint Security (лицензия)			

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 22.01.2024г.

Выпускная квалификационная работа выполнена

Под руководством _____
(Фамилия и инициалы руководителя)

В государственную экзаменационную комиссию представлены следующие материалы:

1. Справка деканата заочного факультета от _____ 2024
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

(подпись)

(Ф.И.О.)

Секретарь государственной экзаменационной комиссии

(подпись)

(Ф.И.О.)

Примерный календарный график выполнения и защиты ВКР

СОГЛАСОВАНО

Зам. директора по УВР
 _____ А.Г. Жуковский
 « ____ » « _____ » 2024 г.

УТВЕРЖДАЮ

Директор СКФ МТУСИ
 _____ Д.Н.Карасев
 « ____ » « _____ » 2024 г.

График подготовки защиты ВКР выпускников филиала 2024 года и сроки вручения дипломов выпускникам очного и заочного факультетов

Этапы	Сроки	Мероприятия	Контингент
1	до 11.02.2024	Ознакомление под роспись выпускников филиала с черновым вариантом приложения на начало последней сессии	все 4 курсы ОФ, специалисты ФИК по УМР
2	до 18.02.2024	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 25.02.2024	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 29.02.2024	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 05.03.2024	Контроль представления ВКР дипломниками	зав. кафедрами, деканат ФИК
8	до 05.03.2024	Заполнение приложений к дипломам бакалавров в электронном виде (без итогов защиты)	все 4 курсы ОФ, вспомогательный персонал
9	до 14.03.2024	Распечатка и проверка набранных приложений к дипломам бакалавров	вспомогательный персонал, специалисты ФИК по УМР, зам. декана ФИК
10	до 20.03.2024	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 01.04.2024	Подготовка приказов об отчислении с 21.04.2024 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 14.04.2024	Корректировка, распечатка приложений к дипломам бакалавров	специалисты ФИК по УМР, зам. декана ФИК, вспомогательный персонал
17	до 16.04.2024	Оформление приложений к дипломам бакалавров и передача их в отдел кадров СКФ	вспомогательный персонал, специалисты ФИК по УМР, зам. декана ФИК
18	до 22.04.2024	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 21.04.2024	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 МТУ-СИ	ОК
22	до 23.04.2024	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 черновики приложений к дипломам бакалавров	вспомогательный персонал, зам. декана ФИК
24	до 29.04.23	Контроль представления ВКР дипломника-	зав. кафедрами,

		ми ОФ	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 защиты)	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	Подписание дипломов и копий у председателей ГЭК. Приём документов деканата,	ОК

	18.07.23	внесение последних данных с вкладышей в журнал выдачи дипломов	
40	до 18.07.2024.	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 2024 года и вручение им дипломов бакалавров	приглашенные гости, администрация, преподаватели и сотрудники СКФ
43	23.07.2024	Организация возвращения всего имущества и документации филиала после торжественного собрания в СКФ	зам. директора по АХР, отдел кадров, деканат ФИК

Декан факультета ИК

Начальник ОК

Зам. директора по АХР

Председатель профкома СКФ

Зав. кафедрой ИТСС

Зав. кафедрой ИВТ

Ефимов С.В.

Шустова В.В.

Гуринович С.М.

Янкина Н.А.

Юхнов В.И.

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