

**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» (МТУСИ)

Утверждаю

Зам. директора по УР

Н.А. Андреева

«25» 04 2026 г.

**РАБОЧАЯ ПРОГРАММА
ИТОГОВОЙ (ГОСУДАРСТВЕННОЙ ИТОГОВОЙ) АТТЕСТАЦИИ**

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

Кафедра: **Информационной безопасности**

Направление подготовки: **10.03.01 Информационная безопасность**

Профиль: **Безопасность компьютерных систем (по отрасли или в сфере
профессиональной деятельности)**

Форма обучения: **очная**

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

Вид учебной работы	ОФО	
	ЗЕ	Часов/семестр
Общая трудоемкость дисциплины, в том числе (по семестрам, курсам):	6	216/8
Контактная работа, в том числе (по семестрам, курсам):		
Лекции		
Лабораторных работ		
Практических занятий		
Семинаров		
Иная контактная работа		20/8
Самостоятельная работа		196/8
Контроль		
Число контрольных работ (по курсам)		
Число КР (по семестрам, курсам)		
Число КП (по семестрам, курсам)		
Число зачетов с оценкой с разбивкой по семестрам (курсам)		
Число экзаменов с разбивкой по семестрам (курсам)		

Программу составил:

К.т.н., доцент Маршаков Д.В.

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 науки и высшего образования Российской
Федерации от 17 ноября 2020 г. N 1427.

Составлена на основании учебного плана

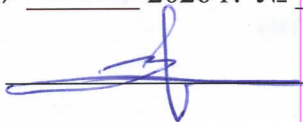
направления **10.03.01 Информационная безопасность**, профиля «Безопасность
компьютерных систем (по отрасли или в сфере профессиональной деятельности)»,
одобренного Учёным советом СКФ МТУСИ, протокол № 8 от 31.03 2026г., и
утвержденного директором СКФ МТУСИ 31.03 2026 г.

Рассмотрена и одобрена на заседании кафедры

«Информационная безопасность»

Протокол от «28» 04 2026 г. № 9

И.О.Зав. кафедрой



Жуковский А.Г

1. Цели Итоговой (государственной итоговой) аттестации (далее ИА)

Целями ИА *"Подготовка к процедуре защиты и защита выпускной квалификационной работы"* выступают проверка конечных результатов освоения ОПОП ВО, уровня освоения компетенций, подготовленности выпускников к заявленным в ОПОП видам профессиональной деятельности, а также определение соответствия уровня теоретических знаний и практических умений выпускника требованиям ФГОС ВО и ОПОП ВО по направлению 10.03.01 «Информационная безопасность».

2. Планируемые результаты обучения

В результате проведения итоговой (государственной итоговой) аттестации проверяется готовность выпускника к решению профессиональных задач в рамках **эксплуатационного** вида деятельности.

Результатом освоения образовательной программы являются сформированные у выпускника следующие компетенции:

УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1. Знает методы поиска, анализа и обработки данных, основы теории систем и системного анализа. УК-1.2. Умеет выбирать методы и модели системного анализа для обработки, анализа и обоснования результатов решения профессиональных задач в прикладной области. УК-1.3. Владеет навыками применения формализованных и неформализованных методов анализа систем для решения профессиональных задач в прикладной области.
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	УК-2.1. Знает способы и подходы формулирования задач, обеспечивающих достижение поставленной цели; необходимые этапы для осуществления жизненного цикла проекта. УК-2.2. Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность, исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности; решать конкретные задачи проекта заявленного качества за установленное время при имеющихся ресурсах и ограничениях. УК-2.3. Владеет навыками решения конкретных задач проекта заявленного качества за установленное время при имеющихся ресурсах и ограничениях.
УК-3. Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	УК-3.1. Знает 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. УК-3.2. Умеет 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. УК-3.3. Владеет методами и приемами социального

	взаимодействия и работы в команде; навыками командной работы, в социальных проектах, распределения ролей в условиях командного взаимодействия.
УК-4. Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	УК-4.1. Знает принципы построения устного и письменного высказывания на русском и иностранном языках; правила и закономерности деловой устной и письменной коммуникации. УК-4.2. Умеет применять на практике деловую коммуникацию в устной и письменной формах, методы и навыки делового общения на русском и иностранном языках. УК-4.3. Владеет навыками чтения и перевода текстов на иностранном языке в профессиональном общении; навыками деловых коммуникаций в устной и письменной форме на русском и иностранном языках; методикой составления суждения в межличностном деловом общении на русском и иностранном языках.
УК-5. Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах	УК-5.1. Знает основные этапы и закономерности исторического развития; основные события отечественной истории; особенности представлений культур друг о друге с учетом наличия общего ценностного контекста; закономерности и особенности социально-исторического развития различных культур в этическом и философском контексте. УК-5.2. Умеет понимать тенденции развития и мотивы политики Российского государства; ориентироваться в мотивах исторического процесса; преодолевать культурный барьер, воспринимая межкультурные различия избегать предубеждений и настраиваться на совместные действия с представителями других культур; оценивать окружающие социальные явления с точки зрения моральных ценностей; демонстрировать понимание необходимости и стремления обучаться в течение всей жизни. УК-5.3. Владеет навыками целостного подхода к анализу проблем общества; способностью позитивно оценивать культурные достижения своей российской истории и толерантно относиться к ценностям других, европейских и восточных культур; навыками нахождения и использования необходимой для взаимодействия с другими информации о культурных особенностях и традициях различных социальных групп.
УК-6. Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни	УК-6.1. Знает основные приемы эффективного управления собственным временем при освоении академических дисциплин; образовательную траекторию при изучении профильных дисциплин и саморазвития в сфере информационной безопасности. УК-6.2. Умеет реализовывать траекторию саморазвития при решении базовых задач будущей профессиональной деятельности; выстраивать траекторию саморазвития при планировании стратегий решения задач будущей профессиональной деятельности; использовать методы самообучения при решении задач будущей профессиональной

	деятельности. УК-6.3. Владеет навыками самообучения при реализации образовательной траектории в различных стратегиях решения задач будущей профессиональной деятельности; навыками самоорганизации различных моделей поведения, необходимых для решения типовых профессиональных задач.
УК-7. Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности	УК-7.1. Знает 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. УК-7.2. Умеет индивидуально подбирать комплексы упражнений физической культуры для поддержания должного уровня физической подготовленности; проводить самоконтроль при занятиях физическими упражнениями; составлять комплексы физических упражнений для поддержания должного уровня работоспособности. УК-7.3. Владеет 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.
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	УК-8.1. Знает 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. УК-8.2. Знает основные положения общевоинских уставов ВС РФ; организацию внутреннего порядка в подразделении; устройство стрелкового оружия, боеприпасов и ручных гранат; основные факторы, определяющие характер, организацию и способы ведения современного общевойскового боя; общие сведения о ядерном, химическом и биологическом оружии, средствах его применения; правила поведения и меры профилактики в условиях заражения радиоактивными, отравляющими веществами и бактериальными средствами. УК-8.3. Умеет 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. УК-8.4. Умеет правильно применять и выполнять положения

	общевоинских уставов ВС РФ; осуществлять разборку и сборку автомата (АК-74) и пистолета (ПМ), подготовку к боевому применению ручных гранат; оборудовать позицию для стрельбы из стрелкового оружия; выполнять мероприятия радиационной, химической и биологической защиты. УК-8.5. Владеет методами контроля и определения опасных и вредных факторов в рамках осуществляемой деятельности; методами обеспечения соблюдения правил охраны труда, приемами оказания первой помощи. УК-8.6. Владеет строевыми приемами на месте и в движении; навыками управления строями взвода; навыками стрельбы из стрелкового оружия; навыками применения индивидуальных средств РХБ защиты; навыками применения индивидуальных средств медицинской защиты и подручных средств для оказания первой медицинской помощи при ранениях и травмах.
УК-9. Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-9.1. Знает основы экономического устройства общества, закономерности функционирования и развития рыночной экономики; основные характеристики и проблемы развития экономики РФ. УК-9.2. Умеет решать задачи по микро- и макроэкономике, самостоятельно выбирать способ решения задачи, используя графические изображения; анализировать информацию, необходимую для принятия обоснованных экономических решений с применением цифровых технологий и инструментов; оценивать индивидуальные риски, связанные с предпринимательской деятельностью и использованием цифровых инструментов управления личными финансами, а также фишинг риски. УК-9.3. Владеет навыками использования экономических терминов и понятий для характеристики реальных экономических проблем; навыками использования экономических методов для описания и анализа хозяйственных явлений и процессов; навыками анализа, необходимой для принятия обоснованных экономических решений информации с применением интернет сервисов и ресурсов.
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1. Знает понятийно-категориальный аппарат в области реализации социальной ответственности; законодательство Российской Федерации в области противодействия экстремизму и терроризму; формы проявления экстремизма, терроризма, коррупционного поведения в различных сферах общественной жизни, антикоррупционные законодательные акты. УК-10.2. Умеет управлять процессами, направленными на развитие социально-ответственного поведения различных социальных групп; применять правовые нормы противодействия экстремизму, терроризму и коррупционному поведению. УК-10.3. Владеет технологиями развития социально-

	ответственного поведения людей в рамках отдельных организаций; навыками использования правовых средств для обеспечения безопасности личности, общества, государства.
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.1. Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности РФ; основные нормативные акты, регламентирующие деятельность по защите информации, направления деятельности по обеспечению информационной безопасности, причины и последствия нарушения требований информационной безопасности. ОПК-1.2. Умеет классифицировать и оценивать угрозы информационной безопасности; оперировать базовой терминологией в области информационных технологий, информационной безопасности личности, общества и государства, гуманитарных аспектов информационной безопасности. ОПК-1.3. Владеет основными информационными технологиями, базовыми методами выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угроз информационной безопасности.
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе, отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Знает программные средства системного и прикладного назначения, в том числе отечественного производства, и принципы их применения при решении задач профессиональной деятельности; принципы работы и правила построения сетей с коммутацией пакетов; основы организации современной вычислительной техники и её общие характеристики, тенденции развития устройств компьютера и компьютерных сетей. ОПК-2.2. Умеет подбирать информационно-коммуникационные технологии и рационально использовать функциональные возможности программных средств системного и прикладного назначения; оценивать эффективность реализации различных моделей данных и знаний и на этой основе делать выбор о практической реализации систем обработки данных и знаний; выбирать методику диагностирования и отладки аппаратных и программных средств. ОПК-2.3. Владеет навыками использования системного и прикладного программного обеспечения для решения задач профессиональной деятельности.
ОПК-3. Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1. Знает основы высшей математики; основные разделы математической логики; методы накопления, передачи и обработки информации; основные понятия и результаты теории вероятностей; ключевые разделы дискретной математики. ОПК-3.2. Умеет решать стандартные профессиональные задачи с применением необходимых математических методов; формализовывать профессиональные задачи в логических терминах, решать прикладные задачи в вероятностных терминах;

	моделировать прикладные задачи дискретными структурами. ОПК-3.3. Владеет математическими методами исследования объектов профессиональной деятельности; методами аналитического и численного расчёта; методами доказательства (включая математическую индукцию и инварианты), приёмами комбинаторного подсчёта и рекурсий, базовыми графовыми алгоритмами и техниками преобразования формул в КНФ/ДНФ для решения прикладных задач.
ОПК-4. Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	ОПК-4.1. Знает основы предметной области, основные физические законы, явления, определения, понятия и связи между ними, широту и ограниченность применения физических законов к исследованию процессов и явлений в природе, связь физики с другими науками и дисциплинами; фундаментальные понятия электроники, основы построения элементной базы, применяемой в вычислительных машинах и системах защиты информации, законы классической и современной физики, основные математические методы, используемые при решении задач электроники; основы имитационного моделирования, методологию теоретического и экспериментального исследования в электронике ОПК-4.2. Умеет применять основные физические законы для решения типовых задач, применять на практике основные модели электронных схем, решать типовые задачи по электронике, представлять результаты экспериментальных и теоретических исследований в аналитическом, численном и графическом видах, решать задачи электроники с применением методов имитационного моделирования; ОПК-4.3. Владеет навыками корректного представления физической информации, в том числе в графической и математической форме, интерпретировать результаты проведенных исследований и передавать их в виде конкретных рекомендаций; навыками расчёта аналоговых электрических цепей с применением современных программных средств и вычислительной техники; навыками имитационного моделирования электронных схем.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1. Знает требования нормативных правовых актов и нормативных и методических документов, регламентирующих деятельность по защите информации; особенности применения нормативной и правовой документации, характерной для защиты персональных данных. ОПК-5.2. Умеет решать задачи профессиональной деятельности на основе применения нормативных и правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации. ОПК-5.3. Владеет навыками применения нормативной и правовой документации, необходимой для защиты персональных данных.
ОПК-6. Способен при	ОПК-6.1. Знает нормативные и правовые акты, регулирующие

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	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. ОПК-6.2. Умеет 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. ОПК-6.3. Владеет 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.
ОПК-7. Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности	ОПК-7.1. Знает принципы структурного и модульного программирования; принципы разработки сложных программных систем, в том числе правила разработки интерфейса; принципы тестирования программных систем; основные понятия объектно-ориентированного программирования. ОПК-7.2. Умеет строить формальную модель системы (подсистемы) по её описанию в терминах предметной области; разрабатывать модульную структуру программной системы, обеспечивающие её функциональную наполненность, и дружественный интерфейс пользователя; производить тестирование и отладку программной системы с целью устранения синтаксических и семантических ошибок с целью повышения надёжности программного обеспечения; применять языки программирования для решения профессиональных задач. ОПК-7.3. Владеет методами программирования, разработки эффективных программных средств решения прикладных задач.
ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1. Знает нормативные и методические материалы по вопросам оценки уровня защищенности объекта защиты информации; перечень необходимых вопросов по выбору справочной литературы по вопросам обеспечения информационной безопасности. ОПК-8.2. Умеет применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач. ОПК-8.3. Владеет практическим опытом поиска, сбора и обработки, критического анализа и синтеза информации;

	навыками работы со справочной и научно-технической литературой по вопросам обеспечения информационной безопасности.
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Знает принципы использования средств криптографической защиты информации при решении задач профессиональной деятельности; методики использования технических средств защиты информации для решения практических задач обеспечения информационной безопасности; виды криптографических протоколов и их место в комплексной системе защиты информации; основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш- функции и криптографические протоколы. ОПК-9.2. Умеет анализировать угрозы безопасности информации в компьютерных сетях; использовать криптографические протоколы, применяемые в компьютерных сетях, применять средства криптографической и технической защиты информации. ОПК-9.3. Владеет 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.
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	ОПК-10.1. Знает угрозы информационной безопасности, меры защиты и противодействия; принципы разработки политики безопасности; принципы управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации. ОПК-10.2. Умеет 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; определять комплекс мер для обеспечения защиты информации объектов информатизации. ОПК-10.3. Владеет 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; аналитикой информационной инфраструктуры информационной системы и ее безопасности объектов информатизации.

ОПК-11. Способен проводить эксперименты по заданной методике и обработку их результатов	ОПК-11.1. Знает методы, технологию организации и проведения испытаний аппаратных и программных средств вычислительной техники; основные понятия и определения, используемые при описании моделей безопасности компьютерных систем; современные методы моделирования систем защиты информации. ОПК-11.2. Умеет выбирать методику испытаний, адекватно оценивающую требуемые показатели; анализировать данные проведенных испытаний и делать выводы о работоспособности устройств и программ; проводить эксперименты по заданным методикам и обработку их результатов; применять комплексный подход к обеспечению информационной безопасности объекта защиты. ОПК-11.3. Владеет навыками проведения испытаний по заданной методике, обработки, оценки погрешности и достоверности результатов испытаний; навыками построения стандартных процедур принятия решений, на основе имеющихся экспериментальных данных; практическими навыками применения современных методов моделирования систем защиты информации.
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1. Знает принципы построения и контроля ИТ-инфраструктуры организации; основные аспекты информационной безопасности; методы защиты объектов от несанкционированного доступа физических лиц и основные направления противодействия техническим средствам разведки; механизмы, используемые для защиты информации, циркулирующей в различных системах. ОПК-12.2. Умеет моделировать типовые и специализированные информационные системы; применять на практике технические методы защиты информации, пользоваться стандартной терминологией и определениями; формулировать и решать задачи проектирования профессионально-ориентированных подсистем и средств обеспечения защиты информации с использованием различных методов и решений. ОПК-12.3. Владеет навыками мониторинга событий информационной безопасности, расследования инцидентов информационной безопасности; навыками выявления и нейтрализации компьютерных атак, оценки защищенности элементов информационных сетей; способностью применять современные теоретические и экспериментальные методы исследования с целью создания новых перспективных средств электросвязи и информатики; методами и средствами инженерной защиты и технической охраны объектов; навыками подготовки технического задания на разработку подсистем защиты информации.
ОПК-13. Способен анализировать основные этапы и закономерности	ОПК-13.1. Знает основные закономерности исторического процесса, этапы исторического развития России, место и роль России в истории человечества и в современном мире; ключевые

исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма	события истории России и мира, выдающихся деятелей России. ОПК-13.2. Умеет соотносить общие исторические процессы и отдельные факты, выявлять существенные черты исторических процессов, явлений и событий; выявлять взаимосвязь отечественных, региональных, мировых социально-экономических, политических и культурных проблем. ОПК-13.3. Владеет навыками системного анализа исторических событий, выявления тенденций и закономерностей; навыками ориентирования в современной экономической, политической, культурной ситуации в России и мире.
ОПК-1.1. Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-1.1.1. Знает понятия информации и информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации; направления обеспечения информационной безопасности; принципы построения систем управления базами данных; виды политик управления доступом в компьютерных системах. ОПК-1.1.2. Умеет использовать механизмы идентификации и аутентификации; использовать антивирусные средства защиты; восстанавливать потерянные компьютерные данные; производить резервное копирование информации; настраивать системы доступа. ОПК-1.1.3. Владеет основными понятиями, связанными с обеспечением доступа к компьютерным системам; навыками работы по основам защиты информации с использованием программно-аппаратных комплексов; навыками настройки ОС с целью установки политики безопасности.
ОПК-1.2. Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-1.2.1. Знает классификацию методов криптографического преобразования информации; структуру и принципы функционирования современных вычислительных систем; основные способы защиты от потери информации и нарушений работоспособности сетей и систем; модели политик информационной безопасности в компьютерных сетях; принципы построения компьютерных сетей. ОПК-1.2.2. Умеет использовать механизмы управления трафиком; классифицировать и оценивать угрозы информационной безопасности в компьютерных сетях; проводить работы по администрированию средств защиты информации в компьютерных сетях; проводить работы по разграничению прав доступа пользователей к сетевым ресурсам; использовать средства защиты информации операционных систем для противодействия угрозам безопасности информации. ОПК-1.2.3. Владеет способностью настраивать коммутационное и маршрутизирующее оборудование; навыками работы по конфигурированию средств защиты компьютерных сетей; методами измерений, контроля и технических расчетов характеристик программно-аппаратных

	средств защиты информации.
ОПК-1.3. Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	ОПК-1.3.1. Знает основные угрозы безопасности баз данных; правила работы с различными информационными системами и базами данных; принципы администрирования средств защиты информации при работе с базами данных в соответствии с требованиями по защите информации. ОПК-1.3.2. Умеет формировать структуру базы данных с точки зрения безопасности информации; работать с различными информационными системами и базами данных; обрабатывать информацию с использованием современных технических средств. ОПК-1.3.3. Владеет навыками создания защищенных баз данных; 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.
ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-1.4.1. Знает методы анализа и оценки защищенности компьютерных систем; этапы и процедуры аудита информационной безопасности защищенных компьютерных систем; особенности комплексного подхода к обеспечению информационной безопасности организации. ОПК-1.4.2. Умеет разрабатывать и применять методики оценки защищенности программно-аппаратных средств защиты информации компьютерных систем; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации. ОПК-1.4.3. Владеет методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищенных компьютерных систем нормативным требованиям по защите информации; владеть методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации; владеть технологией разработки комплекта нормативно-методического обеспечения комплексной защиты информации на предприятии.
ПК-1. Администрирование подсистем защиты информации в операционных системах	ПК-1.1. Знает архитектуру и принципы построения операционных систем; программные интерфейсы операционных систем; виды политик управления доступом; архитектуру подсистем защиты информации в операционных системах; состав типовых конфигураций программно-аппаратных средств защиты информации; методы и средства антивирусной защиты в операционных системах; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации и обеспечению безопасности критической информационной инфраструктуры; методы измерений, контроля

	и технических расчетов характеристик программно-аппаратных средств защиты информации. ПК-1.2. Умеет формировать политики безопасности операционных систем; оценивать угрозы безопасности информации операционных систем; противодействовать угрозам безопасности информации с использованием встроенных средств защиты информации операционных систем; настраивать антивирусные средства защиты информации в операционных системах; устанавливать обновления программного обеспечения и средств антивирусной защиты; оценивать угрозы безопасности информации в операционных системах; обосновывать выбор используемых программно-аппаратных средств защиты информации в операционных системах. ПК-1.3. Владеет навыками определения состава применяемых программно-аппаратных средств защиты информации в операционных системах; навыками установки программно-аппаратных средств защиты информации в операционных системах, включая средства криптографической защиты информации; управлением антивирусной защитой операционных систем в соответствии с действующими требованиями; программно-аппаратными средствами и методами защиты информации в операционных системах; нормативными правовыми актами в области защиты информации.
ПК-2 Администрирование программно-аппаратных средств защиты информации в компьютерных сетях	ПК-2.1. Знает программные средства системного и прикладного назначения, в том числе отечественного производства, и принципы их применения при решении задач профессиональной деятельности; методы и средства обеспечения информационной безопасности в компьютерных сетях; нормативно-правовые акты, регулирующие защиту информации; алгоритмы и протоколы шифрования данных; принципы администрирования сетевых экранов (файрволов); методы мониторинга и анализа событий в компьютерных сетях для выявления потенциальных угроз; инструменты и методы управления доступом к информационным ресурсам; технологии аутентификации и авторизации пользователей в сети; способы обеспечения целостности и доступности информации; принципы функционирования сетевых протоколов, включающих криптографические алгоритмы. ПК-2.2. Умеет настраивать и управлять программными и аппаратными средствами защиты информации в компьютерных сетях; устанавливать и обновлять антивирусное программное обеспечение; настраивать файрволы и другие сетевые экраны для защиты от внешних угроз; настраивать протоколы шифрования данных; управлять политиками безопасности в сетевых операционных системах; реагировать на инциденты безопасности и принимать меры по устранению последствий; настраивать системы обнаружения и предотвращения вторжений (IDS/IPS); оценивать оптимальность выбора программно-аппаратных средств защиты информации и их режимов функционирования в компьютерных сетях.

	ПК-2.3. Владеет навыками настройки и управления программных и аппаратных средств защиты информации в компьютерных сетях; методами мониторинга и анализа событий безопасности в компьютерных сетях; технологиями установки и настройки межсетевых экранов, систем обнаружения и предотвращения вторжений (IDS/IPS); способами настройки антивирусного программного обеспечения и систем защиты от вредоносного ПО; методами управления учётными записями, правами доступа и политиками безопасности; навыками внедрения и настройки систем шифрования данных; навыками конфигурирования защищенного удаленного доступа; навыками конфигурирования аппаратно-программных средств для организации виртуальных частных сетей.
ПК-3. Администрирование средств защиты информации прикладного и системного программного обеспечения	ПК-3.1. Знает виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению; уязвимости используемого программного обеспечения и методы их устранения; средства и методы обнаружения ранее неизвестного вредоносного программного обеспечения; принципы функционирования программных средств криптографической защиты информации; нормативные правовые акты в области защиты информации; методы ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования. ПК-3.2. Умет подбирать программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности; обосновывать правила безопасной эксплуатации программного обеспечения; 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. ПК-3.3. Владеет навыками определения порядка установки программного обеспечения с целью соблюдения требований по защите информации; контроля за соблюдением требований по защите информации при установке программного обеспечения, включая антивирусное программное обеспечение; выполнения работ по обнаружению и ликвидации вредоносного программного обеспечения; навыками установки, конфигурации и эксплуатации программного обеспечения по защите информации.

3. Место дисциплины в структуре образовательной программы

Итоговая (государственная итоговая) аттестация является заключительным этапом освоения основной образовательной программы обучающимся и обязательной частью ОП ВО.

Форма проведения итоговой (государственной итоговой) аттестации – подготовка к процедуре защиты и защита выпускной квалификационной работы.

Время проведения ИА определено календарным графиком учебного процесса и проводится для обучающихся очной формы обучения по завершении 4 семестра.

Общая трудоемкость ИА составляет 6 зачетных единиц.

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

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

4.2. В ИА входит подготовка к процедуре защиты и защита выпускной квалификационной работы.

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

4.4. Сроки выполнения выпускных квалификационных работ в обязательном порядке доводятся до сведения обучающихся не позднее, чем за полгода до начала ИА.

5. Оценочные материалы (оценочные средства) для проведения итоговой (государственной итоговой) аттестации

В основе оценочных материалов лежат принципы валидности, определенности, однозначности, надежности

5.1. Контрольные вопросы и задания

Оценивание ВКР осуществляется по следующим группам критериев:

1) критерии содержания:

- ° обоснованность выбора и актуальность темы ВКР;
- ° обоснование практической и теоретической значимости ВКР;
- ° уровень осмысления теоретических вопросов и обобщения собранного материала;
- ° наличие в ВКР результатов, которые в совокупности решают конкретную научную и (или) практическую задачу;

° обоснованность и четкость сформулированных выводов;

° адекватность использования методов, объем и уровень анализа литературы по рассматриваемой проблеме,

полнота, корректность и содержание цитирования, логичность изложения материала;

2) критерии оформления ВКР:

° владение научно-техническим стилем изложения, орфографическая и пунктуационная грамотность;

° соответствие формы представления работы требованиям, предъявляемым к оформлению такого рода работ;

3) критерии процедуры защиты ВКР:

° качество устного доклада: логичность, точность формулировок, обоснованность выводов;

° презентационные навыки: структура и последовательность изложения материала, соблюдение временных требований, контакт с аудиторией, язык изложения;

° качество ответов на вопросы членов экзаменационной (государственной экзаменационной) комиссии (ЭК): логичность, глубина, правильность и полнота ответов;

4) отзыв руководителя и рецензента - оценка содержания и оформления ВКР.

Оценку результатов выполнения ВКР осуществляют:

– руководитель ВКР, оценивая, качество подготовленной к защите ВКР, поведенческий аспект (способность, готовность, самостоятельность, ответственность) обучающегося в период выполнения работы;

– консультант по разделу ВКР (при наличии), оценивая, качество подготовленного раздела ВКР, поведенческий аспект (способность, готовность, самостоятельность, ответственность) обучающегося в период выполнения работы;

– члены ЭК, оценивая, качество выполнения и защиты ВКР, качество освоения ОПОП ВО.

Объектами оценки являются:

а) пояснительная записка ВКР;

б) презентация, представляемая обучающимся на защите ВКР;

в) доклад обучающегося на заседании экзаменационной (государственной экзаменационной) комиссии;

г) ответы студента на вопросы, заданные членами комиссии в ходе защиты ВКР.

5.2. Примерный перечень тем ВКР

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. Программа мониторинга действий пользователей в компьютерной сети

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

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

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

15. Разработка управляющего и лекционного модулей электронного пособия по дисциплине «Основы информационной безопасности»

16. Разработка лабораторного практикума по дисциплине «Проектный практикум»

17. Разработка электронного пособия по по дисциплине «Основы управления информационной безопасностью»

5.3. Оценочные материалы и перечень видов оценочных средств

Оценочные материалы и перечень видов оценочных средств по дисциплине, требования, предъявляемые ГОСТ к оформлению пояснительной записки, контрольные вопросы для подготовки к защите выпускной квалификационной работы представлены в приложении 1 к настоящей программе.

6. Учебно-методическое и информационное обеспечение ИА

6.1. Рекомендуемая литература

6.1.1. Основная литература

Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л1.1	Галатенко, В.А.	Основы информационной безопасности: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024.	Э1
Л1.2	Суворова, Г.М.	Информационная безопасность: учебное пособие	Саратов: Вузовское образование, 2024.	Э2
Л1.3	А.М. Голиков	Защита информации от утечки по техническим каналам	Томский Государственный университет Систем управления и радиоэлектроники, 2015	Э3
Л1.4	Бузов Г.А.	Защита информации ограниченного доступа от утечки по техническим каналам	М.: Гор. линия-Телеком, 2024. – 585 с.	Э4
Л1.5	Лапони́на О.Р., В.А. Сухомлина	Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учебное пособие	М.: ИНТУИТ, Ай Пи Ар Медиа, 2024— 605 с.	Э5
Л1.6	Бабаш А.В.	Криптографические методы защиты информации. Том 1: учебно-методическое пособие	М.: РИОР: ИНФРА-М, 2021. — 413 с.	Э6
Л1.7	Белоус, А.И., В. А. Солодуха	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения	Москва: Техносфера, 2021. — 482 с.	Э7
Л1.8	Баранова, Е.К., А.В. Бабаш	Информационная безопасность и защита информации: учебное пособие — 3-е изд., перераб. и доп.	Москва: РИОР: ИНФРА-М, 2024. — 336 с.	Э8
Л1.9	Шаньгин, В. Ф.	Комплексная защита информации в корпоративных системах: учебное пособие	Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с.	Э9
6.1.2. Дополнительная литература				
Код	Авторы, составители	Заглавие	Издательство, год	Кол.
Л2.1	Литвинов, Р.В., К.А. Волегов, А.П. Бацула	Технические средства защиты информации. Часть 1: курс лекций	Томск: Томский государственный университет систем управления и радиоэлектроники, 2006. — 170 с.	Э10
Л2.2	Маршаков Д.В., Д.В. Фахти	Методы и средства криптографической защиты информации. Практический курс: учебное пособие	М.: ИНФРА-М, 2022. — 76 с	Э11

Л2.3	Макаренко С.И.	Аудит безопасности критической инфраструктуры специальными информационными воздействиями: монография	Санкт-Петербург: Наукоемкие технологии, 2018	Э12
Л2.4	А. В. Терехов, В. Н. Чернышов, А. В. Платенкин, А. В. Селезнев	Информационная безопасность и правовые основы защиты персональных данных: учебное пособие	Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2023. — 80 с.	Э13
Л2.5		Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (с изм. и доп.)		Э14
Л2.6		Федеральный закон от 06.04.2011 N 63-ФЗ (с изм. и доп.) "Об электронной подписи"		Э15
Л2.7		Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (с изм. и доп.)		Э16
Л2.8		Федеральный закон от 17 июля 1999 г. N 176-ФЗ "О почтовой связи" (с изм. и доп.)		Э17
Л2.9		Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изм. и доп.)		Э18
Л2.10		Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" (с изм. и доп.)		Э19
Л2.11		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"		Э20
Л2.12		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"		Э21
Л2.13		ГОСТ 34.936-91 Информационная технология. Локальные вычислительные сети. Определение услуг уровня управления доступом к среде		Э22
Л2.14		ГОСТ Р 53724-2009 Качество услуг связи. Общие положения		Э23

6.1.3. Учебно-методическое обеспечение				
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 – 3 издание	РнД: СКФ МТУСИ, 2024. – 69 с.	Э24
6.2. Электронные образовательные ресурсы				
Э1	https://www.iprbookshop.ru/142285.html			
Э2	https://www.iprbookshop.ru/142805.html			
Э3	https://www.iprbookshop.ru/72090.html			
Э4	https://elibr.mtuci.ru/view.php?book_id=3168			
Э5	https://www.iprbookshop.ru/142292.html			
Э6	https://znanium.com/catalog/product/1215714			
Э7	https://www.iprbookshop.ru/108023.html			
Э8	https://znanium.ru/catalog/product/2082642			
Э9	http://elibr.mtuci.ru/view.php?book_id=3659			
Э10	https://www.iprbookshop.ru/14027.html			
Э11	https://znanium.ru/catalog/product/1891129			
Э12	https://www.iprbookshop.ru/10615.html			
Э13	https://www.iprbookshop.ru/141049.html			
Э14	https://www.consultant.ru/document/cons_doc_LAW_61801/			
Э15	https://www.consultant.ru/document/cons_doc_LAW_112701/			
Э16	https://www.consultant.ru/document/cons_doc_LAW_43224/			
Э17	https://www.consultant.ru/document/cons_doc_LAW_6719/			
Э18	https://www.consultant.ru/document/cons_doc_LAW_61798/			
Э19	https://www.consultant.ru/document/cons_doc_LAW_2481/			
Э20	https://www.consultant.ru/document/cons_doc_LAW_75586/			
Э21	https://ivo.garant.ru/#/document/70391358/paragraph/1/doclist/376/1/0/0/от%2011%20февраля%202021%20г.%20N%2017:2			
Э22	https://docs.cntd.ru/document/1200021831			
Э23	https://docs.cntd.ru/document/1200082201			
Э24	https://elibr.mtuci.ru/view.php?book_id=170090			
6.3 Информационно-справочные системы и профессиональные базы данных				
6.3.1	Консультант Плюс – https://www.consultant.ru/			
6.3.2	Гарант – https://www.garant.ru/			
6.3.2	Консорциум Кодекс – https://docs.cntd.ru/			
6.3.3	Научная электронная библиотека – https://www.elibrary.ru/			
6.3.4	Профессиональная база данных: Федеральный портал «Российское образование»: [Электронный ресурс] – Режим доступа: http://www.edu.ru/ (открытый доступ)			
6.3.5	Профессиональная база данных: Федеральный центр информационно-образовательных ресурсов: [Электронный ресурс] – Режим доступа: http://fcior.edu.ru/ (открытый доступ)			
5.3.6	Национальный открытый университет «ИНТУИТ» - https://intuit.ru/			
5.3.7	Электронный ресурс http://www.securitylab.ru/			
6.4. Программное обеспечение				
СКФ МТУСИ обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:				
П.1	Linux (свободное ПО)			
П.2	LibreOffice (свободное ПО)			
6.5 Перечень информационных технологий, используемых при проведении Итоговой (государственной итоговой) аттестации				

Проведение Итоговой (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.

7. Материально-техническое обеспечение ИА

7.1 МТО выполнения ВКР
Лаборатория «Программно-аппаратные средства защиты информации», укомплектованная специализированной мебелью, оснащенную программно-аппаратными комплексами защиты информации, включающими в том числе средства криптографической защиты информации,
Учебные аудитории, оборудованные компьютерной техникой, с возможностью подключения к сети «Интернет», и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ
Лаборатория «Технические средства защиты информации», укомплектованная специализированной мебелью, оснащенную техническими средствами защиты информации
7.2 МТО защиты ВКР
Учебная аудитория СКФ МТУСИ, оборудованная ПК, ноутбуками и мультимедийными проекторами
7.3 МТО самостоятельной работы студентов
Помещение для самостоятельной работы обучающихся оснащено компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду СКФ МТУСИ

8. Методические указания по проведению ИА

Методические указания по оформлению и содержанию ВКР представлены в приложении 2 к настоящей программе.

9. Особенности проведения ИА для инвалидов и лиц с ограниченными возможностями здоровья

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

При проведении ИА обеспечивается соблюдение следующих общих требований:

- проведение итоговой (государственной итоговой) аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении итоговой (государственной итоговой) аттестации;
- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочесть и оформить задание, общаться с председателем и членами экзаменационной (государственной экзаменационной) комиссии);
- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении итоговой (государственной итоговой) аттестации с учетом их индивидуальных особенностей.

Обучающийся инвалид не позднее чем за 3 месяца до начала проведения итоговой (государственной итоговой) аттестации подает письменное заявление о необходимости создания для него специальных условий при проведении итоговых (государственных итоговых) аттестационных испытаний с указанием его индивидуальных особенностей. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей.

10. Дополнения и изменения в Рабочей программе

**Лист актуализации рабочей программы ИА
«Подготовка к процедуре защиты и защита
выпускной квалификационной работы БЗ.01»
для использования в 20___/20___ учебном году**

Утверждаю

Зам. директора по УР _____
«__» _____ 20__ г.

Направление: 10.03.01 Информационная безопасность

Профили: Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения: очная

(Возможны следующие варианты):

а) Рабочая программа действует без изменений.

б) В рабочую программу вносятся следующие изменения:

1)

2)

3)

Разработчик (и): _____
(ФИО, ученая степень, ученое звание)

«__» _____ 20__ г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБ

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

Заведующий кафедрой _____

Оценочные материалы (оценочные средства) ВКР

1. Компетенции, подлежащие оценке в выпускной квалификационной работе

Целью оценки уровня качества освоения ОПОП ВО по направлению 10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности) является проверка конечных результатов освоения ОПОП ВО, уровня освоения компетенций, подготовленности выпускников к заявленным в ОПОП видам профессиональной деятельности. В процессе итоговой (государственной итоговой) аттестации выпускник должен проявить свои компетенции, сформированные в течение всего периода обучения.

Выпускник, освоивший программу бакалавриата должен обладать универсальными, общепрофессиональными и профессиональными компетенциями, соответствующими виду профессиональной деятельности, на который ориентирована программа бакалавриата: УК-1 – УК-10, ОПК-1 – ОПК-13, ОПК-1.1 – ОПК-1.4, ПК-1 – ПК-3.

Для оценки результатов освоения ОПОП ВО в выпускной квалификационной работе выделены следующие компетенции:

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

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.

УК-3: Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде.

УК-4: Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах).

УК-5: Способен воспринимать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах.

УК-6: Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни.

УК-7: Способен поддерживать должный уровень физической подготовленности для обеспечения полноценной социальной и профессиональной деятельности.

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.

УК-9: Способен принимать обоснованные экономические решения в различных областях жизнедеятельности.

УК-10: Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности.

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности.

ОПК-3: Способен использовать необходимые математические методы для решения задач профессиональной деятельности.

ОПК-4: Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности.

ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности.

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.

ОПК-7: Способен использовать языки программирования и технологии разработки программных средств для решения задач профессиональной деятельности.

ОПК-8: Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.

ОПК-9: Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности.

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.

ОПК-11: Способен проводить эксперименты по заданной методике и обработку их результатов.

ОПК-12: Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

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.

ОПК-1.1: Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах.

ОПК-1.2: Способен администрировать средства защиты информации в компьютерных системах и сетях.

ОПК-1.3: Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям.

ОПК-1.4: Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

ПК-1: Администрирование подсистем защиты информации в операционных системах.

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

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

2. Примерный 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

3. Требования к ВКР

3.1 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.

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

3.3 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".

3.4 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.

3.5 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.

3.6 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.

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

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

4. Критерии оценки итоговой (государственной итоговой) аттестации бакалавров

4.1. 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».

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

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

4.4. Итоговая оценка складывается из трех составляющих – оценки выполнения задания на ВКР, оценки рецензента и оценки качества защиты.

4.5. Критерии и оценки выполнения задания по ВКР приведены в таблице 1.

Таблица 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	Хорошо

	умение применять свои знания для выполнения пунктов задания, в которых нет явно указанных способов решения. Анализирует полученные результаты, делает правильные выводы	
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

4.6. 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";

Оценка «Отлично» 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 «Хорошо» – 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 «Удовлетворительно» – 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 «Неудовлетворительно» – тема ВКР не раскрыта, обнаруживается существенное непонимание задачи.

4.7. Критерии и оценки качества защиты ВКР приведены в таблице 2.

Таблица 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;	3

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

4.8. 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 ЭК, при этом голос председателя ЭК является решающим при возникновении спорных вопросов.

Методические указания по проведению Итоговой (государственной итоговой) аттестации

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

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

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

3. Результаты ИА выражаются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в день проведения защиты ВКР после оформления протоколов заседания ЭК.

4. Защиты выпускных квалификационных работ проводятся на открытых заседаниях ЭК 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.

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

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

7. По окончании ИА председатель ЭК составляет отчет о работе ЭК, в котором указываются:

- номер и дата приказа ректора МТУСИ об утверждении ЭК;
- состав ЭК 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 ИА, по совершенствованию качества подготовки выпускников.

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

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

10. Протоколы аттестационных испытаний ИА 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 № ____ от _____.202__г.

Выпускная квалификационная работа выполнена

Под руководством _____
(Фамилия и инициалы руководителя)

В государственную экзаменационную комиссию представлены следующие материалы:

1. Справка деканата _____
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 УР
 _____ Н.А. Андреева
 «___» «_____» 202__ г.

УТВЕРЖДАЮ

Директор СКФ МТУСИ
 _____ Д.Н. Карасев
 «___» «_____» 202__ г.

График подготовки защиты ВКР выпускников филиала 202__ года и сроки вручения дипломов выпускникам очного и заочного факультетов

Этапы	Сроки	Мероприятия	Контингент
6.	до 29.04.2__	Набор и распечатка черновиков приложений к дипломам бакалавров	вспомогательный персонал, зам. декана ФИК
7.	до 29.04.2__	Контроль представления ВКР дипломниками ОФО	зав. кафедрами, деканат ФИК
8.	до 16.05.2__	Контроль представления выпускниками законченных ВКР	зав. кафедрами, деканат ФИК
9.	до 20.05.2__	Работа с выпускниками по завершению выполнения ими ВКР и подготовке их к защите	зав. кафедрами, деканат ФИК
10.	до 20.05.2__	Направление приглашений иногородним членам ГЭК для участия в проведении защит выпускников филиала в мае-июне	зав. кафедрами, деканат ФИК
11.	до 23.05.2__	Заполнение приложений к дипломам бакалавров в электронном виде (без итогов защит)	вспомогательный персонал, зам. декана ФИК
12.	до 28.05.2__	Распечатка и проверка набранных приложений к дипломам бакалавров	вспомогательный персонал, зам. декана ФИК
13.	20.06.-30.06.2__	Организация и проведение защиты ВКР выпускниками ОФО филиала	зав. кафедрами, деканат ФИК
14.	С 25.06. по 03.07.2__	Подготовка дипломов, заполнение журналов и актов	ОК
15.	до 03.07.2__	Передача в отдел кадров СКФ приложений к дипломам выпускников ОФО	деканат и декан ФИК
16.	до 06.07.2__	Направление приглашений иногородним членам ГЭК для участия во вручении дипломов выпускников филиала в июле	зав. кафедрами, декан ФИК
17.	с 06. 07. по 09.07.2__	Подписание дипломов бакалавров в МТУСИ	ОК
18.	11.07.2__	Торжественное вручение дипломов выпускникам 4 курсов	ОК, зам. директора по УР, ФИК
19.	до 18.07.102	Прошивка всех дел	ОК

Начальник ОК

Зам. директора по ВиСМР

Зав. кафедрой ИТСС

Зав. кафедрой ИВТ

И.о. зав. кафедрой ИБ

11. Проверка текста пояснительной записки ВКР на оригинальность выполняется посредством Антиплагиат.Вуз.

12. Справка о заимствованиях в формате PDF в электронном виде прилагается к PDF – файлу пояснительной записки 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 ДБ _____

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».	1%, 7.05.202__ 33%, 20.05.2__ 33%, 5.06.202__

	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 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. Вопросы конструктивных разработок – не запланированы Заключение.	32%,23.06.202__ 1%,25.06.202__
--	--	--

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 202__ г.
4. Дата выдачи задания 25 января 202__ г.

Руководитель

Манин А.А., доцент кафедры ИБ, 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 ГЭК.