ПРИЛОЖЕНИЕ 4
к ОПОП-П по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2026 г.

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Область применения программы ГИА

Программа государственной итоговой аттестации (далее – ГИА) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

код *наименование специальности/профессии*

утвержденного Приказом Министерства образования и науки 9 декабря 2016 года № 1551 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44944).

Квалификация выпускника: техник по защите информации.

Образовательная программа реализуется на базе основного общего образования.

Программа государственной итоговой аттестации (далее – программа ГИА) выпускников по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем разработана в соответствии с Законом Российской Федерации от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации», Приказом Минпросвещения России от 08.11.2021 № 800 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования», ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, и определяет совокупность требований к ее организации и проведению.

Цель государственной итоговой аттестации – установление соответствия результатов освоения обучающимися образовательной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем соответствующим требованиям ФГОС СПО с учетом требований регионального рынка труда, их готовность и способность решать профессиональные задачи.

Задачи государственной итоговой аттестации:

– определение соответствия навыков, умений и знаний выпускников современным требованиям рынка труда, квалификационным требованиям ФГОС СПО и регионального рынка труда;

– определение степени сформированности профессиональных компетенций, личностных качеств, соответствующих ФГОС СПО и наиболее востребованных на рынке труда.

По результатам ГИА выпускнику по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем присваивается квалификация: Техник по защите информации.

Программа ГИА является частью ОПОП-П по программе подготовки специалистов среднего звена и определяет совокупность требований к ГИА, в том числе к содержанию, организации работы, оценочным материалам ГИА выпускников по данной специальности.

Выпускник, освоивший образовательную программу, должен быть готов к выполнению видов деятельности, предусмотренных образовательной программой (таблица 1), и демонстрировать результаты освоения образовательной программы (таблица 2).

Таблица 1

Виды деятельности

Код и наименование вида деятельности (ВД)	**Код и наименование профессионального модуля (ПМ), в рамках которого осваивается ВД**
1	2
В соответствии с ФГОС	
Эксплуатация информационно-телекоммуникационных систем и сетей	ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
Защита информации в информационно-телекоммуникационных системах и сетях с	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты
Освоение видов работ по одной или нескольким профессиям рабочих, должностям служащих	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих

Таблица 2

Перечень результатов, демонстрируемых выпускником

Оцениваемые виды деятельности	Профессиональные компетенции
ВД.1 Эксплуатация информационно-телекоммуникационных систем и сетей	ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей.
	ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.
	ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей.
	ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.
ВД.2 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей
	ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях
	ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с

	предъявляемыми требованиями
ВД.3 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.
	ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.
	ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
	ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.
	ПК 3.5. Пользоваться нормативно-технической документацией в области защиты информации
ВД.4 Освоение видов работ по одной или нескольким профессиям рабочих, должностям служащих	ПК 4.1 Выполнять монтаж, демонтаж и техническое обслуживание кабелей связи и оконечных структурированных кабельных устройств в соответствии с действующими отраслевыми стандартами.
ВД.5 Квантовые технологии в цифровых сетях	ПК 5.1 Производить установку, монтаж, настройку и испытания компьютерных и транспортных информационно-телекоммуникационных систем и сетей. ПК 5.2 Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт компьютерных и транспортных информационно-телекоммуникационных систем и сетей ПК 5.3 Сборка и настройка систем квантового распределения ключа ПК 5.4 Осуществлять подбор соответствующих оптических элементов ПК 5.5 Защита гибридных и мультиоблачных сред
ВД.6 Выполнение работ по профессии 16199 "Оператор электронно-вычислительных и вычислительных машин"	ПК 6.1 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах ПК 6.2 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета

Выпускники, освоившие программу по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем, сдают ГИА в форме демонстрационного экзамена профильного уровня и защиты дипломного проекта (работы).

Для выпускников, осваивающих образовательные программы в области подготовки кадров в интересах обороны и безопасности государства, обеспечения законности и правопорядка государственная итоговая аттестация проводится в форме демонстрационного экзамена и защиты дипломного проекта (работы).

1.2. Цели и задачи государственной итоговой аттестации

Целью государственной итоговой аттестации является установление соответствия

уровня освоенности компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся, Федеральному государственному образовательному стандарту среднего профессионального образования. ГИА призвана способствовать систематизации и закреплению знаний и умений обучающегося по специальности при решении конкретных профессиональных задач, определить уровень подготовки выпускника к самостоятельной работе.

1.3. Нормативные правовые документы и локальные акты, регулирующие вопросы организации и проведения ГИА

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с изменениями);

2. Федеральный государственный стандарт среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», утвержденный Приказом Министерства образования и науки 9 декабря 2016 года № 1551 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44944)

3. Приказ Министерства просвещения Российской Федерации от 24 августа 2022 г. №762 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;

4. Приказ Министерства просвещения Российской Федерации от 8 ноября 2021 г. №800 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования»;

5. Приказ Министерства просвещения Российской Федерации от 17 мая 2022 г. №336 «Об утверждении перечней профессий и специальностей среднего профессионального образования и установлении соответствия отдельных профессий и специальностей среднего профессионального образования, указанных в этих перечнях, профессиям и специальностям среднего профессионального образования, перечни которых утверждены приказом Министерства образования и науки Российской Федерации от 29 октября 2013 г. № 1199 «Об утверждении перечней профессий и специальностей среднего профессионального образования»;

6. Положение о проведении государственной итоговой аттестации с использованием механизма демонстрационного экзамена

1.4 Формы проведения государственной итоговой аттестации

Государственная итоговая аттестация проводится в форме демонстрационного экзамена и защиты дипломного проекта (работы).

1.5 Требования к уровню подготовки выпускника по профессиональной образовательной программе в соответствии с ФГОС СПО

1.5.1 Владеть навыками:

– монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС;

– текущем контроле функционирования оборудования ИТКС;

– проведении технического обслуживания, диагностике технического состояния, поиске неисправностей и ремонте оборудования ИТКС.

– установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей;

– поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях;

– защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

– установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам;

– защите информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;

– проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей;

– монтажа, настройки, проверки функционирования и конфигурирования оборудования компьютерных сетей

1.5.2 Уметь

– осуществлять техническую эксплуатацию линейных сооружений связи;

– производить монтаж кабельных линий и оконечных кабельных устройств;

– настраивать, эксплуатировать и обслуживать оборудование ИТКС;

– осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС;

– производить испытания, проверку и приемку оборудования ИТКС;

– проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС.

– выявлять и оценивать угрозы безопасности информации в ИТКС;

– настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;

– проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;

– проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации;

– проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

– проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации;

– проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.

– проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

– проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;

– проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;

– проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;

– использовать средства физической защиты линий связи ИТКС;

– применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– осуществлять техническую эксплуатацию компьютерных сетей

1.5.3 Знать

– принципы построения и основных характеристик информационно-телекоммуникационных систем и сетей (далее - ИТКС);

– принципы передачи информации в ИТКС;

– виды и характеристики сигналов в ИТКС;

– виды помех в каналах связи ИТКС и методы защиты от них;

– разновидности линий передач, конструкции и характеристики электрических и оптических кабелей связи;

– технологии и оборудование удаленного доступа в ИТКС;

– принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС.

– возможные угрозы безопасности информации в ИТКС;

– способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее;

– типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях;

– криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях;

– порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации;

– организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации;

– порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.

– способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;

– основные типы технических средств защиты информации от утечки по техническим каналам;

– методики измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;

– организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;

– порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;

– содержание и организацию работ по физической защите линий связи ИТКС;

– принципы действия и основные характеристики технических средств физической защиты;

– законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;

– принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях;

– принципы построения и основные характеристики компьютерных сетей.

1.5.4 Выпускник, освоивший образовательную программу, должен обладать следующими общими компетенциями:

ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде

ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное

поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках

1.5.5 Выпускник, освоивший образовательную программу, должен обладать профессиональными компетенциями, соответствующими основным видам деятельности:

ВД 1. Эксплуатация информационно-телекоммуникационных систем и сетей:

ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.

ВД 2. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты:

ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.

ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

ВД 3. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты:

ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.

ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.

ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.

ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

ПК 3.5. Пользоваться нормативно-технической документацией в области защиты информации

ВД.4 Выполнение работ по профессии монтажник оборудования связи 14601

ПК 4.1 Выполнять монтаж, демонтаж и техническое обслуживание кабелей связи и оконечных структурированных кабельных устройств в соответствии с действующими отраслевыми стандартами.

ВД.5 Технология эксплуатации цифровых сетей связи

ПК 5.1 Производить установку, монтаж, настройку и испытания компьютерных и транспортных информационно-телекоммуникационных систем и сетей.

ПК 5.2 Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт компьютерных и транспортных информационно-телекоммуникационных систем и сетей

ПК 5.3 Сборка и настройка систем квантового распределения ключа

ПК 5.4 Осуществлять подбор соответствующих оптических элементов

ПК 5.5 Защита гибридных и мультиоблачных сред

ВД.6 Выполнение работ по профессии 16199 "Оператор электронно-вычислительных и вычислительных машин"

ПК 6.1 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах

ПК 6.2 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета

2. ПРОЦЕДУРА ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Проведение демонстрационного экзамена

2.1.1 Требования к проведению демонстрационного экзамена

Демонстрационный экзамен **профильного уровня** проводится по решению образовательной организации на основании заявлений выпускников на основе требований к результатам освоения образовательных программ среднего профессионального образования, установленных в соответствии с ФГОС СПО, включая квалификационные требования, заявленные организациями, работодателями, заинтересованными в подготовке кадров соответствующей квалификации, в том числе являющимися стороной договора о сетевой форме реализации образовательных программ и (или) договора о практической подготовке обучающихся (далее - организации-партнеры).

Демонстрационный экзамен проводится с использованием единых оценочных материалов, включающих в себя конкретные комплекты оценочной документации, варианты заданий и критерии оценивания (далее – оценочные материалы), выбранные образовательной организацией, исходя из содержания реализуемой образовательной программы, из размещенных на официальном сайте оператора в сети «Интернет» единых оценочных материалов.

Комплект оценочной документации (КОД) включает комплекс требований для проведения демонстрационного экзамена, перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания, примерный план застройки площадки демонстрационного экзамена, требования к составу экспертных групп, инструкции по технике безопасности, а также образцы заданий.

2.1.2 Выбор оценочной документации для демонстрационного экзамена

Демонстрационный экзамен предусматривает моделирование реальных производственных условий для решения практических задач профессиональной деятельности в соответствии с лучшими мировыми и национальными практиками.

Для проведения демонстрационного экзамена по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» выбран комплект оценочной документации (КОД) шифр КОД 10.02.04-1-2024, наименование квалификации – Техник по

защите информации, уровень –профильный.

2.1.2 Сроки и место проведения демонстрационного экзамена

Объем времени и сроки, отводимые на подготовку к демонстрационному экзамену: 2 недели, май, июнь.

Сроки проведения демонстрационного экзамена: 1 неделя, май-июнь.

Место проведения демонстрационного экзамена – Центр проведения демонстрационного экзамена по адресу: г.Уфа, ул. Генерала Горбатова, 11.

КОД рассчитан на выполнение заданий продолжительностью – 4 часа 30 мин.

2.1.3 Единое базовое ядро содержания КОД, сформированное на основе вида деятельности в соответствии с ФГОС СПО, включает в себя

Таблица 1 – Единое базовое ядро содержания КОД

Вид деятельности / Вид профессиональной деятельности	Перечень оцениваемых ПК/ОК	Перечень оцениваемых умений, навыков (практического опыта)
Эксплуатация информационно коммуникационных систем и сетей	ПК: Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей	Умение: осуществлять техническую эксплуатацию линейных сооружений связи
		Умение: производить монтаж кабельных линий и оконечных кабельных устройств
		Умение: осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС
		Практический опыт: в монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС
		Умение: производить испытания, проверку и приемку оборудования ИТКС
		Практический опыт: в текущем контроле функционирования оборудования ИТКС
		Практический опыт: в проведении технического обслуживания, диагностике технического состояния, поиске неисправностей и ремонте оборудования ИТКС

Содержательная структура КОД в соответствии с выбранным уровнем ДЭ включает в себя

Таблица 2 – Содержательная структура КОД

Вид деятельности / Вид профессиональной деятельности	Перечень оцениваемых ПК/ОК	Перечень оцениваемых умений, навыков (практического опыта)

Эксплуатация информационно коммуникационных систем и сетей	ПК:Производить монтаж, настройку и проверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей	Умение: осуществлять техническую эксплуатацию линейных сооружений связи
		Умение: производить монтаж кабельных линий и оконечных кабельных устройств
		Умение: осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС
		Практический опыт: в монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС
		Умение: производить испытания, проверку и приемку оборудования ИТКС
		Практический опыт: в текущем контроле функционирования оборудования ИТКС
		Практический опыт: в проведении технического обслуживания, диагностике технического состояния, поиске неисправностей и ремонте оборудования ИТКС
Защита информации в информационно-коммуникационных системах и сетях с использованием программных, программно-аппаратных, в том числе криптографических средств защиты	ПК: Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей	Умение: выявлять и оценивать угрозы безопасности информации в ИТКС
		Умение: проводить установку и настройку программных и программно-аппаратных, в том числе криптографических, средств защиты информации
		Умение: проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации
		Практический опыт: в установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании
	ПК: Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств щиты информации информационно – телекоммуникационных системах и сетях	Умение: выявлять и оценивать угрозы безопасности информации в ИТКС
		Умение: проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических) средств защиты информации
		Практический опыт: в поддержании бесперебойной работы про-

		граммных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно телекоммуникационных системах и сетях
	ПК: Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – коммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями	Умение: выявлять и оценивать угрозы безопасности информации в ИТКС
		Умение: проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации
		Практический опыт: в защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями

Содержательная структура вариативной части КОД для ДЭ ПУ (квалификационные требования работодателей) представлена в таблице 3.

Таблица 3 - Содержательная структура вариативной части КОД для ДЭ ПУ

Вид деятельности / Вид профессиональной деятельности	**Перечень оцениваемых компетенций (ОК/ПК)**	**Перечень оцениваемых умений, навыков (практического опыта)**
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.	**Знать:** порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.
		Знать: проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации;
		Навыки: защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, в том числе криптографических средств защиты в соответствии с предъявляемыми требованиями.

Образец задания демонстрационного экзамена представлен в приложении 2.

2.2 Защита дипломного проекта (работы)

2.2.1 Организация и проведение защиты дипломного проекта (работы)

Программа организации проведения защиты дипломного проекта (работы) как формы ГИА включает общие положения, тематику, структуру и содержание дипломного проекта (работы), порядок оценки результатов дипломного проекта (работы).

Дипломный проект (работа) направлен на систематизацию и закрепление знаний выпускника по специальности, а также определение уровня готовности выпускника к самостоятельной профессиональной деятельности. Дипломный проект (работа) предполагает самостоятельную подготовку (написание) выпускником проекта (работы), демонстрирующего уровень знаний выпускника в рамках выбранной темы, а также сформированность его профессиональных умений и навыков.

Тематика дипломных проектов (работ) определяется образовательной организацией. Выпускнику предоставляется право выбора темы дипломного проекта (работы), в том числе предложения своей темы с необходимым обоснованием целесообразности ее разработки для практического применения. Тема дипломного проекта (работы) должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу среднего профессионального образования.

Для подготовки дипломного проекта (работы) выпускнику назначается руководитель и при необходимости консультанты, оказывающие выпускнику методическую поддержку.

Закрепление за выпускниками тем дипломных проектов (работ), назначение руководителей и консультантов осуществляется распорядительным актом образовательной организации.

Тематику дипломных проектов (работ), структуру и содержание дипломного проекта (работы), порядок оценки результатов и систему оценивания образовательная организация разрабатывает самостоятельно.

2.2.2 Сроки защиты выпускной квалификационной работы

Объем времени и сроки, отводимые на выполнение выпускной квалификационной работы: 2 недели, май,июнь.

Сроки защиты дипломного проекта (работы): 1 неделя, июнь.

2.2.3 Темы дипломного проекта (работы)

Темы дипломного проекта (работы) должны иметь практико-ориентированный характер и должны соответствовать содержанию одного или нескольких профессиональных модулей ПМ.01 «Эксплуатация информационно-телекоммуникационных систем и сетей», ПМ.02 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты», ПМ.03 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты», ПМ.04 Выполнение работы по профессии рабочего «Монтажник оборудования связи» специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

Темы выпускных квалификационных работ с указанием руководителя закрепляются за студентом приказом директора колледжа.

Примерная тематика выпускных квалификационных работ представлена в приложении 1.

3 ТРЕБОВАНИЯ К ДИПЛОМНОМУ ПРОЕКТУ (РАБОТЕ)

3.1 Требования к структуре дипломного проекта (работы)

Структура дипломного проекта (работы) должна включать:

- титульный лист;
- индивидуальный график выполнения дипломного проекта (работы);
- задание на дипломный проект (работу);
- отзыв руководителя дипломного проекта (работы);
- внешняя рецензия;
- пояснительная записка:
    - введение с обоснованием актуальности и практической значимости выбранной темы;
    - общая часть;
    - специальная часть;
    - заключение;
    - список литературы;
    - приложения;
- графическая часть;

Объем дипломного проекта (работы) должен быть не менее 30 страниц машинописного текста.

Требования к содержанию разделов дипломного проекта (работы) описаны в Методических указаниях по выполнению дипломного проекта (работы).

Требования по оформлению дипломного проекта (работы) описаны в Методических рекомендациях по оформлению дипломного проекта (работы).

3.2 Условия подготовки и процедура проведения защиты дипломного проекта (работы)

3.2.1 Условия подготовки дипломного проекта (работы):

К Государственной (итоговой) аттестации допускается студент, не имеющий академической задолженности и в полном объеме выполнивший учебный план по осваиваемой образовательной программе среднего профессионального образования.

После утверждения темы руководителями дипломного проекта (работы) разрабатываются индивидуальные задания. Индивидуальные задания рассматриваются кафедрами и утверждаются заместителем директора УКРТБ.

Индивидуальные задания на дипломный проект (работу) выдаются студентам за 2 недели до начала преддипломной практики.

Общее руководство и контроль за ходом выполнения дипломного проекта (работы) осуществляется заместителем директора УКРТБ, заведующими отделениями, заведующим кафедрой в соответствии с должностными обязанностями.

3.2.2 Защита дипломного проекта (работы)

Допуск к защите дипломного проекта (работы) оформляется приказом директора колледжа.

Защита дипломного проекта (работы) проводится на открытом заседании Государственной экзаменационной комиссии (ГЭК).

На защиту дипломного проекта (работы) отводится 45 минут. Процедура защиты:

- доклад студента 10-15 минут;
- чтение отзыва и рецензии (не более 5 минут);
- вопросы членов ГЭК и ответы студента (не более 15 минут);
- по желанию (необходимости) выступление руководителя дипломного проекта (работы) и рецензента (если они присутствуют на заседании ГЭК) с целью защиты, согласия или несогласия с оценкой конкретной дипломного проекта (работы) (не более 15 минут).

Заседание ГЭК протоколируется. В протоколе записываются:

- итоговая оценка дипломного проекта (работы);
- присуждение квалификации;
- особое мнение членов комиссии.

4. ОЦЕНКА РЕЗУЛЬТАТОВ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

4.1 Оценка результатов выполнения заданий демонстрационного экзамена

Оценку выполнения заданий демонстрационного экзамена осуществляет экспертная группа из числа лиц, приглашенных из сторонних организаций и обладающих профессиональными знаниями, навыками и опытом в сфере, соответствующей профессии или специальности среднего профессионального образования или укрупненной группы профессий и специальностей, по которой проводится демонстрационный экзамен, возглавляемая главным экспертом. Главный эксперт организует и контролирует деятельность возглавляемой экспертной группы, обеспечивает соблюдение всех требований к проведению демонстрационного экзамена и не участвует в оценивании результатов демонстрационного экзамена.

Состав экспертной группы утверждается руководителем образовательной организации. Количество экспертов, участвующих в оценке демонстрационного экзамена по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» – 3 человека.

В день проведения демонстрационного экзамена в центре проведения экзамена присутствуют:

а) руководитель (уполномоченный представитель) организации, на базе которой организован центр проведения экзамена;

б) не менее одного члена ГЭК, не считая членов экспертной группы;

в) члены экспертной группы;

г) главный эксперт;

д) представители организаций-партнеров (по согласованию с образовательной организацией);

е) выпускники;

ж) технический эксперт;

з) представитель образовательной организации, ответственный за сопровождение выпускников к центру проведения экзамена (при необходимости);

и) тьютор (ассистент), оказывающий необходимую помощь выпускнику из числа лиц с ограниченными возможностями здоровья, детей-инвалидов, инвалидов (далее - тьютор (ассистент);

к) организаторы, назначенные образовательной организацией из числа педагогических работников, оказывающие содействие главному эксперту в обеспечении соблюдения всех требований к проведению демонстрационного экзамена.

В случае отсутствия в день проведения демонстрационного экзамена в центре проведения экзамена вышеперечисленных лиц, решение о проведении демонстрационного экзамена принимается главным экспертом, о чём главным экспертом вносится соответствующая запись

в протокол проведения демонстрационного экзамена.

Баллы за выполнение заданий демонстрационного экзамена выставляются в соответствии со схемой начисления баллов, приведенной в комплекте оценочной документации.

Таблица 4 – Распределение баллов по критериям оценивания

№ п/п	**Модуль задания** (вид деятельности, видпрофессиональной деятельности)	**Критерий оценивания**[7]	**Баллы**
1	Эксплуатация информационно –телекоммуникационных систем и сетей	Производство монтажа, настройки, проверки функционирования и конфигурирование оборудования информационно- телекоммуникационных систем и сетей	**9,00**
		Использование информационных технологий в профессиональной деятельности	**2,00**
2	Защита информации в информационно –телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	Производство установки, настройки, испытаний и конфигурирования программных и программно- аппаратных, в том числе криптографических средств защитыинформации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	**12,00**
		Поддержка бесперебойной работы программных и программно- аппаратных, в том числе криптографических средств защиты информации в информационно- телекоммуникационных системах и сетях	**3,00**
3	Эксплуатация информационно –телекоммуникационных систем и сетей	Осуществление контроля функционирования информационно – телекоммуникационных систем и сетей	**6,00**
4	Защита информации в информационно–телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе	Производство установки, настройки, испытаний и конфигурирования программных и программно- аппаратных, в том числе криптографических средств защиты информации от	**6,00**

[7] Формулировка критерия оценивания совпадает с наименованием ПК, ОК и начинается с отглагольногосуществительного.

	криптографических средств защиты	несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей	
		Поддержка бесперебойной работы программных и программно- аппаратных, в том числе криптографических средств защитыинформации в информационно-телекоммуникационных системах и сетях	**6,00**
		Осуществление защитыинформации от несанкционированных действий испециальных воздействий винформационно- телекоммуникационных системах исетях с использованием программных и программно-аппаратных, в том числекриптографических средств всоответствии с предъявляемыми требованиями	**6,00**
5	Эксплуатация информационно –телекоммуникационных систем и сетей	Осуществление контроляфункционирования информационно – телекоммуникационных систем исетей	**14,00**
6	Защита информации в информационно –телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	Поддержка бесперебойной работы программных и программно- аппаратных, в том числе криптографических средств защитыинформации в информационно- телекоммуникационных системах и сетях	**10,00**
		Осуществление защиты информации от Несанкционированных действий и специальных воздействий в информационно- телекоммуникационных системах и сетях с использованием программных и программно- аппаратных в том числе криптографических средств в соответствии с предъявляемыми требованиями	**6,00**
Вариативная часть			
7	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	Разрабатывать документацию к существующей или проектируемой информационной структуре предприятия.	5,00
		Точно описывать инцидент и документировать решение проблемы;	5,00
		Осуществлять поиск информации в открытых источниках и работать с технической документацией.	5,00

		Формировать базу знаний.	5,00
ИТОГО (инвариантная часть)			**80,00**
ВСЕГО (вариативная часть)[8]			**20,00**
ИТОГО (совокупность инвариантной и вариативной частей)			**100,00**

Необходимо осуществить перевод полученного количества баллов в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100%. Перевод баллов в оценку может быть осуществлен на основе таблицы 5.

Таблица 5 – Перевод баллов в оценку

Оценка	"2"	"3"	"4"	"5"
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 11,99%	12,00% - 34,99%	35,00% - 69,99%	70,00% - 100,00%

Таким образом, получаем следующее распределение баллов.

Таблица 6 – Перевод баллов в оценку в соответствии с КОД

Оценка ГИА	«2»	«3»	«4»	«5»
Количество баллов	0,00 – 11,99	12-34,99	35-69,99	70-100

Баллы выставляются в протоколе проведения демонстрационного экзамена, который подписывается каждым членом экспертной группы и утверждается главным экспертом после завершения экзамена для экзаменационной группы.

При выставлении баллов присутствует член ГЭК, не входящий в экспертную группу, присутствие других лиц запрещено.

Подписанный членами экспертной группы и утвержденный главным экспертом протокол проведения демонстрационного экзамена далее передается в ГЭК для выставления оценок по итогам ГИА.

Статус победителя, призера финала чемпионата по профессиональному мастерству "Профессионалы" и финала чемпионата высоких технологий по профилю осваиваемой образовательной программы среднего профессионального образования засчитывается выпускнику в качестве оценки "отлично" по демонстрационному экзамену в рамках проведения ГИА по данной образовательной программе среднего профессионального образования (Пункт в редакции, введенной в действие с 1 марта 2026 года приказом Минпросвещения России от 22 ноября 2024 года N 812. - См. предыдущую редакцию)

В случае досрочного завершения ГИА выпускником по независящим от него причинам результаты ГИА оцениваются по фактически выполненной работе, или по заявлению такого выпускника ГЭК принимается решение об аннулировании результатов ГИА, а такой выпускник признается ГЭК не прошедшим ГИА по уважительной причине.

4.2 Оценка выпускной квалификационной работы

4.2.1 Критерии оценки выпускной квалификационной работы

- соответствие названия работы ее содержанию, четкая целевая направленность;
- логическая последовательность изложения материала;
- необходимая глубина исследования и убедительность аргументации;
- конкретность представления практических результатов работы;
- соответствие оформления выпускной квалификационной работы требованиям ГОСТ

Р 705 -2008 и методическим рекомендациям по оформлению выпускных квалификационных работ.

4.2.2 Критерии оценки защиты выпускной квалификационной работы

- четкость и грамотность доклада;
- четкость, внятность, глубина ответов на вопросы присутствующих на заседании ГАК;
- использование технических средств для сопровождения доклада.

4.2.3 Определение окончательной оценки

При определении окончательной оценки за защиту дипломного проекта (работы) учитываются:

- доклад выпускника по каждому разделу выпускной работы;
- ответы на вопросы;
- оценка рецензента;
- отзыв руководителя.

«Отлично» выставляется за следующую выпускную квалификационную работу:

- работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, глубокий анализ проблемы, характеризуется логичным, последовательным изложением материала с соответствующими выводами и обоснованными предложениями;
- имеет положительные отзывы руководителя и рецензента;
- при защите работы студент показывает глубокие знания вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, во время доклада использует презентацию и наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, легко отвечает на поставленные вопросы.

«Хорошо» выставляется за следующую выпускную квалификационную работу:

- работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, достаточно подробный анализ проблемы, характеризуется последовательным изложением материала с соответствующими выводами, однако с не вполне обоснованными предложениями;
- имеет положительный отзыв руководителя и рецензента;
- при защите студент показывает знания вопросов темы, оперирует данными исследования, вносит предложения, во время доклада использует презентацию и наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, без особых затруднений отвечает на поставленные вопросы.

«Удовлетворительно» выставляется за следующую выпускную квалификационную работу:

- носит исследовательский характер, содержит теоретическую главу, базируется на практическом материале, но отличается поверхностным анализом проблемы, в ней просматривается непоследовательность изложения материала, представлены необоснованные предложения;
- в отзывах руководителя и рецензента имеются замечания по содержанию работы и методике анализа;
- при защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не дает полного, аргументированного ответа на заданные вопросы.

«Неудовлетворительно» выставляется за следующую выпускную квалификационную работу:

- не носит исследовательского характера, не содержит анализа проблемы, не отвечает требованиям, изложенным в методических указаниях;
- не имеет выводов либо они носят декларативный характер;
- в отзывах руководителя и рецензента имеются существенные критические замечания;
- при защите студент затрудняется отвечать на поставленные вопросы по теме, не знает теории вопроса, при ответе допускает существенные ошибки, к защите не подготовлены презентация, наглядные пособия или раздаточный материал.

Общая оценка защиты принимается на закрытых заседаниях простым большинством голосов членов ГЭК, участвующих в заседании, при обязательном присутствии председателя

комиссии или его заместителя. При равном числе голосов голос председательствующего на заседании ГЭК является решающим.

4.3 Общая оценка государственной итоговой аттестации

Общая оценка ГИА выставляется по результатам сдачи демонстрационного экзамена и защиты выпускной квалификационной работы.

Решения ГЭК принимаются на закрытых заседаниях простым большинством голосов членов ГЭК, участвующих в заседании, при обязательном присутствии председателя комиссии или его заместителя. При равном числе голосов голос председательствующего на заседании ГЭК является решающим.

Решение ГЭК оформляется протоколом, который подписывается председателем ГЭК, в случае его отсутствия заместителем ГЭК и секретарем ГЭК и хранится в архиве образовательной организации.

По результатам ГИА составляется отчет по итогам работы государственной экзаменационной комиссии за подписью председателя ГЭК.

5 ПОРЯДОК АПЕЛЛЯЦИИ И ПЕРЕСДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

5.1 Порядок подачи и рассмотрения апелляций

По результатам государственной итоговой аттестации, проводимой с применением механизма демонстрационного экзамена или защиты выпускной квалификационной работы, выпускник имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, установленного порядка проведения государственной итоговой аттестации и (или) несогласии с ее результатами.

Апелляция подается лично выпускником в апелляционную комиссию колледжа.

Апелляция о нарушении порядка проведения итоговой аттестации в форме демонстрационного экзамена подается непосредственно в день проведения до выхода их центра проведения экзамена. Апелляция о нарушении порядка проведения итоговой аттестации в форме защиты выпускной квалификационной работы подается непосредственно в день проведения защиты.

Апелляция о несогласии с результатами ГИА подается не позднее следующего рабочего дня после объявления результатов ГИА.

Апелляция рассматривается апелляционной комиссией не позднее трех рабочих дней с момента ее поступления.

Состав апелляционной комиссии утверждается образовательной организацией одновременно с утверждением состава ГЭК. Апелляционная комиссия состоит из председателя апелляционной комиссии, не менее пяти членов апелляционной комиссии и секретаря апелляционной комиссии из числа педагогических работников образовательной организации, не входящих в данном учебном году в состав ГЭК. Председателем апелляционной комиссии может быть назначено лицо из числа руководителей или заместителей руководителей организаций, осуществляющих образовательную деятельность, соответствующую области профессиональной деятельности, к которой готовятся выпускники, представителей организаций-партнеров или их объединений, включая экспертов, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся выпускники, при условии, что такое лицо не входит в состав ГЭК.

Апелляция рассматривается на заседании апелляционной комиссии с участием не менее двух третей ее состава. На заседание апелляционной комиссии приглашается председатель соответствующей ГЭК, а также главный эксперт при проведении ГИА в форме демонстрационного экзамена. При проведении ГИА в форме демонстрационного экзамена по решению председателя апелляционной комиссии к участию в заседании комиссии могут быть также

привлечены члены экспертной группы, технический эксперт.

По решению председателя апелляционной комиссии заседание апелляционной комиссии может пройти с применением средств видео, конференц-связи, а равно посредством предоставления письменных пояснений по поставленным апелляционной комиссией вопросам.

Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции.

Рассмотрение апелляции не является пересдачей ГИА.

При рассмотрении апелляции о нарушении Порядка апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из следующих решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях Порядка не подтвердились и (или) не повлияли на результат ГИА;

- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях Порядка подтвердились и повлияли на результат ГИА.

В последнем случае результаты проведения ГИА подлежат аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в ГЭК для реализации решения апелляционной комиссии. Выпускнику предоставляется возможность пройти ГИА в дополнительные сроки, установленные образовательной организацией без отчисления такого выпускника из образовательной организации в срок не более четырёх месяцев после подачи апелляции.

В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при прохождении демонстрационного экзамена, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания ГЭК, протокол проведения демонстрационного экзамена, письменные ответы выпускника (при их наличии), результаты работ выпускника, подавшего апелляцию, видеозаписи хода проведения демонстрационного экзамена (при наличии).

В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите дипломного проекта (работы), секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию дипломный проект (работу), протокол заседания ГЭК.

В случае рассмотрения апелляции о несогласии с результатами ГИА, полученными при сдаче демонстрационного экзамена, секретарь ГЭК не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания ГЭК, письменные ответы выпускника (при их наличии).

В результате рассмотрения апелляции о несогласии с результатами ГИА апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата ГИА либо об удовлетворении апелляции и выставлении иного результата ГИА. Решение апелляционной комиссии не позднее следующего рабочего дня передается в ГЭК. Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов ГИА выпускника и выставления новых результатов в соответствии с мнением апелляционной комиссии.

Решение апелляционной комиссии принимается простым большинством голосов. При равном числе голосов голос председательствующего на заседании апелляционной комиссии является решающим.

Решение апелляционной комиссии доводится до сведения подавшего апелляцию выпускника в течение трех рабочих дней со дня заседания апелляционной комиссии.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Решение апелляционной комиссии оформляется протоколом, который подписывается председателем (заместителем председателя) и секретарем апелляционной комиссии и хранится в архиве образовательной организации.

5.2 Порядок пересдачи Государственной итоговой аттестации

В случае досрочного завершения ГИА выпускником по независящим от него причинам результаты ГИА оцениваются по фактически выполненной работе, или по заявлению такого выпускника ГЭК принимается решение об аннулировании результатов ГИА, а такой выпускник признается ГЭК не прошедшим ГИА по уважительной причине.

Выпускникам, не прошедшим ГИА по уважительной причине, в том числе не явившимся по уважительной причине для прохождения одного из аттестационных испытаний, предусмотренных формой ГИА (далее - выпускники, не прошедшие ГИА по уважительной причине), предоставляется возможность пройти ГИА, в том числе не пройденное аттестационное испытание (при его наличии), без отчисления из образовательной организации.

Дополнительные заседания ГЭК организуются в установленные образовательной организацией сроки, но не позднее четырех месяцев после подачи заявления выпускником, не прошедшим ГИА по уважительной причине.

Выпускники, не прошедшие ГИА по неуважительной причине, в том числе не явившиеся для прохождения ГИА без уважительных причин (далее - выпускники, не прошедшие ГИА по неуважительной причине) и выпускники, получившие на ГИА неудовлетворительные результаты, могут быть допущены образовательной организацией для повторного участия в ГИА не более двух раз.

Выпускники, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на ГИА неудовлетворительные результаты, отчисляются из образовательной организации и проходят ГИА не ранее чем через шесть месяцев после прохождения ГИА впервые.

Для прохождения ГИА выпускники, не прошедшие ГИА по неуважительной причине, и выпускники, получившие на ГИА неудовлетворительные результаты, восстанавливаются в образовательной организации на период времени, установленный образовательной организацией самостоятельно, но не менее предусмотренного календарным учебным графиком для прохождения ГИА соответствующей образовательной программы среднего профессионального образования.

Приложение 1

Примерная тематика выпускных квалификационных работ

1. Разработка списков контроля доступа к внешним и внутренним ресурсам организации.
2. Разработка системы контроля и управления доступом.
3. Разработка и построение системы безопасности сети.
4. Разработка корпоративной сети с применением различных технологий.
5. Разработка процессов оптимизации и обеспечение безопасности компьютерной сети организации.
6. Проектирование систем видеонаблюдения.
7. Разработка защищенной локальной вычислительной сети предприятия.
8. Разработка комплексной защиты предприятия.
9. Построение защиты информационных систем персональных данных предприятия.
10. Проектирование систем ОПС.
11. Разработка системы защиты персональных данных на предприятии
12. Модернизация и построение защиты локальной вычислительной сети предприятия.
13 Разработка системы защиты информации от спама.

Приложение 2.
План мероприятий по организации проведения демонстрационного экзамена в рамках государственной итоговой аттестации выпускников

	Время	Мероприятие
День Д-1 (поток 1,2)	8:30 – 08:40	Получение главным экспертом задания демонстрационного экзамена
	08:40 – 08:50	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности/неготовности
	08:50 – 09:00	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение Протокола о распределении
	09:00 – 09:30	Инструктаж экспертной группы по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	09:30 – 09:50	**Регистрация участников ДЭ (поток 1)**
	09:50 – 10:00	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	10:00 – 11:00	Распределение рабочих мест (жеребьевка) и ознакомление участников с рабочими местами, оборудованием, графиком работы
	11:00 – 11:20	**Регистрация участников ДЭ (поток 2)**
	11:20 – 11:30	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	11:50 – 12:30	Распределение рабочих мест (жеребьевка) и ознакомление участников с рабочими местами, оборудованием, графиком работы
	12:30 – 13:00	Обед
День Д1 (поток 1)	08:00 – 08:15	Печать задания. Ознакомление с заданием и правилами. Инструктаж по ТБ и ОТ экспертов и участников
	08:15 – 08:30	Брифинг
	08:30 – 08:50	**Выполнение задания модуля 1 (поток 1)**
	08:50-08:55	Перерыв, проветривание помещения
	08:55-09:40	**Выполнение задания модуля 2 (поток 1)**
	09:40-09:45	Перерыв, проветривание помещения
	09:45-10:15	**Выполнение задания модуля 2 (поток 1)**
	10:15-10:20	Перерыв, проветривание помещения
	10:20-10:30	**Выполнение задания модуля 1 (поток 1)**
	10:30-11:50	**Выполнение задания модуля 1 (поток 1)**
	11:50-11:55	Перерыв, проветривание помещения
	11:55-12:25	**Выполнение задания модуля 2 (поток 1)**
	12:25 -13:00	**Обед**
	13:00 – 15:00	Работа экспертов, заполнение форм и оценочных ведомостей
	15:00-17:00	Подведение итогов работ потока 1, внесение главным экспертом баллов в CSO
День Д2 (поток 2)	08:00 – 08:15	Печать задания. Ознакомление с заданием и правилами. Инструктаж по ТБ и ОТ экспертов и участников
	08:15 – 08:30	Брифинг
	08:30 – 08:50	**Выполнение задания модуля 1 (поток 2)**
	08:50-08:55	Перерыв, проветривание помещения
	08:55-09:40	**Выполнение задания модуля 2 (поток 2)**
	09:40-09:45	Перерыв, проветривание помещения
	09:45-10:15	**Выполнение задания модуля 2 (поток 2)**
	10:15-10:20	Перерыв, проветривание помещения

	10:20-10:30	**Выполнение задания модуля 1 (поток 2)**
	10:30-11:50	**Выполнение задания модуля 1 (поток 2)**
	11:50-11:55	Перерыв, проветривание помещения
	11:55-12:25	**Выполнение задания модуля 2 (поток 2)**
	12:25 -13:00	**Обед**
	13:00 – 15:00	Работа экспертов, заполнение форм и оценочных ведомостей
	15:00-17:00	Подведение итогов работ потока 1, внесение главным экспертом баллов в CSO
	17:00-19:00	Заполнение итогового протокола, отчет

Приложение 3

Примерное задание для демонстрационного экзамена
по комплекту оценочной документации по специальности
10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»
квалификация техник по защите информации, профильный уровень

Модуль № 1:

Эксплуатация информационно – телекоммуникационных систем и сетей

Вид аттестации/уровень ДЭ:

ПА, ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах (Главный офис — виртуальные машины, Офис филиал — виртуальные машины).

При выполнении заданий необходимо при помощи текстового редактора,сформировать отчет, в котором представить скриншоты ключевых настроек. В ходе выполнения данного задания нужно установить основное ПО нарабочие станции будущей защищенной сети, задать пароли.

Задача 1.1 Произвести настройки сетевого окружения.

Для правильной работы сети надо создать или убедиться в наличии сетей:Host only или внутренняя сеть адаптер для сети центрального офиса,Host only или внутренняя сеть адаптер для сети филиала,

Host only или внутренняя сеть адаптер для сети межсетевого взаимодействия,

Host only адаптер, NAT или Bridge для виртуального «Интернета».

IP адреса защищенных сетей:

Центральный офис «Сеть 1 ЦО»:192.10.10.0/27 Офис филиал «Сеть 1 Филиал»:110.110.10.64/28Офис сеть 2 «Сеть 2 Офис»: 172.16.128.128/25

«Интернет» для всех координаторов:200.100.100.0/24

Адреса выбираются самостоятельно из указанного диапазона.

Необходимые приложения: отсутствуют.

Модуль № 2:

Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в томчисле криптографических средств защиты

Вид аттестации/уровень ДЭ:

ПА, ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 2.1. Развертывание ПК Administrator в качестве центра сертификации Установить и настроить рабочее место администратора (на базе виртуальноймашины Net1-Admin (ЦО)): Центр управления сетью (серверное и клиентскоеприложение ЦУС), Удостоверяющий и ключевой центр (УКЦ).

Задача 2.2. Установка ПО VPN Client на рабочее место администратора и дляорганизации сети филиала

На виртуальной машине Net1-Admin (ЦО) установить ПО Client (Пользовательская или серверная ОС), рабочее место администратора;

На виртуальной машине Net2-Client (филиал) установить ПО Client, рабочееместо пользователя.

Необходимые приложения: отсутствуют.

Модуль № 1:

Эксплуатация информационно – телекоммуникационных систем и сетейВид аттестации/уровень ДЭ:

ПА, ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 1.2. Инициализация VPN Coordinator

На виртуальной машине Net1-Coord (ЦО) инициализировать Coordinator HW-VA, на виртуальной машине Net2-Coord (Филиал) инициализировать Coordinator HW-VA.

Необходимые приложения: отсутствуют.

Модуль № 2:

Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в томчисле криптографических средств защиты

Вид аттестации/уровень ДЭ:

ПА, ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 2.3. Развертывание защищенной сети

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологиивиртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

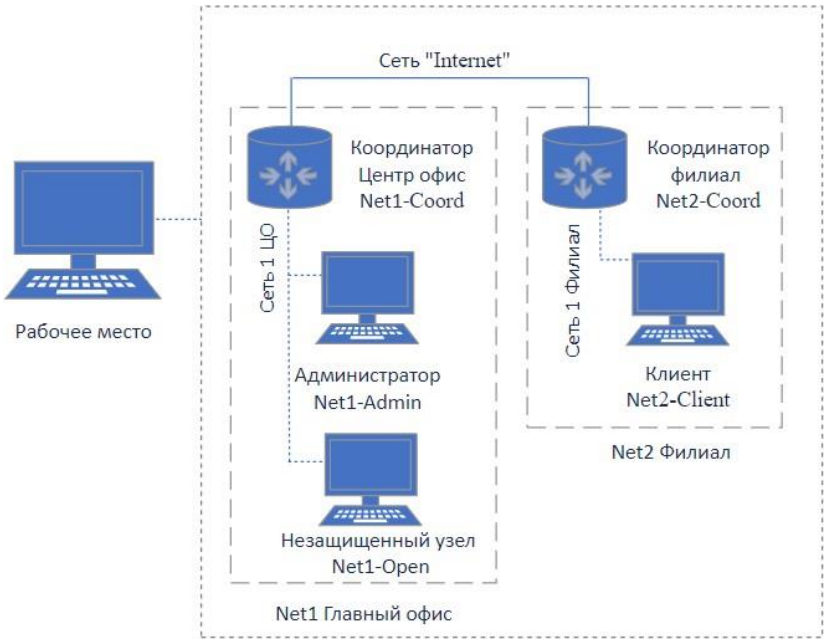

Рисунок 1 Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу 1).

Таблица 1 - Узлы защищенной сети

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла
Net1-Admin (ЦО)	Администратор сети	Administrator (БД, ЦУС сервер и клиент, УКЦ),Client	Пользовательская или серверная ОС	AdmN
Net1-Coord (ЦО)	Координатор офиса	Coordinator	HW-VA	CoordO
Net2-Coord (филиал)	Координатор филиала	Coordinator	HW-VA	CoordB
Net2-Client (филиал)	Пользователь филиала	Client	Пользовательская или серверная ОС	UserB

Задача 2.4. Создание структуры защищенной сети

Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой, представленной на рисунке 1. Создать пользователей узлов и их связи в соответствии со схемой, представленной в таблице 2.

Таблица 2 - Схема связей пользователей

Пользователь	CoordO	AdmN	CoordB	UserB
CoordO	×	*	*	
AdmN	*	×		*
CoordB	*		×	*
UserB		*	*	×

Провести инициализацию УКЦ, поменять тип паролей для пользователей («собственный»). Сформировать дистрибутивы ключей для всех сетевых узлов. Разнести дистрибутивы ключей по АРМ, провести первичную инициализацию узлов защищенной сети, проверить доступность узловзащищенной сети и сделать скриншоты работоспособности узлов.

Задача 2.5. Отправить письмо по Деловой почте пользователю UserB с узла Администратора сети, отправить текстовое сообщение пользователю AdmN от пользователя UserB.
В отчете необходимо зафиксировать: скриншоты текстового сообщения и деловой почты на отправителе и получателе, скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.

Необходимые приложения: отсутствуют.

Модуль № 2:

Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в томчисле криптографических средств защиты

Вид аттестации/уровень ДЭ:

ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 2.6. Реализовать межсетевое взаимодействие защищённых сетей (со связями «все со всеми»), развернув на виртуальной машине Net3-Admin рабочее место Администратора партнёрской сети. Схема межсетевого взаимодействия представлена на рисунке 2.
Создать структуру второй сети: рабочее место администратора на виртуальной машине Net3-Admin, координатор (Net3-Coord-HW-VA).
Установить и настроить необходимое ПО. Настроить межсетевое взаимодействие, с использованием ассиметричных межсетевых ключей, между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

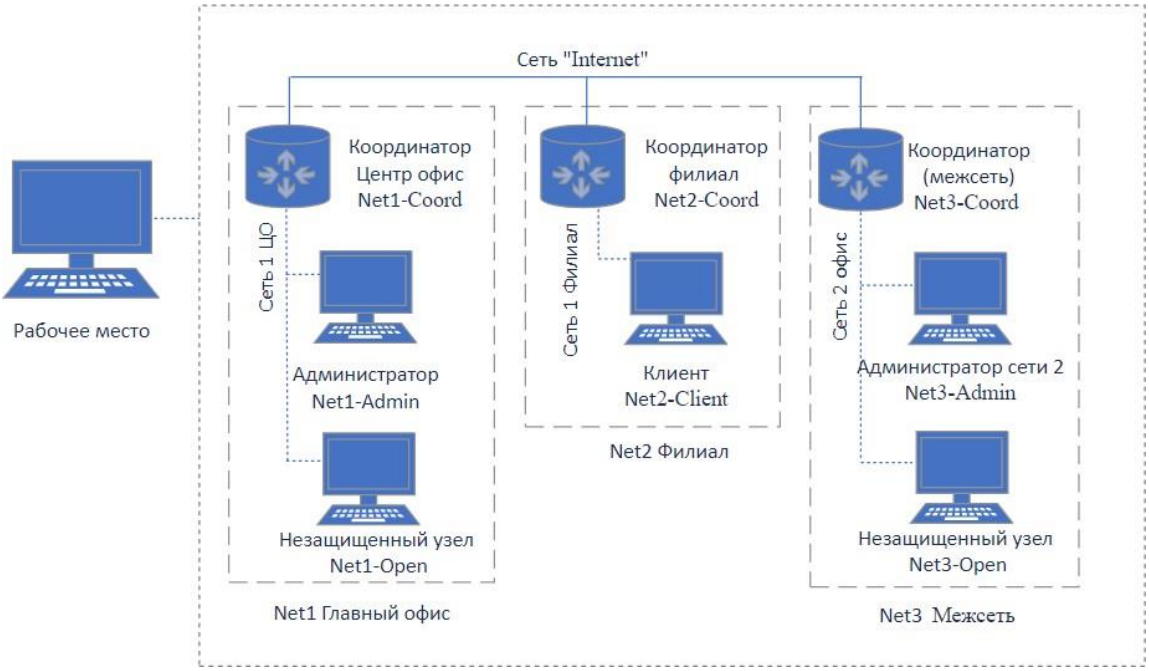

Рисунок 2 - Схема межсетевого взаимодействия

Проверить взаимодействие узлов, отправив сообщение деловой почты с узлаАдминистратор сети (Net1-Admin) на Admin (Net3-Admin).

Необходимые приложения: отсутствуют.

Модуль № 2:

Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в томчисле криптографических средств защиты

Вид аттестации/уровень ДЭ:

ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 2.7. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС: скомпрометировать ключи пользователя User на узле Пользователь филиала, произвести смену ключей пользователя и сетевых узлов, отправить обновления и произвести процедурусмены ключа пользователя на узле Пользователь филиала, проверить работу защищенной сети после обновления отправив сообщение от пользователя User

администратору. В отчете необходимо зафиксировать процесс настройки скриншотами.

Задача 2.8. Настройка правил в сети.

Произвести конфигурацию сетевых фильтров: настроив удаленное подключение по протоколу RDP от Net2-Client к Net1-Open, разрешив SSH- доступ к Net1-Coord от узла Net1-Open. При необходимости на виртуальные машины можно самостоятельно установить любой SSH-клиент.

Необходимые приложения: отсутствуют.

Модуль № 1:

Эксплуатация информационно – телекоммуникационных систем и сетейВид аттестации/уровень ДЭ:

ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 1.3. Туннелирование в рамках межсетевого взаимодействия Подключить незащищенную машину в сети 3 (Net3-Open).

Для второй открытой машины использовать Net1-Open узел в сети

1. Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по шифрованному каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping), а также любым другим протоколом, например smb (общая сетевая папка) или другим удобным (кроме ICMP); проанализировать журналы IP-пакетов на координаторах.

В отчет поместить скриншоты выполнения данной задачи и проверки работоспособности механизма туннелирования.

Необходимые приложения: отсутствуют.

Вариативная часть:

Задание модуля:

Составить руководство администратора для администрирования настроенной защищённой сети, используя техническую документацию программного обеспечения для защиты информации в телекоммуникационных системах.