ПРИЛОЖЕНИЕ 4
к ОПОП-П по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных 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

10.02.05 Обеспечение информационной безопасности автоматизированных систем

код *наименование специальности/профессии*

утвержденного Приказ Минобрнауки России от 09.12.2016 N 1553 (ред. от 03.07.2024) "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем" (Зарегистрировано в Минюсте России 26.12.2016 N 44938).

Квалификация выпускника: техник по защите информации.

Образовательная программа реализуется на базе основного общего образования.

Программа государственной итоговой аттестации (далее – программа ГИА) выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем разработана 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 10.02.05 Обеспечение информационной безопасности автоматизированных систем, и определяет совокупность требований к ее организации и проведению.

Цель государственной итоговой аттестации – установление соответствия результатов освоения обучающимися образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных 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 10.02.05 Обеспечение информационной безопасности автоматизированных 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 автоматизированных (информационных) систем в защищенном исполнении	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами
Защита информации техническими средствами	ПМ.03 Защита информации техническими средствами
16199 Оператор электронно-вычислительных и вычислительных машин	ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих
25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)"	ПМ.05 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)"
ВД по направленности по запросу работодателя	
ВД 6 Интеграция облачных технологий в цифровую экономику	ПМ 06. Интеграция облачных технологий в цифровую экономику

Таблица 2

Перечень результатов, демонстрируемых выпускником

Оцениваемые виды деятельности	Профессиональные компетенции
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
	ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.
	ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.
	ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
	ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
	ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
	ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.
	ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.
	ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.
Защита информации техническими средствами	ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
	ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
	ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.
	ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
	ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.
ВД.4 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"	ПК 4.1 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ВД по выбору	
ВД 05 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)»	ПК. 5.1 Организовывать и осуществлять предварительную и предполетную подготовку беспилотных воздушных судов смешанного типа ПК 5.2 Организовывать и осуществлять эксплуатацию беспилотных воздушных судов смешанного типа, в том числе в особых условиях и особых случаях в полете
ВД по запросу работодателя	
ВД 06 Интеграция облачных технологий в цифровую экономику	ПК 6.1 Сборка и настройка систем квантового распределения ключа

	ПК 6.2 Осуществлять подбор соответствующих оптических элементов ПК 6.3 Выполнять работы по анализу источников ошибок ПК 6.4 Выполнение работ по реализации связки классической и квантовой систем ПК 6.5 Применение программных средств обеспечения безопасности информации веб приложений ПК 6.6 Обработка запросов заказчика в службе технической подд*ержки в соответствии с трудовым заданием*

Выпускники, освоившие программу по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, сдают ГИА в форме демонстрационного экзамена профильного уровня 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

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Порядок разработки примерных основных образовательных программ среднего профессионального образования, проведения их экспертизы и ведения реестра примерных основных образовательных программ среднего профессионального образования (Приказ Минпросвещения России от 08.04.2021 № 153);

Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (Приказ Минобрнауки России от 09.12. 2016 г. № 1553);

Порядок организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования (Приказ Минпросвещения России от 24.08.2022 № 762);

Порядок проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования (Приказ Минпросвещения России от 08.11.2021 № 800);

Положение о практической подготовке обучающихся (Приказ Минобрнауки России № 885, Минпросвещения России № 390 от 05.08.2020);

Перечень профессий рабочих, должностей служащих, по которым осуществляется профессиональное обучение (Приказ Минпросвещения России от 14.07.2023 № 534);

Перечень профессий среднего профессионального образования, реализация образовательных программ по которым не допускается с применением исключительно электронного обучения, дистанционных образовательных технологий (приказ Министерства Просвещения Российской Федерации от 13 декабря 2023 г. № 932);

Приказ Министерства науки и высшего образования Российской Федерации и Министерства просвещения Российской Федерации от 05.08.2020 № 882/391 «Об организации и осуществлении образовательной деятельности при сетевой форме реализации образовательных программ»;

Приказ Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 536н «Об утверждении профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях»»;

Приказ Министерства труда и социальной защиты Российской Федерации от 14.09.2022. № 533н «Об утверждении профессионального стандарта «Специалист по безопасности компьютерных систем и сетей»;

Приказ Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н «Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах»;

Приказ Министерства труда и социальной защиты Российской Федерации от 09.08.2022 № 474н «Об утверждении профессионального стандарта «Об утверждении профессионального стандарта «Специалист по технической защите информации»»;

Приказ Министерства труда и социальной защиты Российской Федерации от 05.10.2015 № 686н «Об утверждении профессионального стандарта «Специалист по администрированию сетевых устройств информационно-коммуникационных систем»;

Приказ Министерства труда и социальной защиты Российской Федерации от 17.11.2020 № 791н «Об утверждении профессионального стандарта «Специалист по монтажу телекоммуникационного оборудования»;

Приказ Министерства труда и социальной защиты Российской Федерации от 29.09.2020 № 680н «Об утверждении профессионального стандарта «Системный администратор информационно-коммуникационных систем».

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:

- установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем
- администрирование автоматизированных систем в защищенном исполнении
- эксплуатация компонентов систем защиты информации автоматизированных систем
- диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении
- установка, настройка программных средств защиты информации в автоматизированной системе
- обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами;
- использование программных и программно-аппаратных средств для защиты информации в сети

− тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации

− решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;

− применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных

− учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности

− работа с подсистемами регистрации событий;

− выявление событий и инцидентов безопасности в автоматизированной системе

− установка, монтаж и настройка технических средств защиты информации;

− техническое обслуживание технических средств защиты информации;

− применение основных типов технических средств защиты информации

− применение основных типов технических средств защиты информации;

− выявление технических каналов утечки информации;

− участие в мониторинге эффективности технических средств защиты информации;

− диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации

− проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации

− проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

− выявление технических каналов утечки информации

− установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты

− оформление эксплуатационной документации на программно-аппаратные средства защиты информации в операционных системах

− установка программно-аппаратных средств защиты информации

− настройка программно-аппаратных средств защиты информации, в том числе средств антивирусной защиты, в операционных системах по заданным шаблонам

− изучение полетного задания, отработка порядка его выполнения и действий при управлении беспилотным воздушным судном с максимальной взлетной массой 30 килограммов и менее

− подбор и подготовка картографического материала

− ознакомление с ограничениями в районе выполнения полета по маршруту (трассе)

− ведение полетной и технической документации, в том числе в электронном виде с использованием сервисов цифрового журналирования операций

− монтаж оборудования систем

− первичная настройка и проверка функционирования систем

− монтаж программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД

− установка программных и программно-аппаратных (в том числе криптографических) средств и систем защиты систем от НД

− первичная настройка и проверка функционирования программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД

− текущий, в том числе автоматизированный, контроль функционирования систем с установленными показателями

− текущий, в том числе автоматизированный, контроль функционирования с установленными показателями программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях

− восстановление процесса функционирования после сбоев и отказов систем, программных, программно-аппаратных (в том числе криптографических), технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях

− составления базы знаний технической поддержки на основе обрабатываемых прецедентов

− работы с оборудованием КРК; анализа и оценки угроз в квантовых коммуникациях; разработки и реализации решений по квантовой защите данных.

1.5.2 Уметь

− осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем

− организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней

− осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем;

− производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы

− настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам

− обеспечивать работоспособность, обнаруживать и устранять неисправности

− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации

− устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации

− диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации

− применять программные и программно-аппаратные средства для защиты информации в базах данных;

− проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

− применять математический аппарат для выполнения криптографических преобразований;

− использовать типовые программные криптографические средства, в том числе электронную подпись

− применять средства гарантированного уничтожения информации

− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

− осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных

− применять технические средства для криптографической защиты информации конфиденциального характера;

− применять технические средства для уничтожения информации и носителей информации;

− применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных

− применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

− применять инженерно-технические средства физической защиты объектов информатизации

− оформлять эксплуатационную документацию программно-аппаратных средств защиты информации

− устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации

− читать аэронавигационные материалы

− анализировать метеорологическую, орнитологическую и аэронавигационную обстановку

− использовать специализированные цифровые платформы полетно-информационного обслуживания и сервисы цифрового журналирования операций

− оценивать техническое состояние и готовность к использованию беспилотных авиационных систем

− оформлять полетную и техническую документацию

− проводить монтаж (для программных средств - установку) систем, средств и систем защиты систем от НД

− проводить первичную настройку и проверку функционирования систем, средств и систем защиты систем от НД

− проводить проверку комплектности систем, средств и систем защиты систем от НД

− проводить текущий контроль показателей и процесса функционирования систем, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях электросвязи, предусмотренный регламентом их эксплуатации

− проводить предусмотренные регламентом работы по восстановлению процесса и параметров функционирования систем, а также программных, программно-аппаратных (в том числе криптографических) и технических средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях

− выяснять из беседы с заказчиком и понимать причины возникших аварийных ситуаций с информационным ресурсом;

− применять установленные правила делового общения при общении с заказчиком;

− отвечать на запросы заказчика в установленные регламентом сроки;

− анализировать и решать типовые запросы заказчиков;

− работать с программным обеспечением по приему, обработке и регистрации запросов заказчика;

− координировать решение запросов заказчиков со специалистами соответствующих подразделений;

− объяснять заказчикам пути решения возникшей проблемы.

− настраивать и эксплуатировать оборудование КРК;

– оценивать безопасность и стойкость систем квантовой криптографии; интегрировать КРК с существующими криптографическими системами.

1.5.3 Знать

– состав и принципы работы автоматизированных систем, операционных систем и сред;

– принципы разработки алгоритмов программ, основных приемов программирования;

– модели баз данных;

– принципы построения, физические основы работы периферийных устройств

– теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации

– порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях

– принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных

– методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации

– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;

– типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;

– основные понятия криптографии и типовых криптографических методов и средств защиты информации

– особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации

– типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа

– порядок технического обслуживания технических средств защиты информации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам

– физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

– порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

– методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

– номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам

– номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

– структуру и условия формирования технических каналов утечки информации

– номенклатура применяемых средств защиты информации от несанкционированной утечки по техническим каналам

– основные принципы действия и характеристики технических средств физической защиты;

– основные способы физической защиты объектов информатизации;

– номенклатуру применяемых средств физической защиты объектов информатизаци

– порядок оформления эксплуатационной документации

– типовые средства защиты информации в операционных системах

– правила и порядок, установленные воздушным законодательством Российской Федерации, получения разрешения на использование воздушного пространства, в том числе при выполнении полетов над населенными пунктами, при выполнении авиационных работ

– нормативные правовые акты об установлении запретных зон и зон ограничения полетов; порядок получения информации о запретных зонах и зонах ограничения полетов

– требования эксплуатационной документации

– летно-технические характеристики беспилотной авиационной системы и влияние на них эксплуатационных факторов

– правила ведения и оформления полетной и технической документации, требования к ведению и оформлению полетной и технической документации, в том числе в цифровом виде с использованием специализированных сервисов

– нормативные требования к составу и содержанию эксплуатационной документации систем, а также средств и систем защиты систем от НД

– нормативные правовые акты в области связи, информатизации и защиты информации

– номенклатура, функциональное назначение и основные характеристики систем

– номенклатура, функциональное назначение и основные характеристики средств и систем защиты систем от НД

– типы, основные характеристики средств измерений и контроля процесса и параметров функционирования систем, а также средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях электросвязи

– - Последовательность действий в целях изменения настроек систем, а также средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях электросвязи без прерывания процесса их функционирования

– последовательность действий в целях восстановления процесса и параметров функционирования систем, а также средств и систем защиты систем от НД, средств для поиска признаков компьютерных атак в сетях электросвязи

– организационные меры по защите информации

– нормативные правовые акты в области связи, информатизации и защиты информации, обеспечения безопасности критической информационной инфраструктуры

– принципы устройства и функционирования информационных ресурсов;

– основ управления изменениями;

– возможностей ИР;

– инструментов и методов коммуникаций;

– каналов коммуникаций;

– моделей коммуникаций;

– технологий межличностной и групповой коммуникации в деловом взаимодействии, основ конфликтологии.

– основные понятия и принципы квантовой механики, необходимые для понимания квантовой криптографии; принципы работы и архитектуру систем КРК;

– методы оценки безопасности и стойкости систем квантовой криптографии;

– перспективы развития квантовой криптографии и квантовых коммуникаций

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 российских духовно-нравственных 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:

1 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении:

ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

2. Защита информации в автоматизированных системах программными и программно-аппаратными средствами:

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

3. Защита информации техническими средствами:

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

4. Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин"

ПК 4.1 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах

ПК 4.2 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета

5. Выполнение работ по профессии 25331 «Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)»

ПК. 5.1 Организовывать и осуществлять предварительную и предполетную подготовку беспилотных воздушных судов смешанного типа

ПК 5.2 Организовывать и осуществлять эксплуатацию беспилотных воздушных судов смешанного типа, в том числе в особых условиях и особых случаях в полете

6. Интеграция облачных технологий в цифровую экономику

ПК 6.1 Сборка и настройка систем квантового распределения ключа

ПК 6.2 Осуществлять подбор соответствующих оптических элементов

ПК 6.3 Выполнять работы по анализу источников ошибок

ПК 6.4 Выполнение работ по реализации связки классической и квантовой систем

ПК 6.5 Применение программных средств обеспечения безопасности информации веб приложений

ПК 6.6 Обработка запросов заказчика в службе технической поддержки в соответствии с трудовым заданием

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 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» выбран комплект оценочной документации (КОД) шифр КОД 10.02.05-1-2026, 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 – 3 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

ЕДИНОЕ БАЗОВОЕ ЯДРО СОДЕРЖАНИЯ КОД[2]		
Вид деятельности/ Вид профессиональной деятельности	**Перечень оцениваемых ОК/ПК**	**Перечень оцениваемых умений, навыков (практического опыта)**
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК: администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	Умение: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней
		Умение: производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
	ОК: использовать информационные технологии в профессиональной деятельности.	Умение: применять средства информационных технологий для решения профессиональных задач; использовать Современное программное обеспечение
Защита информации в автоматизированных системах программными и программно- аппаратными средствами	ПК: осуществлять установку и настройку отдельных программных, программно- аппаратных средств защиты информации	Умение: устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации
	ПК: обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Умение: устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации

		Практический опыт: в использовании программных и программно-аппаратных средств для защиты информации в сети
	ПК: осуществлять тестирование функций отдельных программных и программно- аппаратных средств защиты информации	Практический опыт: в тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации

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

Таблица 2 – Содержательная структура КОД

Вид деятельности (вид профессиональной деятельности)	**Перечень оцениваемых ОК, ПК**	**Перечень оцениваемых умений, навыков (практического опыта)**
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК: администрировать программные и программно- аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	Умение: организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней
		Умение: производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
	ОК: использовать информационные технологии в профессиональной деятельности.	Умение: использовать информационные технологии в профессиональной деятельности.

Защита информации в автоматизированных системах программными и программно- аппаратными средствами	ПК: обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	Умение: устанавливать, настраивать, применять программные и программно- аппаратные средства защиты информации
		Практический опыт: в использовании программных и программно-аппаратных средств для защиты информации в сети
	ПК: осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	Умение: устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации
	ПК: осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Практический опыт: в тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК: администрировать программные и программно- аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	Умение: осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем
		Практический опыт: в администрировании автоматизированных систем в защищенном исполнении
	ПК: производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии требованиями эксплуатационной документации	Практический опыт: установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем

	ПК: осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность	Практический опыт: диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление
	автоматизированных (информационных) систем в защищенном исполнении	работоспособности автоматизированных (информационных) систем в защищенном исполнении
		Умения: обеспечивать работоспособность, обнаруживать и устранять неисправности
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК: осуществлять обработку, хранение и передачу информации ограниченного доступа	Умение: использовать типовые программные криптографические средства, в том числе электронную подпись
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПК: обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Умение: настраивать и устранять неисправности программно- аппаратных средств защиты информации в компьютерных сетях по заданным правилам
Защита информации в автоматизированных системах программными и программно- аппаратными средствами	ПК: осуществлять установку и настройку отдельных программных, программно- аппаратных средств защиты информации	Практический опыт: в установке, настройке программных средств защиты информаци в автоматизированной системе
	ПК: осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	Умение: диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно- аппаратных средств защиты информации
	ПК: осуществлять обработку, хранение и передачу информации ограниченного доступа	Практический опыт: в решении задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации
		Практический опыт: в при-

		менении электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных

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 автоматизированных (информационных) систем в защищенном исполнении», ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами», ПМ.03 «Защита информации техническими средствами», ПМ.04 Выполнение работ по профессии "Оператор электронно-вычислительных и вычислительных машин", ПМ 05 Выполнение работ по профессии 25331 "Оператор беспилотных авиационных систем (с максимальной взлетной массой 30 килограммов и менее)" ПМ 06 Интеграция облачных технологий в цифровую экономику 10.02.05 «Обеспечение информационной безопасности автоматизированных 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 10.02.05 «Обеспечение информационной безопасности автоматизированных 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, вид профессиональ-ной деятельно-сти)	**Критерий оценивания**[6]	**Баллы**
1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	**4,00**
		Использование информационных технологий впрофессиональной деятельности	**2,00**
2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации	**6,00**
		Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	**12,00**
		Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации	**2,00**
3	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Производство установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	**4,00**
		Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной)системы в защищенном исполнении	**6,00**

		Осуществление проверки технического состояния, технического обслуживания и текущего ремонта, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	**10,00**
4	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление обработки, хранения и передачи информации ограниченного доступа	**4,00**
5	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	**3,00**
		Обеспечение бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	**5,00**
6	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации	**6,00**
		Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации	**6,00**
		Осуществление обработки, хранения и передачи информации ограниченного доступа	**10,00**
		Итого	**80**

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 – 9,59	9,60 - 27,99	28 - 55,99	56 - 80

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.

Оригинал протокола проведения демонстрационного экзамена передается на хранение в образовательную организацию в составе архивных документов.

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 государственного 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
10.02.05 «Обеспечение информационной безопасности автоматизированных систем»
квалификация техник по защите информации, профильный уровень

Модуль № 1:

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

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 на рабочие станции будущей защищенной сети, задать пароли пользователей и администраторов сети.

Для правильной работы сети надо создать или убедиться в наличии 4 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»: 172.16.224.224/27 Офис

филиал «Сеть 1 Филиал»: 10.10.20.128/25 Офис сеть 2

«Сеть 2 Офис»: 192.168.88.64/26 «Интернет» для всех координаторов: 10.8.248.0/24

Адреса выбираются самостоятельно из указанного диапазона.

В связи с особенностями работы системы на различных версиях пользовательских или серверных ОС, может потребоваться установка компонентов системы вручную.

Задача 1.1 Установить SQL-сервер, входящий в комплект дистрибутивов программного комплекса, на виртуальную машину Net1-Open (незащищенный узел).
Необходимые приложения: отсутствуют.

Модуль № 2:

Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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 виртуальной машины Net1-AdminCA(ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленный SQL-сервер. Установить клиент ЦУС на ВМ Net1-Open (незащищенный узел).

Задача 2.2. Инициализация VPN Coordinator и установка ПО VPN Client на виртуальной машине Net1-AdminCA (ЦО) установить ПО Client (Пользовательская или серверная ОС), рабочее место администратора, на виртуальной машине Net1-Coord (ЦО) инициализировать Coordinator HW-VA.

Задача 2.3. Инициализация VPN Coordinator и установка ПО VPN Client для организации сети филиала

На виртуальной машине Net2-Coord (филиал) инициализировать Coordinator HW-VA, на виртуальной машине Net2-Client (филиал) установить ПО Client, рабочее место пользователя. В отчете необходимо зафиксировать процесс установки скриншотами форм.

Модуль № 2:

Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Вид аттестации/уровень ДЭ:

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

Задача 2.4 Развертывание удостоверяющего центра в составе защищенной сети

Необходимо использовать рабочее место администратора (созданное ранее) для создания

структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

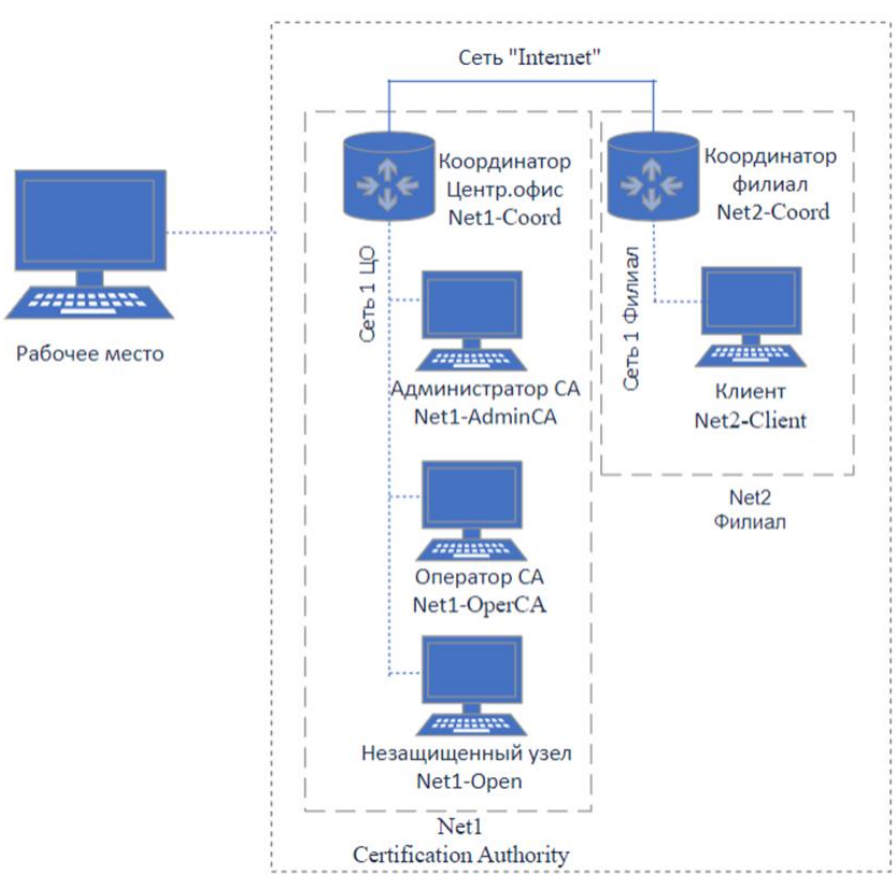

Рисунок 1 Схема защищенной сети

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

Задача 2.5 Создание структуры защищенной сети

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

Таблица 1 - Узлы защищенной сети

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла,уровень полномочий

Net1-AdminCA (ЦО)	Администратор ИБ	Administrator (ЦУС сервер, УКЦ), Client, CA Informing	Пользовательская или серверная ОС	AdminS
Net1-CoordCA (ЦО)	Корневой координатор	Coordinator	HW-VA	Root_ Coordinator
Net1-OperCA (ЦО)	Узел ЦР	Client, Publication Service, Registration Point	Пользовательская или серверная ОС	Node_CR
Net2-Coord (Филиал)	Подчиненный координатор	Coordinator	HW-VA	Sub_Coordinator
Net2-Client (филиал)	Удаленный клиент	Client	Пользовательская или серверная ОС	Rem_Client

Таблица 2 - Схема связей пользователей

Пользователь	Root_ Coordinator	AdminS	Node_CR	Sub_Coordinator	Rem_Client
Root_Coordinator	×	*	*	*	
AdminS	*	×	*		*
Node_CR	*	*	×	*	
Sub_Coordinator	*		*	×	*
Rem_Client		*		*	×

Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке, 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 узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задача 2.6 Отправить письмо по Деловой почте пользователю Rem_Client с узла AdminS, отправить текстовое сообщение пользователю AdminS от пользователя Rem_Client. В отчете необходимо представить скриншоты текстового сообщения и деловой почты на отправителе и получателе (при отправке письма), а также скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.

Необходимые приложения: отсутствуют.

Модуль № 1:

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Вид аттестации/уровень ДЭ:

ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 1.2 Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

На виртуальной машине Net1-OperCA (ЦО) установить ПО Client, Сервис публикации. На виртуальной машине Net1-OperCA (ЦО) установить ПО Центр регистрации. На виртуальной машине Net1-AdminCA (ЦО) установить ПО Сервис информирования.

Модуль № 1:

Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Вид аттестации/уровень ДЭ:

ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Задача 1.3 Настройка работы удостоверяющего центра в аккредитованном режиме

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов.

После перевода УКЦ в аккредитованный режим необходимо выпустить:

- корневой квалифицированный сертификат, назначить текущим,
- квалифицированную электронную подпись для пользователя AdminS, выдать с новым дистрибутивом ключей,
- квалифицированную электронную подпись для пользователя Rem_Client, сохранить электронные ключи в файл.

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации. Настроить переход в автоматический режим: передачу на публикацию и обновление CRL с периодичностью 1 день. Реализовать автоматическую публикацию сертификатов издателей на FTP-сервере.

Посредством Центра Регистрации: зарегистрировать пользователя Rem_Client, отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос. Отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

Посредством Сервиса Информирования настроить способ выдачи уведомлений, сформировать отчет о выданных за текущие сутки сертификатах.

Задача 1.4. Компрометация пользователя

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС: скомпрометировать ключи пользователя Rem_Client на узле Удаленный клиент, произвести смену ключей пользователя и сетевых узлов, отправить обновления и произвести процедуру смены ключа пользователя на узле Удаленный клиент, проверить работу защищенной сети после обновления отправив сообщение от пользователя Rem_Client администратору.

В отчете необходимо зафиксировать процесс настройки скриншотами.

Задача 1.5 Настроить агрегированный канал связи (интерфейс) на Net2-Coord в сторону внешней сети Inet (задействовать eth0 и eth1). Применить режим, который используется для балансировки нагрузки на подчиненных физических интерфейсах и защищает от сбоев (преимущественно применим в сетях с простой топологией).

Необходимые приложения: отсутствуют.

Модуль № 2:

Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Вид аттестации/уровень ДЭ:

ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

Задача 2.7. 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.

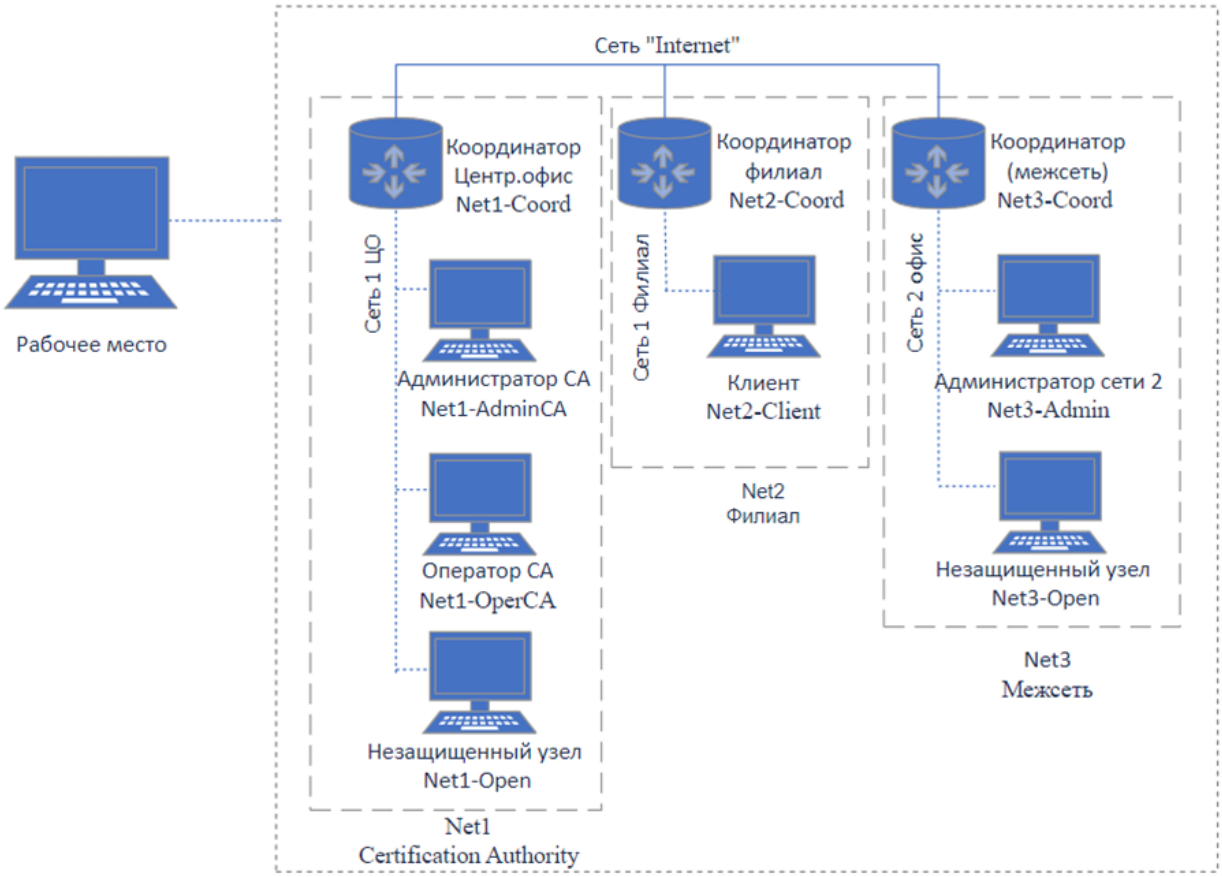

Рисунок 2 Схема межсетевого взаимодействия

Создать структуру второй сети: рабочее место администратора на виртуальной машине Net3-Admin (БД, ЦУС, УКЦ, Client), 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. Проверить взаимодействие узлов, отправив сообщение чата и деловой почты с узла Администратор сети (Net1-AdminCA) на Admin (Net3-Admin).

Необходимые приложения: отсутствуют.