

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Костылева Татьяна Александровна
Должность: Проректор по образовательной деятельности
Дата подписания: 26.02.2026 10:01:42
Уникальный программный ключ:
9eb8208ad98201234f464200700cb8ba94333b66

10.02.05 Обеспечение информационной безопасности автоматизированных систем

**ПРИЛОЖЕНИЕ 4
к ОПОП-П по специальности**

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

СОДЕРЖАНИЕ

Общие положения	3
Примерные требования к проведению демонстрационного экзамена	5
Организация и проведение защиты дипломного проекта (работы)	6

Общие положения

Программа государственной итоговой аттестации (далее – программа ГИА) выпускников по специальности *10.02.05 Обеспечение информационной безопасности автоматизированных 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 *10.02.05 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	
ВД 01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	ПМ 01. Эксплуатация автоматизированных (информационных) систем в защищенном исполнении
ВД 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПМ 02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами
ВД 03. Защита информации	ПМ 03. Защита информации

техническими средствами	техническими средствами
ВД 04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин	ПМ 04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин
По запросу работодателя (при наличии)	
ВД 05. Планирование стратегии цифрового развития телекоммуникационных систем	ПМ 05. Планирование стратегии цифрового развития телекоммуникационных систем

Таблица 2

Перечень результатов, демонстрируемых выпускником

Оцениваемые виды деятельности	Профессиональные компетенции
ВД 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
ВД 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.
ВД 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
ВД 04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профессии 16199 Оператор электронно-вычислительных и вычислительных машин	ПК 4.1 Осуществлять подготовку оборудования компьютерной системы к работе, производить установку, настройку и обслуживание программного обеспечения
	ПК 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
	ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
	ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе
ВД 05. Планирование стратегии цифрового развития телекоммуникационных систем	ПК 5.1 Обслуживать абонентское и терминальное телекоммуникационное оборудование с использованием программных и программно-аппаратных средств
	ПК 5.2 Обслуживать линейное телекоммуникационное оборудование с использованием программных и программно-аппаратных средств
	ПК 5.3 Обслуживать станционное телекоммуникационное оборудование с использованием программных и программно-аппаратных средств

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)

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.

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.

1. Основные положения

Образовательная программа: Программа подготовки специалистов среднего звена (ППССЗ) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Нормативно-правовые акты, в соответствии с которыми разработана программа ГИА.

Программа государственной итоговой аттестации (ГИА) разработана в строгом соответствии со следующей нормативно-правовой базой Российской Федерации:

1. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (статьи 59, 60).

2. Приказ Министерства просвещения Российской Федерации от 12.08.2020 № 397 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования».

3. Приказ Министерства образования и науки Российской Федерации от 13.08.2013 № 968 (в действующей редакции) «Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования».

4. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденный приказом Министерства образования и науки РФ от 28 июля 2014 г. № 837 (с изменениями).

5. Локальные нормативные акты образовательной организации (ОО):

- Устав образовательной организации.
- Положение о государственной итоговой аттестации выпускников.
- Положение о выпускной квалификационной работе (ВКР) / Положение о демонстрационном экзамене (в зависимости от формы ГИА).

- Основная профессиональная образовательная программа по специальности 10.02.05.

Программа ГИА и все сопутствующие материалы (темы ВКР, оценочные средства, комплекты заданий для демонстрационного экзамена) разрабатываются цикловой (предметной) комиссией по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» или профильным методическим объединением преподавателей, обеспечивающих реализацию ППССЗ.

Проект программы ГИА с приложениями рассматривается и принимается на заседании цикловой комиссии.

Программа ГИА согласовывается с:

- Заместителем руководителя (директора) по учебно-методической (или учебной) работе.
- Представителями работодателей (в лице руководителей базовых организаций, членов государственной экзаменационной комиссии (ГЭК) от производства).

Утверждается приказом руководителя (директора) образовательной организации на текущий учебный год не позднее, чем за 6 месяцев до начала проведения ГИА. Утвержденная программа становится локальным нормативным актом ОО, обязательным для исполнения.

2. Паспорт программы государственной итоговой аттестации

Программа государственной итоговой аттестации (далее - Программа ГИА, ГИА) разработана в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в части освоения видов деятельности по специальности и соответствующих профессиональных компетенций (далее – ПК):

Вид деятельности	Требования к знаниям, умениям, практическим действиям
Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	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

	<p>периферийных устройств, основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации; теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации;</p> <p>порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях.</p> <p>уметь:</p> <p>обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем;</p> <p>производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы;</p> <p>организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней;</p> <p>настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам.</p> <p>иметь практический опыт в:</p> <p>эксплуатации компонентов систем защиты информации автоматизированных систем, их диагностике, устранении отказов и восстановлении работоспособности;</p> <p>администрировании автоматизированных систем в защищенном исполнении;</p> <p>установке компонентов систем защиты информации автоматизированных информационных систем.</p>
<p>Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p>	<p>знать:</p> <p>особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;</p> <p> типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;</p> <p> типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа;</p> <p> основные понятия криптографии и типовых криптографических методов и средств защиты информации.</p> <p>уметь:</p> <p>устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;</p> <p>диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;</p>

	<p>проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; использовать типовые программные криптографические средства, в том числе электронную подпись; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; 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.</p> <p>иметь практический опыт в:</p> <p>установке и настройке программных средств защиты информации;</p> <p>тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;</p> <p>учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.</p>
<p>Защита информации техническими средствами</p>	<p>знать:</p> <p>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;</p> <p>номенклатуру и характеристики аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок (далее - ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;</p> <p>основные принципы действия и характеристики, порядок технического обслуживания, устранение неисправностей и организацию ремонта технических средств защиты информации; основные способы физической защиты объектов информатизации;</p> <p>методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;</p> <p>номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам и физической защиты объектов информатизации.</p> <p>уметь:</p> <p>применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</p> <p>применять технические средства для криптографической защиты информации конфиденциального характера;</p> <p>применять технические средства для уничтожения информации и носителей информации, защиты информации в условиях применения мобильных устройств обработки и передачи данных;</p>

	<p>применять инженерно-технические средства физической защиты объектов информатизации.</p> <p>иметь практический опыт в:</p> <p>выявлении технических каналов утечки информации; применении, техническом обслуживании, диагностике, устранении отказов, восстановлении работоспособности, установке, монтаже и настройке инженерно-технических средств физической защиты и технических средств защиты информации; проведении измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;</p> <p>проведении измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.</p>
--	---

2.1. Цели и задачи программы государственной итоговой аттестации

Целью программы ГИА является определение степени готовности обучающегося к самостоятельной профессиональной деятельности, уровня сформированности профессиональных компетенций в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС, ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Задача ГИА: определение практического и теоретического уровня подготовленности обучающегося к выполнению профессиональных задач, установленных ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

3. Структура, содержание и условия допуска к государственной итоговой аттестации

3.1 В соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем ГИА проводится в форме демонстрационного экзамена и защиты дипломного проекта.

3.2 Объем времени проведения ГИА составляет 6 недель, в том числе по срокам (таблица 4):

Таблица 4 - Объем времени проведения ГИА

Этапы и виды работ	Объем времени
Демонстрационный экзамен	1 неделя
Подготовка дипломного проекта	4 недели
Защита дипломного проекта	1 неделя

3.3 К ГИА допускаются обучающиеся, не имеющие академических задолженностей и в полном объеме выполнившие учебный план по осваиваемой ОП СПО. Допуск к ГИА оформляется приказом руководителя образовательной организации.

3.4 ГИА проводится государственной экзаменационной комиссией (далее – ГЭК).

Состав ГЭК утвержден Приказом образовательной организации.

В составе ГЭК создается экспертная группа из числа лиц, приглашенных сторонней

организацией и обладающих профессиональными знаниями, навыками и опытом в сфере, соответствующей специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (далее - экспертная группа, эксперты).

Экспертную группу возглавляет главный эксперт, назначаемый из числа экспертов, включенных в состав ГЭК.

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.

Программа государственной итоговой аттестации, форма, критерии оценивания, продолжительность ГИА утверждаются образовательной организацией и доводятся до сведения обучающихся не позднее, чем за шесть месяцев до начала ГИА.

4. Организация и порядок проведения государственной итоговой аттестации

4.1 Организация разработки тематики дипломных проектов

Темы дипломных проектов разрабатываются преподавателями образовательной организации совместно со специалистами предприятий или организаций, заинтересованных в разработке данных тем, рассматриваются на заседании предметной цикловой комиссии.

Выпускнику предоставляется право выбора темы дипломного проекта, в том числе предложения своей темы с необходимым обоснованием целесообразности ее разработки для практического применения.

Тема дипломного проекта должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу среднего профессионального образования (Приложение 1).

Темы дипломных проектов должны отвечать современным требованиям развития науки, техники, производства, экономики и иметь практико-ориентированный характер.

При определении темы следует учитывать, что ее содержание может основываться: на обобщении результатов выполненной ранее курсовой работы (проекта), если она выполнялась студентом в рамках соответствующего профессионального модуля, с использованием результатов выполненных ранее практических заданий, а также конкретных производственных данных предприятия – базы производственной практики.

4.2 Выполнение дипломного проекта

Для подготовки дипломного проекта выпускнику приказом руководителя образовательной организации назначается руководитель и при необходимости консультанты, оказывающие выпускнику методическую поддержку.

4.3 Объем учебной нагрузки по данному виду работы и количество обучающихся, закрепленное за одним преподавателем, определяются локальными нормативными актами образовательной организации в соответствии со штатным расписанием и требованиями к кадровому обеспечению сопровождения ГИА.

4.4 В обязанности руководителя дипломного проекта входит:

- разработка задания на подготовку дипломного проекта;
- оказание помощи обучающемуся в разработке индивидуального графика работы на весь период выполнения дипломного проекта;
- консультирование обучающегося по вопросам содержания и последовательности выполнения дипломного проекта;
- рекомендации по сбору необходимого для выполнения дипломного проекта материала, оказание помощи в подборе необходимых информационных источников;
- консультирование обучающегося по возникающим в ходе выполнения дипломного проекта проблемам теоретического и практического характера;
- консультирование по оформлению всех частей дипломного проекта в соответствии с требованиями образовательной организации к оформлению документов;
- контроль хода выполнения дипломного проекта в соответствии с установленным

графиком в форме обсуждения хода работ;

- оказание помощи (консультирование обучающегося) в подготовке презентации и доклада для защиты дипломного проекта;
- предоставление письменного отзыва на дипломный проект.

4.5 Выполненный дипломный проект должен:

- соответствовать разработанному заданию;
- демонстрировать требуемый уровень подготовки выпускника, его способность и умение применять на практике освоенные знания, практические умения, общие и профессиональные компетенции в соответствии с ФГОС СПО.

Задание для каждого обучающегося разрабатывается в соответствии с утвержденной темой. Задание на дипломный проект рассматривается на заседании предметной цикловой комиссии, подписывается руководителем дипломного проекта и утверждается заместителем директора по учебно-производственной работе.

В отдельных случаях допускается выполнение дипломного проекта группой обучающихся. При этом индивидуальные задания выдаются каждому обучающемуся.

Задание на дипломный проект выдается обучающемуся не позднее, чем за две недели до начала производственной (преддипломной) практики, что обусловлено необходимостью сбора практического материала в период ее прохождения.

4.6 По завершению подготовки дипломного проекта руководитель проверяет качество проекта, подписывает его и вместе с заданием и своим письменным отзывом передает заведующему отделением.

4.7 В отзыве руководителя дипломного проекта указываются характерные особенности проекта, его достоинства и недостатки, отношение обучающегося к выполнению проекта, проявленные (не проявленные) им способности. Оцениваются уровень освоения общих и профессиональных компетенций, знания, умения обучающегося, продемонстрированные им при выполнении проекта, а также степень самостоятельности обучающегося и его личный вклад в раскрытие проблем и разработку предложений по их решению. Заканчивается отзыв выводом о возможности (невозможности) допуска дипломного проекта к защите.

4.8 Структура дипломного проекта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем включает:

- Введение;
- Основную часть:

Глава №1 Теоретическое обоснование темы (аналитическое исследование); Глава №2. Исследовательская практическая часть (практическое исследование);

- Заключение;
- Список используемых информационных источников.

Во введении раскрывается цель, обоснование состава, задачи, решаемые в ходе выполнения дипломного проекта.

В основной части дипломного проекта каждая глава должна состоять не менее чем из трех разделов, а каждый раздел может включать в себя несколько пунктов, заключение и список используемых источников.

В заключении содержатся общие выводы по проекту.

Графическая часть дипломного проекта иллюстрирует технологическую часть проекта и включает в себя: планы проектируемых объектов, схемы, таблицы, графики, технологические карты.

Список используемых источников отражает перечень источников, которые использовались при написании ВКР (не менее 30), составленный в следующем порядке:

- федеральные законы;
- указы Президента Российской Федерации (в той же очередности);
- постановления Правительства Российской Федерации (в той же очередности);
- иные нормативные правовые акты;

- иные официальные материалы (резолюции-рекомендации международных организаций и конференций, официальные доклады, официальные отчеты и др.);
- монографии, учебники, учебные пособия (в алфавитном порядке);
- иностранная литература;
- интернет ресурсы.

Рекомендуемый объем текстовой части дипломного проекта 40 – 60 страниц печатного текста (без приложений).

Текст дипломного проекта должен быть подготовлен с использованием компьютера в текстовом редакторе MS Word, шрифт Times New Roman, размер 14, распечатан на одной стороне белой бумаги формата А4 (210 × 297 мм).

4.9 Правила оформления дипломного проекта регламентируются методическими рекомендациями по оформлению курсовых и дипломных проектов, выпускных квалификационных работ.

4.9.1 Выполненный дипломный проект предоставляется для защиты не менее чем за 7 дней:

4.9.1.1 для проведения нормативного контроля;

4.9.1.2 формирования отзыва руководителя;

4.9.1.3 внешней рецензии.

При проведении нормоконтроля консультант или руководитель дипломного проекта руководствуются:

- указателями (каталогами, перечнями) государственных, международных и отраслевых стандартов, технических условий и др.;
- действующими нормативными документами, распространяющимися на объект стандартизации;
- терминологическими словарями (справочниками, сборниками); картотеками внедрения нормативных документов;
- таблицами систематизации и др. Консультант по нормоконтролю имеет право:
- возвращать дипломный проект при несоответствии требованиям, небрежного выполнения, отсутствия необходимых подписей, отсутствия документов, на которые имеются ссылки в работе и т.д.;
- требовать разъяснений и дополнительных материалов по возникшим при проверке вопросам;
- не подписывать дипломный проект при невыполнении требований.

4.9.2 Дипломный проект подлежит обязательному рецензированию.

Рецензирование дипломного проекта проводится в целях обеспечения объективной оценки труда выпускника. Выполненные квалификационные работы рецензируются специалистами по тематике дипломного проекта из числа инженерно-технических работников профильных предприятий.

Рецензенты дипломного проекта определяются не позднее, чем за месяц до защиты. Рецензия должна включать:

- заключение о соответствии дипломного проекта заявленной теме, заданию;
- оценку качества выполнения каждого раздела дипломного проекта
- оценку степени разработки поставленных вопросов и практической значимости работы;
- общую оценку качества выполнения дипломного проекта.

Содержание рецензии доводится до сведения обучающегося не позднее, чем за день до защиты работы.

Внесение изменений в дипломный проект после получения рецензии не допускается. Образовательная организация после ознакомления с отзывом руководителя и рецензией решает вопрос о допуске обучающегося к защите и передает дипломного проекта в ГЭК. Процедура передачи определяется локальным нормативным актом образовательной организации.

4.9.3 Публичная защита

Для допуска к публичной защите необходимо иметь следующие материалы и

документы:

- выполненный дипломный проект, заверенный подписями, обозначенными на титульном листе;

- письменный отзыв руководителя;
- рецензию (подпись рецензента должна быть заверена печатью);
- зачетную книжку, заполненную в точном соответствии с учебным планом.

В ходе подготовки к защите дипломного проекта обучающийся совместно с руководителем дипломного проекта составляют текст доклада, который должен содержать:

- полное наименование темы дипломного проекта;
- цели и задачи проектирования;
- характеристику объекта проектирования;
- сущность и эффективность проектных решений;
- выводы о практической целесообразности и экономической эффективности проекта в целом.

Публичная защита дипломных проектов проводится на открытом заседании Государственной экзаменационной комиссии (далее – ГЭК) с участием не менее двух третей ее состава.

В ГЭК должны быть представлены следующие документы:

- Приказ руководителя образовательной организации о проведении государственной итоговой аттестации по образовательной программе;
- Приказ руководителя образовательной организации об утверждении тем дипломных проектов;

- Приказ руководителя образовательной организации об утверждении состава ГЭК;
- Приказ руководителя образовательной организации о допуске обучающихся к защите дипломного проекта

- Программа ГИА;
- Выполненные дипломные проекты с отзывом руководителя, рецензией;
- Зачетные книжки;
- Сводная ведомость итоговых оценок;
- Книга протоколов заседаний ГЭК.

В ГЭК могут быть предоставлены документы, подтверждающие учебные достижения обучающегося (грамоты и дипломы участника олимпиад, конкурсов, научно-практических конференций и т.д.).

На защиту дипломного проекта отводится до 30 минут на одного обучающегося.

Рекомендуемый регламент защиты дипломного проекта:

- презентация дипломного проекта в форме публичного доклада обучающегося не более 10 - 15 минут. Во время защиты дипломного проекта рекомендуется пользоваться планом доклада или тезисами. В ходе доклада необходимо использовать чертежи и другие графические материалы, представленные на стендах, слайдах.

- вопросы ГЭК (по теме дипломного проекта) и ответы обучающихся – до 5 минут.
- представление секретарем ГЭК или руководителем и рецензентом дипломного проекта соответственно отзыва и рецензии на дипломный проект – до 2 минут.

Для защиты дипломного проекта отводится специально подготовленный кабинет. Оснащение кабинета:

- Рабочее место для членов ГЭК;
- Места для выпускников, родителей выпускников, социальных партнеров;
- Стенды;
- Компьютер, мультимедиа проектор, экран;
- Лицензионное программное обеспечение общего назначения.

4.10 Для оценки выполнения и защиты дипломного проекта формируется фонд оценочных средств (далее ФОС). ФОС включает в себя:

Требования к результатам освоения профессиональной образовательной программы. Темы

дипломных проектов.

Задания на дипломный проект.

Критерии оценки дипломного проекта руководителем дипломного проекта. Форма отзыва на дипломный проект руководителя.

Критерии оценки дипломного проекта рецензентом. Форма рецензии на дипломный проект.

Критерии оценивания защиты дипломного проекта.

4.11 Демонстрационный экзамен по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем проводится на профильном уровне.

4.12 Демонстрационный экзамен проводится с использованием единых оценочных материалов - комплектом оценочной документации КОД 10.02.05-1-2025. (Приложение 3). Полная версия КОД 10.02.05-1-2025 для проведения демонстрационного экзамена размещен в информационно-телекоммуникационной сети «Интернет» на сайте <https://bom.firpo.ru/Public>.

КОД 10.02.05-1-2025 включает комплекс требований для проведения демонстрационного экзамена, перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания, план застройки площадки демонстрационного экзамена, требования к составу экспертных групп, инструкцию по технике безопасности, а также образцы заданий.

Задание демонстрационного задания включает комплексную практическую задачу, моделирующую профессиональную деятельность и выполняемую в режиме реального времени.

Выпускники, участники демонстрационного экзамена и эксперты должны быть зарегистрированы в электронной системе интернет мониторинга ЦП с учетом требований Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных».

4.13 Демонстрационный экзамен по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем проводится в центре проведения демонстрационного экзамена.

4.14 Площадка для проведения демонстрационного экзамена оборудована и оснащена в соответствии с требованиями комплекта оценочной документации (КОД 10.02.05-1-2025).

4.15 Дата, время начала проведения демонстрационного экзамена, расписание сдачи экзаменов в составе экзаменационных групп, планируемая продолжительность проведения демонстрационного экзамена, технические перерывы в проведении демонстрационного экзамена определяются планом проведения демонстрационного экзамена, утверждаемым ГЭК совместно с образовательной организацией не позднее, чем за двадцать календарных дней до даты проведения демонстрационного экзамена.

4.16 Образовательная организация знакомит с планом проведения демонстрационного экзамена выпускников, сдающих демонстрационный экзамен и лиц, обеспечивающих проведение демонстрационного экзамена в срок не позднее, чем за пять рабочих дней до даты проведения экзамена (Приложение 2).

4.17 В день проведения демонстрационного экзамена в центре проведения экзамена присутствуют:

- руководитель (уполномоченный представитель) организации, на базе которой организован центр проведения экзамена;
- не менее одного члена ГЭК, не считая членов экспертной группы;
- члены экспертной группы;
- главный эксперт;
- представители организаций-партнеров (по согласованию с образовательной организацией);
- выпускники;
- технический эксперт;
- представитель образовательной организации, ответственный за сопровождение выпускников к центру проведения экзамена (при необходимости);
- тьютор (ассистент), оказывающий необходимую помощь выпускнику из числа лиц с ограниченными возможностями здоровья, детей-инвалидов, инвалидов (далее - тьютор (ассистент));
- организаторы, назначенные образовательной организацией из числа педагогических

работников, оказывающие содействие главному эксперту в обеспечении соблюдения всех требований к проведению демонстрационного экзамена.

4.18 В случае отсутствия в день проведения демонстрационного экзамена в центре проведения экзамена лиц, указанных выше, решение о проведении демонстрационного экзамена принимается главным экспертом, о чем главным экспертом вносится соответствующая запись в протокол проведения демонстрационного экзамена.

Допуск выпускников в центр проведения экзамена осуществляется главным экспертом на основании документов, удостоверяющих личность.

4.19 Главным экспертом осуществляется осмотр центра проведения экзамена, распределение обязанностей между членами экспертной группы, а также распределение рабочих мест между выпускниками с использованием способа случайной выборки.

4.20 Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между выпускниками фиксируются главным экспертом в соответствующих протоколах.

4.21 Под руководством главного эксперта выпускники знакомятся со своими рабочими местами, повторно знакомятся с планом проведения демонстрационного экзамена, условиями оказания первичной медицинской помощи в центре проведения экзамена. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

4.22 Технический эксперт под подпись знакомит членов экспертной группы, выпускников с требованиями охраны труда и безопасности производства.

4.23 Члены ГЭК, не входящие в состав экспертной группы, наблюдают за ходом проведения демонстрационного экзамена и вправе сообщать главному эксперту о выявленных фактах нарушения Порядка.

Члены экспертной группы осуществляют оценку выполнения заданий демонстрационного экзамена самостоятельно.

4.24 Выпускники проходят демонстрационный экзамен в составе экзаменационных групп.

Допуск выпускников к выполнению заданий осуществляется при условии обязательного их ознакомления с требованиями охраны труда и производственной безопасности.

4.25 Задания для проведения демонстрационного экзамена доводятся до главного эксперта в день, предшествующий дню начала демонстрационного экзамена.

В день проведения демонстрационного экзамена, в соответствии с планом, главный эксперт знакомит выпускников с заданиями и передает им их копии.

После того как все участники и привлечённые лица займут свои рабочие места согласно протоколу распределения и в соответствии с требованиями охраны труда, производственной безопасности главный эксперт объявляет начало демонстрационного экзамена.

После объявления о начале демонстрационного экзамена выпускники приступают к выполнению заданий демонстрационного экзамена.

4.26 Время начала экзамена фиксируется в протоколе проведения демонстрационного экзамена.

4.27 Демонстрационный экзамен проводится при неукоснительном соблюдении выпускниками, лицами, привлечёнными к проведению демонстрационного экзамена, требований охраны труда и производственной безопасности, а также с соблюдением принципов объективности, открытости и равенства выпускников.

После объявления главным экспертом окончания времени выполнения заданий выпускники прекращают любые действия по выполнению заданий демонстрационного экзамена.

Результаты выполнения выпускниками заданий демонстрационного экзамена подлежат фиксации экспертами экспертной группы в соответствии с требованиями комплекта оценочной документации и задания демонстрационного экзамена.

5. Критерии оценки уровня и качества подготовки обучающихся

5.1 Оценка результатов ГИА определяется в ходе заседания ГЭК оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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

Заседания ГЭК протоколируются.

Результаты ГИА объявляются в тот же день после оформления в установленном порядке протоколов заседаний ГЭК.

На основании решения ГЭК лицам, успешно прошедшим государственную итоговую аттестацию, выдаются документы об образовании и о квалификации установленного образца

5.2 Основные требования и показатели, по которым производится оценка выполнения и защиты дипломного проекта и уровня профессиональной подготовленности обучающегося:

– умение четко формулировать рассматриваемую задачу, определять ее актуальность и значимость, структурировать решаемую задачу;

– обоснованно выбирать и корректно использовать наиболее эффективные методы решения задач;

– уметь генерировать и анализировать альтернативные варианты и принимать оптимальные решения с учетом множественности критериев, влияющих факторов и характера информации;

– использовать в работе современные информационные технологии, средства компьютерной техники и их программное обеспечение;

– уметь осуществлять поиск информации и работать со специальной литературой;

– грамотно, с использованием профессиональной терминологии и лексики, четко, в логической последовательности излагать содержание выполненных разработок.

Оценка «отлично» ставится выпускнику, если:

- соблюдены все правила оформления работы в соответствии с методическими рекомендациями по написанию выпускной квалификационной работы;

- четко обозначена актуальность работы;

- содержание соответствует теме работы;

- обучающийся четко, обоснованно и конкретно выражает свое мнение по поводу основных аспектов содержания работы;

- обучающийся достаточно свободно ориентируется в терминологии, используемой в работе;

- практическая часть строится на выводах теоретической части;

- ответы на вопросы членов ГЭК четкие, краткие, правильные;

- в процессе защиты соблюдены логика изложения, уместность использования наглядности, владение терминологией.

Оценка «хорошо» ставится выпускнику, если:

- имеются небольшие неточности в оформлении выпускной квалификационной работы;

- обозначена актуальность работы;

- содержание соответствует теме работы;

- практическая часть строится на выводах теоретической части;

- ответы на вопросы членов ГЭК правильные, но содержат технические или терминологические ошибки;

- присутствует логика изложения, уместность использования наглядности, владение терминологией.

Оценка «удовлетворительно» ставится выпускнику, если:

- допущено много нарушений в оформлении выпускной квалификационной работы;

- актуальность работы либо не сформулирована, либо сформулирована в самых общих чертах;

- содержание работы не соответствует заявленной теме;

- обучающийся слабо ориентируется в понятиях, терминах, которые использует в своей работе;

- в докладе выпускника нет четкости, последовательности изложения мысли. Оценка «неудовлетворительно» ставится выпускнику, если:

- допущены грубые нарушения в оформлении выпускной квалификационной работы;
- обнаружено значительное непонимание темы;
- основная мысль не выражена;
- в ответах выпускника нет смыслового единства, связанности; выпускник не ориентируется в терминологии работы;
- отсутствует логика изложения материала, графическая часть имеет ряд грубых ошибок.

5.3 Основные требования и показатели, по которым производится оценка результатов демонстрационного экзамена

Основные требования и показатели, по которым производится оценка результатов демонстрационного экзамена.

Процедура оценивания выполнения заданий демонстрационного экзамена осуществляется членами экспертной группы в соответствии с требованиями комплекта оценочной документации.

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100 %. Перевод баллов в оценку осуществляется по шкале:

Оценка ГИА	«2»	«3»	«4»	«5»
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 19,99%	20% - 39,99%	40% - 69,99%	70% – 100%

Баллы выставляются в протоколе проведения демонстрационного экзамена. Протокол проведения демонстрационного экзамена 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.

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.

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.

Лицам, прошедшим демонстрационный экзамен, выдается цифровой паспорт компетенций, подтверждающий уровень владения профессиональными умениями и навыками.

Цифровой паспорт компетенций содержит информацию об освоённой специальности, виде аттестации, пройденной выпускником, уровне демонстрационного экзамена, результатах сдачи демонстрационного экзамена.

6. Порядок апелляции и пересдачи государственной итоговой аттестации

6.1 По результатам ГИА выпускник имеет право подать в апелляционную комиссию письменное заявление о нарушении, по его мнению, установленного порядка проведения ГИА и/или несогласии с её результатами (далее – апелляция).

6.2 Апелляция подаётся лично выпускником или родителями (законными

представителями) несовершеннолетнего выпускника в апелляционную комиссию колледжа. Апелляция о нарушении порядка проведения ГИА подаётся непосредственно в день проведения ГИА. Апелляция о несогласии с результатами ГИА подаётся не позднее следующего рабочего дня после объявления результатов ГИА.

6.3 Апелляция рассматривается апелляционной комиссией не позднее трёх рабочих дней от даты её поступления.

6.4 Состав апелляционной комиссии утверждается руководителем образовательной организации в те же сроки, что и состав ГЭК.

6.5 Апелляционная комиссия формируется в количестве не менее пяти членов из числа педагогических работников образовательной организации, не входящих в данном учебном году в состав ГЭК и не являющихся председателем или секретарём ГЭК. Председателем апелляционной комиссии является руководитель образовательной организации, либо лицо, исполняющее в установленном порядке обязанности руководителя колледжа. Секретарь избирается из числа членов апелляционной комиссии.

6.6 Апелляция рассматривается на заседании апелляционной комиссии с участием не менее двух третей её состава.

На заседание апелляционной комиссии приглашается председатель соответствующей ГЭК. Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции. С несовершеннолетним выпускником имеет право присутствовать один из родителей (законных представителей). Указанные лица должны иметь при себе документы, удостоверяющие личность.

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

6.7 Рассмотрение апелляции не является пересдачей ГИА.

6.8 При рассмотрении апелляции о нарушении порядка проведения ГИА апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях порядка проведения ГИА выпускника не подтвердились и/или не повлияли на результат ГИА;

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

В случае удовлетворения апелляции результат проведения ГИА подлежит аннулированию, а протокол о рассмотрении апелляции, не позднее следующего рабочего дня, передаётся ГЭК для реализации решения 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.

6.9 Для рассмотрения апелляции о несогласии с результатами ГИА, полученными при защите дипломного проекта, 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 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.

6.10 При рассмотрении апелляции о несогласии с результатами ГИА апелляционная комиссия выносит одно из решений:

- об отклонении апелляции и сохранении результата ГИА;

- об удовлетворении апелляции и выставлении иного результата ГИА.

Решение апелляционной комиссии не позднее следующего рабочего дня передаётся в ГЭК и в случае удовлетворения апелляции является основанием для аннулирования ранее выставленных результатов ГИА выпускника и выставления новых.

6.11 Решение апелляционной комиссии принимается простым большинством голосов. При

равном числе голосов, голос председательствующего на заседании апелляционной комиссии является решающим.

6.12 Решение апелляционной комиссии оформляется протоколом, который подписывается председателем и секретарём апелляционной комиссии и хранится в архиве образовательной организации.

6.13 Решение апелляционной комиссии доводится до сведения подавшего апелляцию выпускника (под роспись) в течение трёх рабочих дней со дня заседания апелляционной комиссии.

6.14 Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

6.15 Обучающийся, не прошедший ГИА в установленные сроки по уважительной причине, имеет право пройти её без отчисления из образовательной организации.

При этом обучающийся должен предоставить в образовательную организацию документ, подтверждающий причину его отсутствия.

Дополнительные заседания ГЭК организуются в установленные образовательной организацией сроки, но не ранее 1 (одного) месяца и не позднее 4 (четырёх) месяцев после подачи заявления выпускником не прошедшим ГИА по уважительным причинам.

6.16 Обучающиеся, не прошедшие ГИА в связи с неявкой по неуважительной причине или в связи с получением оценки «неудовлетворительно» могут быть допущены для повторного участия в ГИА не более двух раз.

Обучающиеся, не прошедшие ГИА в связи с неявкой по неуважительной причине или в связи с получением оценки «неудовлетворительно», отчисляются из колледжа с выдачей справки об обучении, как не выполнившие обязанностей по добросовестному освоению образовательной программы. Такие выпускники проходят ГИА не ранее чем через 6 (шесть) месяцев после прохождения после прохождения ГИА впервые и не позднее чем через пять лет после срока проведения ГИА.

Для повторного прохождения ГИА указанное лицо, по его заявлению, восстанавливается в образовательной организации на установленный период времени, но не менее периода времени, предусмотренного календарным учебным графиком для ГИА.

ПРИЛОЖЕНИЕ

Предлагаемые темы дипломных проектов

№	Темы дипломных проектов	Соответствие тем дипломных проектов профессиональным модулям
1.	Анализ уязвимостей информационной безопасности в организации и разработка мер по их устранению	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
2.	Внедрение DLP-системы в комплексную систему обеспечения информационной безопасности компании	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
3.	Внедрение биометрического контроля доступа в организации	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
4.	Защита акустической информации в каналах связи предприятия	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
5.	Моделирование информационной безопасности предприятия	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами

6.	Обеспечение информационной безопасности в (название предприятия) от сетевых атак	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
7.	Организация защиты информации в локальной вычислительной сети предприятия	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
8.	Организация защиты информации по виброакустическому каналу утечки информации	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
9.	Построение системы активного отражения атак в корпоративных сетях.	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
10.	Проектирование и внедрение комплексного обеспечения информационной безопасности и защиты конфиденциальной информации в (название предприятия)	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
11.	Проектирование и внедрение сетевой инфраструктуры предприятия на базе ОС Альт	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>

12.	Проектирование и модернизация комплексной системы защиты информации в кабинете руководителя предприятия	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
13.	Проектирование и модернизация систем видеонаблюдения и сигнализации для обеспечения защиты информации в (название предприятия)	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
14.	Проектирование и модернизация систем видеонаблюдения и сигнализации для обеспечения защиты информации в (название предприятия)	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
15.	Проектирование и модернизация системы защиты информации предприятия (название предприятия)	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
16.	Проектирование информационной безопасности в беспроводных сетях	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
17.	Проектирование информационной безопасности предприятия	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>

18.	Проектирование комплексной защиты информации (название предприятия)	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
19.	Проектирование комплексной информационной безопасности на предприятии	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
20.	Проектирование комплексной системы обеспечения информационной безопасности в (название предприятия)	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
21.	Проектирование системы антивирусной защиты сети в торгово- сервисном центре	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
22.	Проектирование системы защиты и перехвата данных, обнаружение прослушивающих приложений	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>
23.	Проектирование системы защиты информации на основе биометрических данных в деятельности индивидуального предпринимателя	<p>ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении</p> <p>ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами</p> <p>ПМ.03 Защита информации техническими средствами</p>

24.	Проектирование системы защиты информации на предприятиях, применяющих сетевые технологии	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
25.	Проектирование системы защиты информации с использованием видеонаблюдения в организации	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
26.	Проектирование системы защиты информации с использованием СЭД (системы электронного документооборота)	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
27.	Проектирование системы защиты информации с применением видеонаблюдения	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
28.	Проектирование системы защиты персональных данных клиентов (название предприятия)	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
29.	Проектирование системы защиты персональных данных на предприятии	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами

30.	Проектирование системы защиты с использованием биометрических данных	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
31.	Проектирование системы инженерно-технической защиты кабинета руководителя предприятия	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
32.	Проектирование системы информационной безопасности в деятельности индивидуального предпринимателя	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
33.	Проектирование системы обеспечения инженерно-технической защиты объекта офиса	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
34.	Проектирование системы обеспечения инженерно-технической защиты объекта офиса	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
35.	Проектирование структуры виртуальной личной сети предприятия	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами

36.	Разработка виртуальной защищенной сети на базе ПО ViPNet	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
37.	Разработка виртуальной защищенной сети с использованием программного обеспечения ViPNet для обеспечения информационной безопасности	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
38.	Разработка защищенной структуры сегмента сети предприятия	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
39.	Совершенствование процедур и методов обеспечения защиты информации в (название предприятия)	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
40.	Совершенствование системы защиты персональных данных	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами
41.	Создание комплексной системы защиты персональных данных в организации	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами ПМ.03 Защита информации техническими средствами

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
 ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
 МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ

ПЛАН МЕРОПРИЯТИЙ

по организации проведения демонстрационного экзамена
 в рамках государственной итоговой аттестации выпускников

№ п/п	Мероприятия	Срок реализации	Ответственный исполнитель
Обязательная составляющая			
1	Подготовка экспертов для проведения ГИА с использованием механизма ДЭ	В течение года	Образовательная организация
Этапы подготовки и проведения ДЭ			
2	Формирование рабочей группы	Сентябрь	Образовательная организация
3	Определение и формирование количества выпускников среднего профессионального образования, сдающих государственную итоговую аттестацию в форме демонстрационного экзамена, установленного соответствующим федеральным государственным образовательным стандартом среднего профессионального образования (далее - ФГОС СПО)	Октябрь	Образовательная организация Образовательная организация
4	Изучение комплектов оценочной документации по определенным профессиям и специальностям, размещенных на сайте Института развития профессионального образования (ИРПО) https://bom.firpo.ru/	Октябрь	Образовательная организация
5	Разработка и согласование программы итоговой государственной аттестации	До 1 декабря	Образовательная организация
6	Составление графика проведения демонстрационного экзамена согласно учебному плану по специальностям и профессиям	До 20 декабря	Образовательная организация
7	Ознакомление выпускников, родителей, членов ГЭК с программой государственной итоговой аттестации, информировании о сроках и порядке проведения демонстрационного экзамена согласно графику	Не позднее 6 месяцев до начала ДЭ	Образовательная организация

8	Сбор заявлений выпускников профильного уровня 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.	Не позднее 6 месяцев до начала ДЭ	Образовательная организация
9	Сбор пакета документов по обучающимся (паспортные данные, ИНН, СНИЛС, электронная почта)		Образовательная организация
10	Назначение организационного эксперта, отвечающего за подготовку и сопровождение участников ДЭ	Январь	Образовательная организация
11	Проведение консультации психолога с обучающимися выпускных групп	Май-июнь	Образовательная организация
12	Определение регламента проведения ДЭ на площадке (план проведения ДЭ)	Май	Образовательная организация
13	Доведение до сведения обучающихся регламента	За день до начала ДЭ	Образовательная организация
2. Определение площадки			
14	Определение места (площадки) проведения ДЭ, формирование пакета документов и оформление заявки для аккредитации центра проведения демонстрационного экзамена	Март (не позднее 3-х месяцев до проведения ДЭ)	Образовательная организация
15	Формирование перечня оборудования и оснащения площадки, в соответствии с КОД и необходимого для проведения ДЭ	Январь-март	Образовательная организация
16	Назначение технического эксперта, отвечающего за подготовку оборудования и его работу во время ДЭ	Март	Образовательная организация
17	Подготовка площадки, установка оборудования и проверка его работоспособности	Ма1-июнь (не позднее 2-х дней до начала проведения ДЭ)	Образовательная организация
18	Проверка главным экспертом площадки проведению ДЭ на предмет готовности к проведению ДЭ, составление «Акта о готовности»	Май-июнь (за один день до проведения)	Главный эксперт
3. Проведение ДЭ			

19	Утверждение графика проведения ДЭ	Март -апрель	Образовательная организация
20	Формирование и согласование кандидатур на главных экспертов, составов экспертных групп по каждой профессии и специальности	Март-май	Образовательная организация
21	Распределение рабочих мест и инструктаж по технике безопасности	За день до начала ДЭ	Образовательная организация, главный эксперт, технический эксперт
22	Проведение процедуры ДЭ в соответствии с утвержденным регламентом		Образовательная организация
23	Обеспечение видеотрансляции проведения демонстрационного экзамена в сети Интернет	В день проведения ДЭ	Образовательная организация
4. Оценка выполнения заданий, формирование отчетной документации			
24	Утверждение главного эксперта	Ежегодно до 20 декабря (в случае если это председатель ГЭК)	Департамент образования и науки Тюменской области
25	Проведение процедуры оценивания в соответствии с утвержденными критериями оценивания, определенными в КОД	В день проведения ДЭ	Экспертная группа
26	Оформление ведомостей, протоколов	В день проведения ДЭ	Главный эксперт, экспертная группа
27	Подведение итогов демонстрационного экзамена и анализ результатов		Главный эксперт, ГЭК

План проведения демонстрационного экзамена

Наименование центра проведения демонстрационного экзамена:	Федеральное государственное бюджетное образовательное учреждение высшего образования «Югорский государственный университет» Многопрофильный колледж
Полный адрес места центра проведения демонстрационного экзамена:	г. Ханты-Мансийск, ул. Чехова 16
Кабинет, цех, площадка, иной индивидуализируемый объект:	Кабинет №2/525
Уровень демонстрационного экзамена:	Профильный
Код и наименование специальности СПО:	10.02.05 Обеспечение информационной безопасности автоматизированных систем
Номер (наименование) комплекта оценочной документации:	КОД 10.02.05-1-2025
Количество рабочих мест:	8

Примерное расписание сдачи демонстрационного экзамена*

Дата	Мероприятие	Рабочее время	Время на представление задания
С-1 ПОДГОТОВИТЕЛЬНЫЙ ДЕНЬ			
	Прибытие экспертов и участников демонстрационного экзамена. Встреча и знакомство экспертов. Знакомство участников и экспертов с конкурсными местами. Подготовка и обучение экспертов. Подготовка участков к демонстрационному экзамену в соответствии с документацией.	8:00 - 16:00	
ДЕНЬ ПРОВЕДЕНИЯ ЭКЗАМЕНА – 1 группа			
	Сбор обучающихся и регистрация на демонстрационном участке. Инструктаж по ОТ и ТБ. Выдача заданий, обсуждение, вопросы эксперту.	8:00 - 8:30	
	Работа участников	8:30 - 12:00	3 ч. 30 мин.
	Оценка заданий членами экспертной группы	12:10 - 12:40	
	Внесение оценок главным экспертом в ЦП	12:40 - 14:00	
	Проверка и подписание оценочных ведомостей экспертами. Блокировка оценок	14:00 - 14:30	
ДЕНЬ ПРОВЕДЕНИЯ ЭКЗАМЕНА – 2 группа			
	Сбор обучающихся и регистрация на демонстрационном участке. Инструктаж по ОТ и ТБ. Выдача заданий, обсуждение, вопросы эксперту.	8:00 - 8:30	
	Работа участников	8:30 - 12:00	3 ч. 30 мин.
	Оценка заданий членами экспертной группы	12:10 - 12:40	
	Внесение оценок главным экспертом в ЦП	12:40 - 14:00	
	Проверка и подписание оценочных ведомостей экспертами. Блокировка оценок	14:00 - 14:30	
ДЕНЬ ПРОВЕДЕНИЯ ЭКЗАМЕНА – 3 группа			

	Сбор обучающихся и регистрация на демонстрационном участке. Инструктаж по ОТ и ТБ. Выдача заданий, обсуждение, вопросы эксперту.	8:00 - 8:30	
	Работа участников	8:30 - 12:00	3 ч. 30 мин.
	Оценка заданий членами экспертной группы	12:10 - 12:40	
	Внесение оценок главным экспертом в ЦП	12:40 - 14:00	
	Проверка и подписание оценочных ведомостей экспертами. Блокировка оценок	14:00 - 14:30	

* дата и время начала проведения демонстрационного экзамена, расписание сдачи экзаменов в составе экзаменационных групп, планируемая продолжительность проведения демонстрационного экзамена, технические перерывы в проведении демонстрационного экзамена определяются планом проведения демонстрационного экзамена, утверждаемым ГЭК совместно с образовательной организацией не позднее чем за двадцать календарных дней до даты проведения демонстрационного экзамена

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

Том 1

(комплект оценочной документации)

Код и наименование специальности среднего профессионального образования	10.02.05 Обеспечение информационной безопасности автоматизированных систем
Наименование квалификации (наименование направленности)	Техник по защите информации
Федеральный государственный образовательный стандарт среднего профессионального образования по профессии (специальности) среднего профессионального образования (СПО)	ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, Приказ Министерства образования и науки России от 09.12.2016 N 1553 (ред. от 17.12.2020)
Вид аттестации	Государственная итоговая аттестация
Уровень демонстрационного экзамена	Профильный
Шифр комплекта оценочной документации	КОД 10.02.05-1-2025

Список используемых сокращений

ГИА - государственная итоговая аттестация

ДЭ - демонстрационный экзамен

ДЭ ПУ - демонстрационный экзамен профильного уровня

КОД - комплект оценочной документации

ОК - общая компетенция

ОМ - оценочный материал

ПА - промежуточная аттестация

ПК - профессиональная компетенция

СПО - среднее профессиональное образование

ФГОС СПО – федеральный государственный образовательный стандарт среднего профессионального образования, на основе которого разработан комплект оценочной документации

ЦПДЭ - центр проведения демонстрационного экзамена

Структура КОД

1. Комплекс требований для проведения демонстрационного экзамена;
2. Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания;
3. Примерный план застройки площадки ДЭ;
4. Требования к составу экспертных групп;
5. Инструкции по технике безопасности;
6. Образец задания.

Комплект оценочной-документации (КОД)

1 Комплекс требований для проведения ДЭ

Применимость КОД. Настоящий КОД предназначен для организации и проведения ДЭ (уровней ДЭ) в рамках ГИА по образовательным программам СПО, указанным в таблице № 1.

Таблица № 1

Вид аттестации	Уровень демонстрационного экзамена
Государственная итоговая аттестация	Профильный

КОД в части ГИА (ДЭ ПУ) разработан на основе требований к результатам освоения образовательной программы СПО, установленных в соответствии с ФГОС СПО, включая квалификационные требования, заявленные организациями, работодателями, заинтересованными в подготовке кадров соответствующей квалификации.

КОД в части ГИА (ДЭ ПУ) включает инвариантную часть, содержание которой определяет образовательная организация самостоятельно, на основе содержания реализуемой основной образовательной программы СПО, включая квалификационные требования, заявленные организациями, работодателями, заинтересованными в подготовке кадров соответствующей квалификации, в том числе стороной договора о сетевой форме реализации образовательных программ и (или) договора о практической подготовке обучающихся.

Общие организационные требования

1. ДЭ направлен на определение уровня освоения выпускником материала, предусмотренного образовательной программой, и степени сформированности профессиональных умений и навыков путем проведения независимой экспертной оценки выполненных выпускником практических заданий в условиях реальных или смоделированных производственных процессов.

2. ДЭ в рамках ГИА проводится с использованием КОД, включенных образовательными организациями в программу ГИА.

3. Задания ДЭ доводятся до главного эксперта в день, предшествующий дню начала ДЭ.

4. Образовательная организация обеспечивает необходимые технические условия для обеспечения заданиями во время ДЭ обучающихся, членов ГЭК, членов экспертной группы.

5. ДЭ проводится в ЦПДЭ, представляющем собой площадку, оборудованную и оснащенную в соответствии с КОД.

6. ЦПДЭ может располагаться на территории образовательной организации, а при сетевой форме реализации образовательных программ — также на территории иной организации, обладающей необходимыми ресурсами для организации ЦПДЭ.

7. Обучающиеся проходят ДЭ в ЦПДЭ в составе экзаменационных групп.

8. Образовательная организация знакомит с планом проведения ДЭ обучающихся, сдающих ДЭ, и лиц, обеспечивающих проведение ДЭ, в срок не позднее чем за 5 рабочих дней до даты проведения экзамена.

9. Количество, общая площадь и состояние помещений, предоставляемых для проведения ДЭ, должны обеспечивать проведение ДЭ в соответствии с КОД.

10. Не позднее, чем за один рабочий день до даты проведения ДЭ главным экспертом проводится проверка готовности ЦПДЭ в присутствии членов экспертной группы, обучающихся, а также технического эксперта, назначаемого организацией, на территории которой расположен ЦПДЭ, ответственного за соблюдение установленных норм и правил охраны труда и техники

безопасности.

11. Главным экспертом осуществляется осмотр ЦПДЭ, распределение обязанностей между членами экспертной группы по оценке выполнения заданий ДЭ, а также распределение рабочих мест между обучающимися с использованием способа случайной выборки. Результаты распределения обязанностей между членами экспертной группы и распределения рабочих мест между обучающимися фиксируются главным экспертом в соответствующих протоколах.

12. Обучающиеся знакомятся со своими рабочими местами, под руководством главного эксперта также повторно знакомятся с планом проведения ДЭ, условиями оказания первичной медицинской помощи в ЦПДЭ. Факт ознакомления отражается главным экспертом в протоколе распределения рабочих мест.

13. Допуск обучающихся в ЦПДЭ осуществляется главным экспертом на основании документов, удостоверяющих личность.

14. Образовательная организация обязана не позднее, чем за один рабочий день до дня проведения ДЭ уведомить главного эксперта об участии в проведении ДЭ тьютора (ассистента).

Требование к продолжительности ДЭ

Продолжительность ДЭ

Таблица 2

Вид аттестации	Уровень демонстрационного экзамена	Составная часть	Продолжительность демонстрационного экзамена
ГИА	Профильный	Инвариантная часть	3 ч. 30 мин

Требования к содержанию КОД

Единое базовое ядро содержания КОД (таблица № 3) сформировано на основе вида деятельности (вида профессиональной деятельности) в соответствии с ФГОС СПО и является общей содержательной основой заданий ДЭ вне зависимости от вида аттестации и уровня ДЭ.

Таблица № 3

ЕДИНОЕ БАЗОВОЕ ЯДРО СОДЕРЖАНИЯ КОД		
Вид деятельности / Вид профессиональной деятельности	Перечень оцениваемых ОК / ПК	Перечень оцениваемых умений, навыков (практического опыта)
Эксплуатация информационно – телекоммуникационных систем и сетей	ПК: производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей	Практический опыт: монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей Умения: настраивать, эксплуатировать и обслуживать оборудование ИТКС
	ОК: использовать информационные технологии в профессиональной деятельности	Умения: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
	Защита информации в информационно – телекоммуникационных системах и сетях с использованием 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 и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей
ПК: поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях		Умения: проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации

Инвариантная часть КОД		
Эксплуатация информационно – телекоммуникационных систем и сетей	ПК: производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей	Практический опыт: монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей Умения: настраивать, эксплуатировать и обслуживать оборудование ИТКС
	ОК: использовать информационные технологии в профессиональной деятельности	Умения: применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение
	ПК: 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	Умения: проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации Умения: проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации
Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	ПК: поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	Умения: проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации
	ПК: осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей	Умения: проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС
Эксплуатация информационно – телекоммуникационных систем и сетей	ПК: производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств	Практический опыт: установки, настройки, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС

криптографических средств защиты	защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно – телекоммуникационных систем и сетей	
	ПК: поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	Практический опыт: поддержания бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС
	ПК: 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 предъявленными требованиями.	Практический опыт: защиты 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 Умения: проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации
Эксплуатация информационно – телекоммуникационных систем и сетей	ПК: осуществлять контроль функционирования информационно – телекоммуникационных систем и сетей	Практический опыт: текущего контроля функционирования оборудования ИТКС
		Умения: настраивать, эксплуатировать и обслуживать оборудование ИТКС
		Умения: производить испытания, проверку и приемку оборудования ИТКС
Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	ПК: поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях	Умения: проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации
		Умения: проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации

Требования к оцениванию

Распределение значений максимальных баллов (таблица № 5) зависит от вида аттестации, уровня ДЭ, составной части КОД.

Таблица № 5

Вид аттестации	Уровень ДЭ	Составная часть КОД	Максимальный
ГИА	ДЭ ПУ	Инвариантная	80 из 80

Распределение баллов по критериям оценивания для ДЭ в рамках ГИА представлено в таблице № 6.

Таблица №6

№ п/п	Модуль задания (вид деятельности, вид профессиональной деятельности)	Критерий оценивания	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 защиты информации 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	3,00

		криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	
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 криптографических средств защиты	Производство установки, настройки, испытаний и конфигурирования программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетей	6,00
		Поддержка бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	6,00
		Осуществление защиты информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием	6,00

		программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями	
5	Эксплуатация информационно – телекоммуникационных систем и сетей	Осуществление контроля функционирования информационно – телекоммуникационных систем и сетей	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 защиты информации 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
ИТОГО			80

3.4 Требования к составу экспертных групп

Количественный состав экспертной группы определяется образовательной организацией, исходя из числа сдающих одновременно ДЭ обучающихся. Один эксперт должен иметь возможность оценить результаты выполнения обучающимися задания в полной мере согласно критериям оценивания.

Количество экспертов ДЭ ГИА представлено в таблице № 7.

Таблица 7

Кол-во рабочих мест в ЦПДЭ	Максимальное кол-во обучающихся участников ДЭ (одновременно в ЦПДЭ)	Кол-во экспертов (одновременно в ЦПДЭ)
8	8	3

Инструкция по технике безопасности

1. Общие требования по технике безопасности и охране труда.

1.1. Оператор ПК обязан: — соблюдать требования настоящей инструкции, инструкции о мерах пожарной безопасности, инструкции по электробезопасности; — соблюдать правила личной гигиены; — уметь оказывать первую помощь пострадавшему, знать место нахождения аптечки, а также уметь пользоваться средствами пожаротушения и знать место их нахождения.

1.2. На площадке, в зоне проведения ДЭ необходимо создать оптимальные условия зрительной работы. Освещенность рабочего места при смешанном освещении (в горизонтальной плоскости в зоне размещения клавиатуры и рабочих документов) должна быть в пределах от 300 до 500 Лк. Основной поток естественного света должен быть слева, солнечные лучи и блики не должны попадать в поле зрения работающего и на экраны видеомониторов.

1.3. Монитор должен находиться на расстоянии 50-70 см от глаз оператора ПК и иметь антибликовое покрытие. Покрытие должно также обеспечивать снятие электростатического заряда с поверхности экрана, исключать искрение и накопление пыли.

1.4. Нельзя загораживать заднюю стенку системного блока или ставить ПК вплотную к стене, это приводит к нарушению охлаждения системного блока и его перегреву.

1.5. Непрерывная продолжительность работы с ПК не должна превышать 4 часа. Через каждый час работы необходимо делать перерывы на отдых по 5-10 минут или по 15-20 минут каждые два часа работы.

2. Требования по технике безопасности и охране труда перед началом работы.

2.1 Перед началом выполнения работ участнику ДЭ необходимо: - осмотреть и привести в порядок рабочее место, убрать все посторонние предметы, которые могут отвлекать внимание и затруднять работу; - проверить правильность установки стола, стула, подставки под ноги, угол наклона экрана монитора, положения клавиатуры в целях исключения неудобных поз и длительных напряжений тела.

Особо обратить внимание на то, что дисплей должен находиться на расстоянии не менее 50 см от глаз (оптимально 60-70 см);

- проверить правильность расположения оборудования;
- кабели электропитания, удлинители, сетевые фильтры должны находиться с тыльной стороны рабочего места, сетевые фильтры не должны лежать на полу;
- убедиться в отсутствии засветок, отражений и бликов на экране монитора;
- убедиться в том, что на устройствах ПК (системный блок, монитор, клавиатура) не располагаются сосуды с жидкостями, сыпучими материалами (чай, кофе, сок, вода и пр.);
- включить электропитание в последовательности, установленной инструкцией по эксплуатации на оборудование;
- убедиться в правильном выполнении процедуры загрузки оборудования, правильных настройках.

2.2 Участнику запрещается приступать к выполнению задания при обнаружении неисправности оборудования. О замеченных недостатках и неисправностях немедленно сообщить эксперту и до устранения неполадок к заданию не приступать.

3. Требования по технике безопасности и охране труда во время работы.

3.1. Во время работы быть внимательным, не отвлекаться на посторонние дела и разговоры, не отвлекать других.

3.2. Рабочее место должно быть оборудовано так, чтобы исключать неудобные позы и длительные статические напряжения тела.

3.3. При работе на ПК должна быть исключена возможность одновременного прикосновения к оборудованию и к частям помещения или оборудования, имеющим соединение с землей (радиаторы батарей, металлоконструкции).

3.4. Во время работы нельзя класть на монитор бумаги, книги и другие предметы, которые могут закрыть его вентиляционные отверстия.

3.5. Участнику демонстрационного экзамена во время работы запрещается:

— касаться одновременно экрана монитора и клавиатуры; — прикасаться к задней панели системного блока при включенном питании;

— переключение разъемов интерфейсных кабелей периферийных устройств при включенном питании;

— загромождать верхние панели устройств бумагами и посторонними предметами;

— допускать захламленность рабочего места бумагой, в цепях не должно накапливаться пыль;

— производить отключение питания во время выполнения активной задачи;

— производить частые переключения питания;

— допускать попадание влаги на поверхность системного блока, монитора;

— производить самостоятельно вскрытие и ремонт оборудования.

4. Требования по технике безопасности и охране труда в аварийных ситуациях.

4.1. При обнаружении неисправности в работе электрических устройств, находящихся под напряжением (повышенном их нагреве, появления искрения, запаха гари, задымления и т.д.), участнику следует немедленно сообщить о случившемся экспертам.

Выполнение конкурсного задания продолжить только после устранения возникшей неисправности.

4.2. В случае возникновения у участника плохого самочувствия или получения травмы сообщить об этом эксперту.

4.3. При поражении участника электрическим током немедленно отключить электросеть, оказать первую помощь (самопомощь) пострадавшему, сообщить эксперту, при необходимости обратиться к врачу.

4.4. При несчастном случае или внезапном заболевании необходимо в первую очередь отключить питание электрооборудования, сообщить о случившемся экспертам, которые должны принять мероприятия по оказанию первой помощи пострадавшим, вызвать скорую медицинскую помощь, при необходимости отправить пострадавшего в ближайшее лечебное учреждение.

4.5. При возникновении пожара необходимо немедленно оповестить Главного эксперта и экспертов. При последующем развитии событий следует руководствоваться указаниями Главного эксперта.

4.6. При обнаружении взрывоопасного или подозрительного предмета не подходите близко к нему, предупредите о возможной опасности находящихся поблизости экспертов или обслуживающий персонал. При происшествии взрыва необходимо спокойно уточнить обстановку и действовать по указанию экспертов.

5. Требования по технике безопасности и охране труда по окончании работы.

5.1 По окончании работы участник соревнования обязан соблюдать следующую последовательность отключения оборудования: - произвести завершение всех выполняемых на ПК задач; - отключить питание в последовательности, установленной инструкцией по эксплуатации данного оборудования.

5.2. Убрать со стола рабочие материалы и привести в порядок рабочее место.

5.3. Обо всех замеченных неполадках сообщить эксперту.

Организационные требования:

1. Технический эксперт под подпись знакомит главного эксперта, членов экспертной группы, обучающихся с требованиями охраны труда и безопасности производства.

2. Все участники ДЭ должны соблюдать установленные требования по охране труда и производственной безопасности, выполнять указания технического эксперта по соблюдению указанных требований

Образец задания

Модуль № 1: Эксплуатация информационно – телекоммуникационных систем и сетей

Вид аттестации/уровень ДЭ: 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.

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»:110.110.10.64/28 Офис 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 том числе криптографических средств защиты

Вид аттестации/уровень ДЭ: 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-Admin (ЦО)): Центр управления сетью (серверное и клиентское приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ).

Задача 2.2. Установка ПО VPN Client на рабочее место администратора и для организации 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, рабочее место пользователя. Необходимые приложения: отсутствуют.

Модуль № 1: Эксплуатация информационно – телекоммуникационных систем и сетей

Вид аттестации/уровень ДЭ: ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

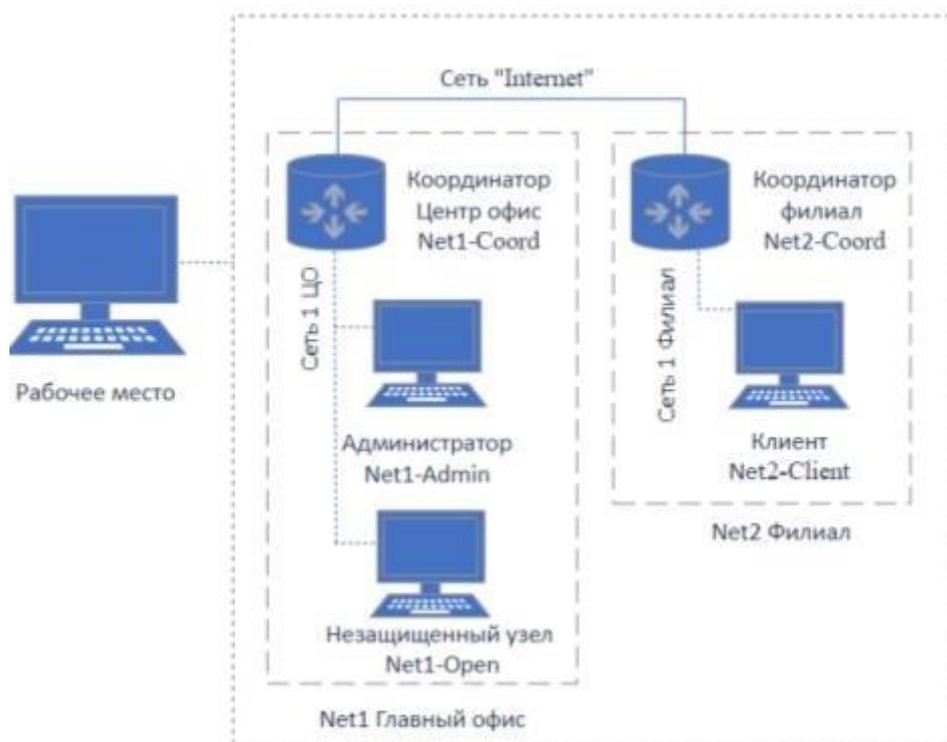
Задача 1.2. Инициализация VPN Coordinator На виртуальной машине Net1-Coord (ЦО) инициализировать Coordinator HWVA, на виртуальной машине Net2-Coord (Филиал) инициализировать Coordinator HW-VA. Необходимые приложения: отсутствуют.

Модуль № 2: Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты

Вид аттестации/уровень ДЭ: 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 технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.



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

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 узлов защищенной 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 том числе криптографических средств защиты

Вид аттестации/уровень ДЭ: 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 меж сетевого 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 асимметричных межсетевых ключей, между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

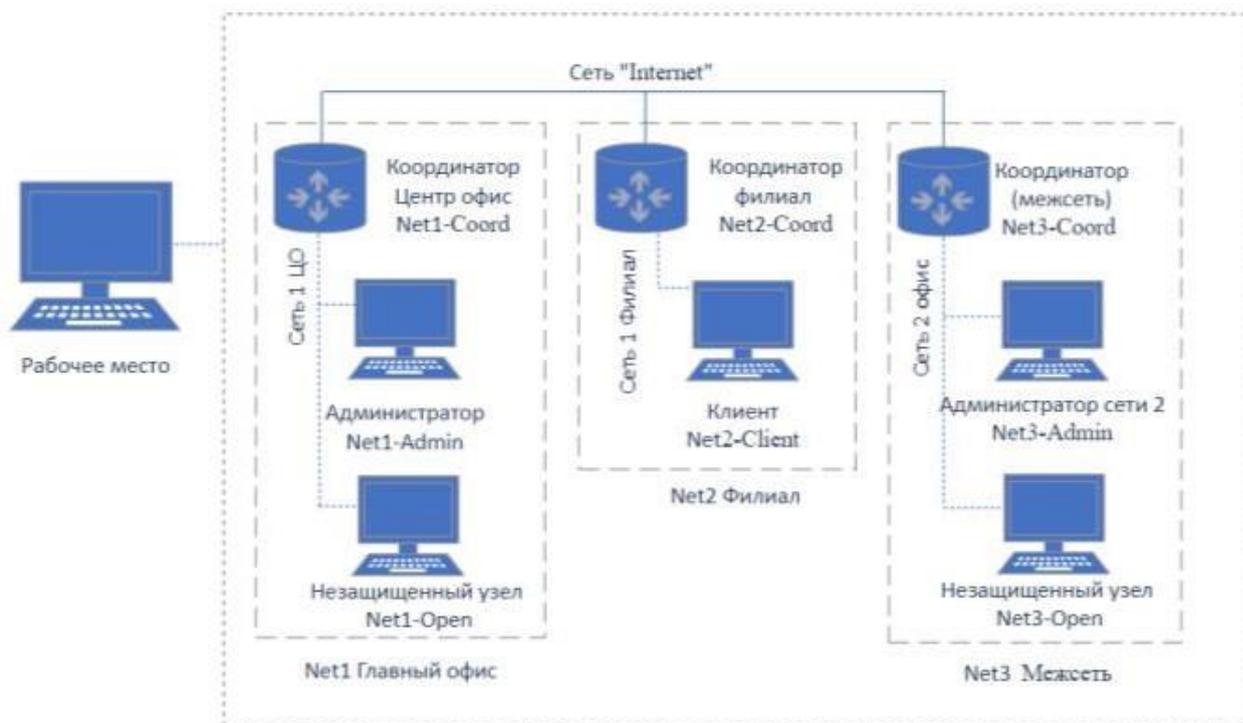


Рисунок 2 - Схема межсетевого взаимодействия

Проверить взаимодействие узлов, отправив сообщение деловой почты с узла Администратор 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 том числе 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 процедуру смены 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 сетей

Вид аттестации/уровень ДЭ: ГИА ДЭ ПУ (инвариантная часть)

Текст задания:

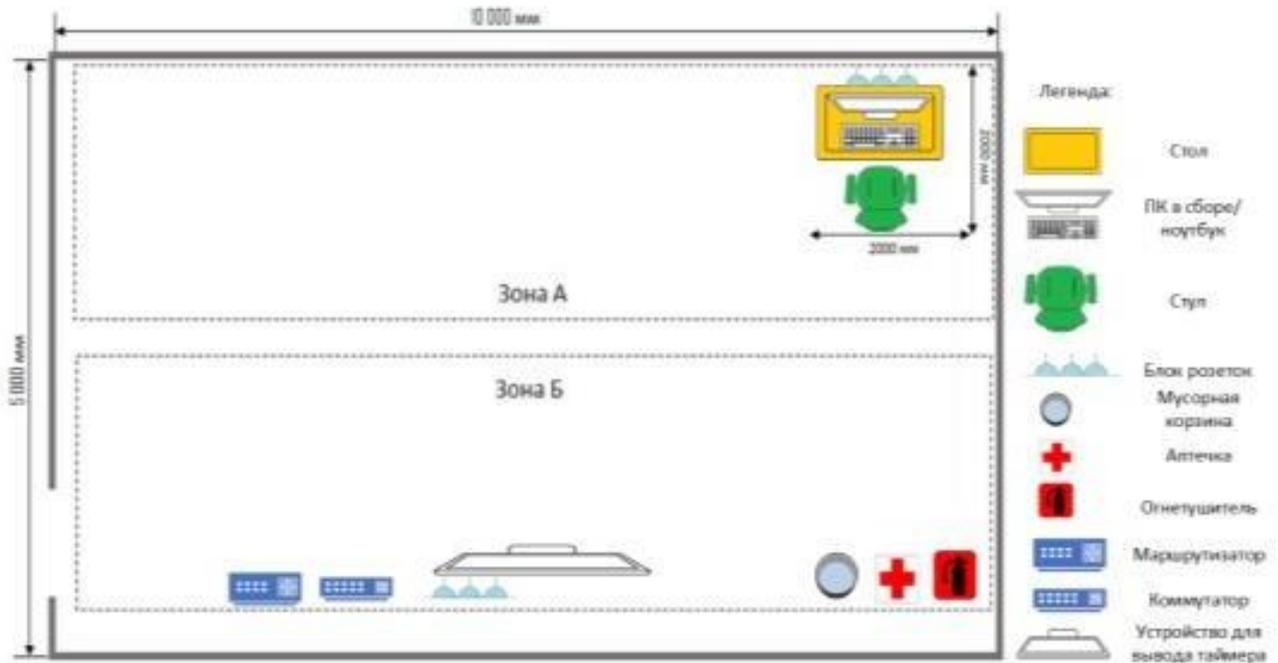
Задача 1.3. Туннелирование в рамках межсетевого взаимодействия

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 зашифрованному 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.

Примерный план застройки площадки для ГИА в форме ДЭ ПУ



ЛИСТ ОЗНАКОМЛЕНИЯ
с программой государственной итоговой аттестации

Специальность: 10.02.05 Обеспечение информационной безопасности
автоматизированных систем Группа ____

№	Фамилия, имя, отчество обучающегося	Дата ознакомления	Подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			

С программой государственной итоговой аттестации выпускников ознакомил:

_____ наименование должности	_____ подпись	<i>(И.О. Фамилия)</i> _____ расшифровка подписи
---------------------------------	------------------	---