

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ДАГЕСТАН  
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
РЕСПУБЛИКИ ДАГЕСТАН «ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н. АШУРАЛИЕВА»

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ**  
**государственной итоговой аттестации**  
выпускников по специальности  
среднего профессионального образования  
10.02.05 Обеспечение информационной безопасности автома-  
тизированных систем  
2024 -2025 учебный год

Квалификации выпускника: техник по защите информации

г. Махачкала, 2024 г.

## Оглавление:

1.	ОБЩИЕ ПОЛОЖЕНИЯ.....	3
1.1.	Нормативные и методические основания: .....	3
1.2.	Результаты освоения образовательной программы и формы проверки их освоения	4
2.	ДЕМОНСТРАЦИОННЫЙ ЭКЗАМЕН.....	15
2.1.	Оценивание результатов демонстрационного экзамена .....	16
2.2.	Образец задания демонстрационного экзамена профильного уровня в рамках ГИА (ГИА/ДЭ ПУ) .....	17
2.3.	Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания.....	22
2.4.	План застройки площадки ЦПДЭ .....	29
2.5.	Примерный план проведения демонстрационного экзамена в рамках государственной итоговой аттестации выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.....	30
3.	ДИПЛОМНЫЙ ПРОЕКТ .....	32
3.1.	Методика оценивания дипломных проектов.....	33
3.2.	Темы дипломных проектов .....	43

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

Фонд оценочных средств государственной итоговой аттестации выпускников по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем (далее – ФОС ГИА) является частью программы ГИА по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

ФОС ГИА выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем включает в себя результаты освоения образовательной программы и формы проверки их освоения, задания ГИА выпускников. Задания ГИА выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем включает в себя тематику дипломных проектов и комплект оценочной документации для демонстрационного экзамена.

Государственная итоговая аттестация по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем проводится в форме демонстрационного экзамена и защиты дипломного проекта.

ГИА представляет собой форму оценки степени и уровня освоения обучающимися образовательной программы.

ГИА проводится государственной экзаменационной комиссией (далее ГЭК) в целях определения соответствия результатов освоения обучающимися основной профессиональной образовательной программы специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем соответствующим требованиям федерального государственного образовательного стандарта.

ГЭК принимает решение о присвоении выпускникам квалификации «Техник по защите информации» на основе выявления готовности выпускников к решению профессиональных задач, соответствующих основным видам деятельности; степени освоения выпускниками профессиональных компетенций, сформированности общих компетенций.

### 1.1. Нормативные и методические основания:

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

Приказ Минпросвещения России от 08.11.2021 N 800 "Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования" (Зарегистрировано в Минюсте России 07.12.2021 N 66211);

Приказ Министерства образования и науки Российской Федерации № 1553 от 9 декабря 2016 г. "Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденным (зарегистрирован Министерством юстиции РФ 26 декабря 2016 г. N 44938);

Приказ Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022 г. N 536н «Об утверждении профессионального стандарта "Специалист по защите информации в телекоммуникационных системах и сетях"» (Зарегистрировано в Минюсте России 18 октября 2022 г. N 70596);

Приказ Министерства труда и социальной защиты Российской Федерации от 14.09.2022 N 533н "Об утверждении профессионального стандарта "Специалист по безопасности компьютерных систем и сетей" (Зарегистрировано в Минюсте России 14.10.2022 N 70515);

Приказ Министерства труда и социальной защиты Российской Федерации от 14.09.2022 N 525н "Об утверждении профессионального стандарта "Специалист по защите информации в автоматизированных системах" (Зарегистрировано в Минюсте России 14.10.2022 N 70543);

Приказ Министерства труда и социальной защиты Российской Федерации от 09.08.2022 N 474н "Об утверждении профессионального стандарта "Специалист по технической защите информации" (Зарегистрировано в Минюсте России 09.09.2022 N 70015)

Приказ Минпросвещения России от 24.08.2022 N 762 "Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования" (Зарегистрировано в Минюсте России 21.09.2022 N 70167);

Оценочные материалы для демонстрационного экзамена профильного уровня опубликованные на сайте <https://de.firpo.ru/> (комплект оценочной документации КОД 10.02.05-1-2025 для организации и проведения аттестации обучающихся по программе среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем в форме демонстрационного экзамена;

ГОСТ 2.051-2013. Межгосударственный стандарт. Единая система конструкторской документации. Электронные документы. Общие положения (введен в действие Приказом Росстандарта от 22.11.2013 N 1628-ст);

ГОСТ 7.32-2017. Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления (введен в действие Приказом Росстандарта от 24.10.2017 N 1494-ст);

ГОСТ Р 7.0.100-2018. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая запись. Библиографическое описание. Общие требования и правила составления (утв. и введен в действие Приказом Росстандарта от 03.12.2018 N 1050-ст);

ГОСТ Р 7.0.5-2008. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления (утв. и введен в действие Приказом Ростехрегулирования от 28.04.2008 N 95-ст);

ГОСТ 19.201-78 (СТ СЭВ 1627-79). Государственный стандарт Союза ССР. Единая система программной документации. Техническое задание. Требования к содержанию и оформлению (введен в действие Постановлением Госстандарта СССР от 18.12.1978 N 3351);

ГОСТ 25123-82 (СТ СЭВ 1625-79). Машины вычислительные и системы обработки данных. Техническое задание. Порядок построения, изложения и оформления. (введен Постановлением Госстандарта СССР от 09.02.1982 N 496);

Учебный план и календарный учебный график по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем;

Локальные акты, регулирующие вопросы организации и проведения государственной итоговой аттестации в Колледже, в том числе: Положение об организации и порядке проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования в государственном бюджетном профессиональном образовательном учреждении Республики Дагестан «Технический колледж Р.Н. Ашуралиева».

## **1.2. Результаты освоения образовательной программы и формы проверки их освоения**

Выпускник готовится к следующим основным видам деятельности:

- Эксплуатация автоматизированных (информационных) систем в защищенном исполнении;
- Защита информации в автоматизированных системах программными и программно-аппаратными средствами;
- Защита информации техническими средствами;
- Освоение профессии рабочего 16199 Оператор электронно-вычислительных и вычислительных машин.

В результате освоения образовательной программы у выпускника должны быть сформированы общие и профессиональные компетенции соответствующие основным видам

деятельности.

Выпускник, освоивший образовательную программу, должен обладать следующими общими компетенциями (далее - ОК):

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

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

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

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

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

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

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

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

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

Выпускник, освоивший образовательную программу, должен обладать профессиональными компетенциями (далее - ПК), соответствующими основным видам деятельности (профессиональным модулям - ПМ):

### **01. 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.

### **02. 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.

### **03. 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.

### **03 Освоение профессии рабочего 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;

Профессиональные модули (ПМ) и профессиональные компетенции (ПК) ФГОС СПО специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, **проверяемые на демонстрационном экзамене** по компетенции F7 Корпоративная защита внутренних угроз информационной безопасности в соответствии с комплектом оценочной документации 1.2-2023-2025:

#### **01. 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.

#### **02. 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.

### Основные показатели оценки результатов освоения образовательной программы и форма проверки освоения компетенций

Таблица 1 – Показатели и форма проверки сформированности общих компетенций (ОК)

	<b>Общие компетенции</b>	<b>Показатели освоения компетенции (знания, умения)</b>	<b>Форма проверки сформированности компетенции</b>
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	<p><b>Умения:</b> распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы;</p> <p>составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).</p> <p><b>Знания:</b> актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте.</p> <p>алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.</p>	ДП
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	<p><b>Умения:</b> определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска;</p> <p>применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение</p> <p><b>Знания</b> номенклатура информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации;</p> <p>современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности</p>	ДЭ
ОК 03	Планировать и реализовывать собственное профессиональное и	<p><b>Умения:</b> определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития</p>	ДП

	личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях	<b>Знания:</b> содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования	
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде	<b>Умения:</b> организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами <b>Знания:</b> психология коллектива; психология личности; основы проектной деятельности	ДП
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	<b>Умения:</b> излагать свои мысли на государственном языке; оформлять документы. <b>Знания:</b> особенности социального и культурного контекста; правила оформления документов.	ДП
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	<b>Умения:</b> описывать значимость своей профессии Презентовать структуру профессиональной деятельности по специальности <b>Знания:</b> сущность гражданско-патриотической позиции Общечеловеческие ценности Правила поведения в ходе выполнения профессиональной деятельности	ДП
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях	<b>Умения:</b> соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности. <b>Знания:</b> правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения.	ДП
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	<b>Умения:</b> использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности <b>Знания:</b> роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.	ДП

ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках	<b>Умения:</b> понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	ДП
		<b>Знания:</b> правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности	

Таблица 2 – Показатели освоения и форма проверки общих (ОК) и профессиональных компетенций (ПК)

Основные виды деятельности (профессиональные модули ПМ)	Перечень оцениваемых ОК, ПК	Перечень оцениваемых умений, навыков (практического опыта)	Форма проверки освоения компетенций
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	<b>Практический опыт:</b> установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем	ДП и ДЭ
		<b>Умения:</b> осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем	ДП
		<b>Знания:</b> состав и принципы работы автоматизированных систем, операционных систем и сред; принципы разработки алгоритмов программ, основных приемов программирования; модели баз данных; принципы построения, физические основы работы периферийных устройств	ДП
	ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	<b>Практический опыт:</b> администрирование автоматизированных систем в защищенном исполнении	ДП и ДЭ
		<b>Умения:</b> организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы	ДП и ДЭ
		<b>Знания:</b> теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации	ДП

	ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	<b>Практический опыт:</b> эксплуатация компонентов систем защиты информации автоматизированных систем	ДП
		<b>Умения:</b> настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам	ДП и ДЭ
		<b>Знания:</b> порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях	ДП
	ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении	<b>Практический опыт:</b> диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении	ДП и ДЭ
		<b>Умения:</b> обеспечивать работоспособность, обнаруживать и устранять неисправности	ДП и ДЭ
		<b>Знания:</b> принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации	ДП
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	<b>Практический опыт:</b> установка, настройка программных средств защиты информации в автоматизированной системе	ДП и ДЭ
		<b>Умения:</b> устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	ДП и ДЭ
		<b>Знания:</b> особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	ДП
	ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	<b>Практический опыт:</b> обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами;	ДП
		<b>Практический опыт:</b> использование программных и программно-аппаратных средств для защиты информации в сети	ДП и ДЭ
		<b>Умения:</b> устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	ДП и ДЭ
		<b>Знания:</b> особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных	ДП

	ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	<b>Практический опыт:</b> тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации	ДП и ДЭ
		<b>Умения:</b> диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;	ДП и ДЭ
		<b>Знания:</b> методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации	ДП
	ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	<b>Практический опыт:</b> решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных	
		<b>Умения:</b> применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований;	ДП
		<b>Умения:</b> использовать типовые программные криптографические средства, в том числе электронную подпись	ДП и ДЭ
		<b>Знания:</b> особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации	ДП
	ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	<b>Практический опыт:</b> учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности	ДП
		<b>Умения:</b> применять средства гарантированного уничтожения информации	
		<b>Знания:</b> особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации	
	ПК 2.6. Осуществлять регистрацию основных	<b>Практический опыт:</b> работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе	ДП

	<p>событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</p>	<p><b>Умения:</b> устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак</p> <p><b>Знания:</b> типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа</p>	
<p>Защита информации техническими средствами</p>	<p>ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации</p>	<p><b>Практический опыт:</b> установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации</p> <p><b>Умения:</b> применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных</p> <p><b>Знания:</b> порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам</p>	<p>ДП</p>
	<p>ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации</p>	<p><b>Практический опыт:</b> применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации</p> <p><b>Умения:</b> применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами</p> <p><b>Знания:</b> физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и</p>	<p>ДП</p>

		<p>организации ремонта технических средств защиты информации;</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</p>	
	<p>ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа</p>	<p><b>Практический опыт:</b> проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации</p> <p><b>Умения:</b> применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных</p> <p><b>Знания:</b> номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;</p> <p>структуру и условия формирования технических каналов утечки информации;</p>	ДП
	<p>ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации</p>	<p><b>Практический опыт:</b> проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;</p> <p>выявление технических каналов утечки информации</p> <p><b>Умения:</b> применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных</p> <p><b>Знания:</b> номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам</p>	ДП
	<p>ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации</p>	<p><b>Практический опыт:</b> установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты</p> <p><b>Умения:</b> применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;</p> <p>применять инженерно-технические средства физической защиты объектов информатизации</p> <p><b>Знания:</b> основные принципы действия и характеристики технических средств физической защиты;</p> <p>основные способы физической защиты объектов информатизации;</p> <p>номенклатуру применяемых средств физической защиты объектов информатизации</p>	ДП

Таблица 3 Содержательная структура КОД 09.02.07-2-25.

Показатели освоения общих (ОК) и профессиональных компетенций (ПК) на демонстрационном экзамене:

Основные виды деятельности (профессиональные модули ПМ)	Перечень оцениваемых ОК, ПК	Перечень оцениваемых умений, навыков (практического опыта)
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	<b>Практический опыт:</b> установка и настройка компонентов систем защиты информации автоматизированных (информационных) систем
	ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении	<b>Практический опыт:</b> администрирование автоматизированных систем в защищенном исполнении <b>Умения:</b> организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; осуществлять конфигурирование, настройку компонент систем защиты информации автоматизированных систем; производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы
	ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	<b>Умения:</b> настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам
	ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении	<b>Практический опыт:</b> диагностика компонентов систем защиты информации автоматизированных систем, устранение отказов и восстановление работоспособности автоматизированных (информационных) систем в защищенном исполнении <b>Умения:</b> обеспечивать работоспособность, обнаруживать и устранять неисправности
		ОК 02. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	<b>Практический опыт:</b> установка, настройка программных средств защиты информации в автоматизированной системе <b>Умения:</b> устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
	ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	<b>Практический опыт:</b> использование программных и программно-аппаратных средств для защиты информации в сети <b>Умения:</b> устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

		устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;
	ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	<b>Практический опыт:</b> тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации <b>Умения:</b> диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;
	ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	<b>Практический опыт:</b> решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных <b>Умения:</b> использовать типовые программные криптографические средства, в том числе электронную подпись

## 2. ДЕМОНСТРАЦИОННЫЙ ЭКЗАМЕН

Демонстрационный экзамен 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.

По решению Колледжа на основании заявлений выпускников проводится демонстрационный экзамен профильного уровня.

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

Демонстрационный экзамен профильного уровня проводится с использованием единых оценочных материалов, включающих в себя конкретные комплекты оценочной документации, варианты заданий и критерии оценивания, разрабатываемых оператором с участием организаций-партнеров, отраслевых и профессиональных сообществ и размещенных на официальном сайте оператора в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет") не позднее 1 октября года, предшествующего проведению ГИА (Электронный ресурс: <https://de.firpo.ru/>).

Демонстрационный экзамен профильного уровня по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем проводится с использованием комплекта оценочной документации КОД 10.02.05-1-2025

КОД 10.02.05-1-2025 рассчитан на выполнение экзаменационного задания продолжительностью 3 часа 30 минут. Продолжительность экзамена (в днях) – однодневный. Форма участия – индивидуальная.

Комплект оценочной документации 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, инструкции по технике безопасности, а также образцы заданий.

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

Демонстрационный экзамен проводится в центре проведения демонстрационного экзамена (далее - ЦПДЭ), представляющем собой площадку, оборудованную и оснащенную в

соответствии с комплектом оценочной документации (в Мастерской, оснащенной современной материально-технической базой по компетенции Корпоративная защита внутренних угроз информационной безопасности), по графику, утвержденному Министерством образования и науки РД.

## 2.1. Оценивание результатов демонстрационного экзамена

Таблица 4 – Количество постов-рабочих мест на экзаменационной площадке и количество экспертов на экзаменационной площадке

Кол-во рабочих мест в ЦПДЭ	Максимальное кол-во обучающихся-участников ДЭ (одновременно в ЦПДЭ)	Кол-во экспертов (одновременно в ЦПДЭ)
12	12	3

Процедура оценивания результатов выполнения заданий демонстрационного экзамена профильного уровня (инвариантная часть) осуществляется членами экспертной группы по 80-балльной системе в соответствии с требованиями КОД 10.02.05-1-2025.

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

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

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

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

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100%.

Требования к оцениванию представлена в таблице № 4.

Таблица № 5 Распределение баллов по критериям оценивания для демонстрационного экзамена профильного уровня (инвариантная часть КОД) в рамках ГИА

№ п/п	Модуль задания (вид профессиональной деятельности)	Критерий оценивания	Баллы
1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	<b>4,00</b>
		Использование информационных технологий в профессиональной деятельности	<b>2,00</b>
2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	Осуществление установки и настройки отдельных программных, программно-аппаратных средств защиты информации	<b>6,00</b>
		Обеспечение защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	<b>12,00</b>
		Осуществление тестирования функций отдельных программных и программно-аппаратных средств защиты информации	<b>2,00</b>
3	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	Производство установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	<b>4,00</b>
		Администрирование программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	<b>6,00</b>

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

Перевод полученного количества баллов в оценки "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", осуществляется государственной экзаменационной комиссией с обязательным участием главного эксперта.

Перевод баллов в оценку осуществляется на основе таблицы 5.

Таблица 6 – Перевод баллов в оценку

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

## 2.2. Образец задания демонстрационного экзамена профильного уровня в рамках ГИА (ГИА/ДЭ ПУ)

Продолжительность выполнения каждого модуля задания представлена в таблице:

Таблица № 7

Номер и наименование модуля задания	Продолжительность выполнения модуля задания
Модуль № 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	0 ч. 20 мин.
Модуль № 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами	1 ч. 10 мин.
Модуль № 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	1 ч.30 мин.
Модуль № 2 Защита информации в автоматизированных системах программными и программно-аппаратными средствами	0 ч. 30 мин.

Текст образца задания:

### Модуль № 1:

## **Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**

Текст задания:

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

При выполнении заданий необходимо при помощи текстового редактора, сформировать отчет, в котором представить скриншоты ключевых настроек.

В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети, задать пароли пользователей и администраторов сети.

Для правильной работы сети надо создать или убедиться в наличии 4 сетей:  
Host only или внутренняя сеть адаптер для сети центрального офиса  
Host only или внутренняя сеть адаптер для сети филиала  
Host only или внутренняя сеть адаптер для сети межсетевое взаимодействия;  
Host only адаптер, NAT или Bridge для виртуального «Интернета».

IP адреса защищенных сетей:

Центральный офис «Сеть 1 ЦО»: 172.16.224.224/27  
Офис филиал «Сеть 1 Филиал»: 10.10.20.128/25  
Офис сеть 2 «Сеть 2 Офис»: 192.168.88.64/26  
«Интернет» для всех координаторов: 10.8.248.0/24

Адреса выбираются самостоятельно из указанного диапазона.

В связи с особенностями работы системы на различных версиях пользовательских или серверных ОС, может потребоваться установка компонентов системы вручную (например, БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов.

Задача 1.1 Установить базу данных MSSQL на виртуальную машину Net1- Open (незащищенный узел).

Необходимые приложения: отсутствуют.

### **Модуль № 2:**

#### **Защита информации в автоматизированных системах программными и программно-аппаратными средствами**

Текст задания:

Задача 2.1 Развертывание ПК Administrator в качестве центра сертификации Установить и настроить рабочее место администратора (на базе виртуальной машины Net1-AdminCA (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД. Установить клиент ЦУС на VM Net1-Open (незащищенный узел).

Задача 2.2 . Инициализация VPN Coordinator и установка ПО VPN Client

На виртуальной машине Net1-AdminCA (ЦО) установить ПО Client (Пользовательская или серверная ОС), рабочее место администратора, на виртуальной машине Net1 -Coord (ЦО) инициализировать Coordinator HW-VA. Задача 2.3 . Инициализация VPN Coordinator и установка ПО VPN Client для организации сети филиала

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

Задача 2.4 Развертывание удостоверяющего центра в составе защищенной сети

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

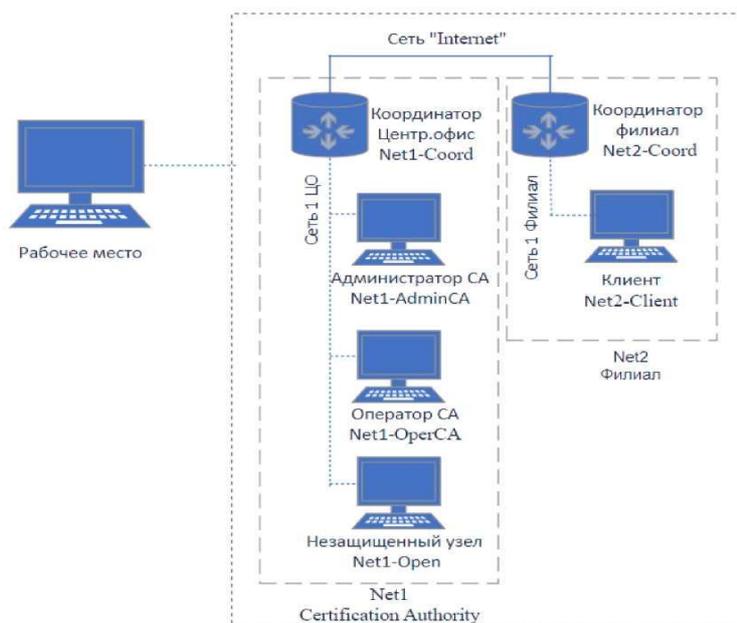


Рисунок 1 Схема защищенной сети

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

#### Задача 2.5 Создание структуры защищенной сети

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

Таблица 1 - Узлы защищенной сети

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1- AdminCA (ЦО)	Администратор ИБ	Administrator (ЦУС сервер, УКЦ), Client, CA Informing	Пользовательская или серверная ОС	AdminS
Net1- CoordCA (ЦО)	Корневой координатор	Coordinator	HW-VA	Root_Coordinator
Net1- OperCA (ЦО)	Узел ЦР	Client, Publication Service, Registration Point	Пользовательская или серверная ОС	Node_CR
Net2-Coord (Филиал)	Подчиненный координатор	Coordinator	HW-VA	Sub_Coordinator
Net2-Client (филиал)	Удаленный клиент	Client	Пользовательская или серверная ОС	Rem_Client

Таблица 2 - Схема связей пользователей

Пользователь	Root_Coordinator	AdminS	Node_CR	Sub_Coordinator	Rem_Client
Root_Coordinator	X	*	*	*	
AdminS	*	X	*		*
Node_CR	*	*	X	*	
Sub_Coordinator	*	*	*	X	*
Rem_Client		*		*	X

Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке, поменять тип паролей для пользователей («собственный»).

Сформировать дистрибутивы ключей для всех сетевых узлов. Разнести дистрибутивы ключей по АРМ, провести первичную инициализацию узлов защищенной сети, проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

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

Необходимые приложения: отсутствуют.

## **Модуль № 1:**

### **Эксплуатация автоматизированных (информационных) систем в защищенном исполнении**

Текст задания:

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

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

Задача 1.3 Настройка работы удостоверяющего центра в аккредитованном режиме

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

После перевода УКЦ в аккредитованный режим необходимо выпустить:

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

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

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

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

Задача 1.4. Компрометация пользователя

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС: скомпрометировать ключи

пользователя Rem\_Client на узле Удаленный клиент, произвести смену ключей пользователя и сетевых узлов, отправить обновления и произвести процедуру смены ключа пользователя на узле Удаленный клиент, проверить работу защищенной сети после обновления отправив

сообщение от пользователя Rem Client администратору. В отчете необходимо зафиксировать процесс настройки скриншотами.

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

Необходимые приложения: отсутствуют.

## Модуль № 2:

### Защита информации в автоматизированных системах программными и программно-аппаратными средствами

Текст задания:

Задача 2.7. Реализовать межсетевое взаимодействие защищённых сетей (со связями «все со всеми»), развернув на виртуальной машине Net3-Admin рабочее место Администратора партнёрской сети.

Схема меж сетевого взаимодействия представлена на рисунке 2.

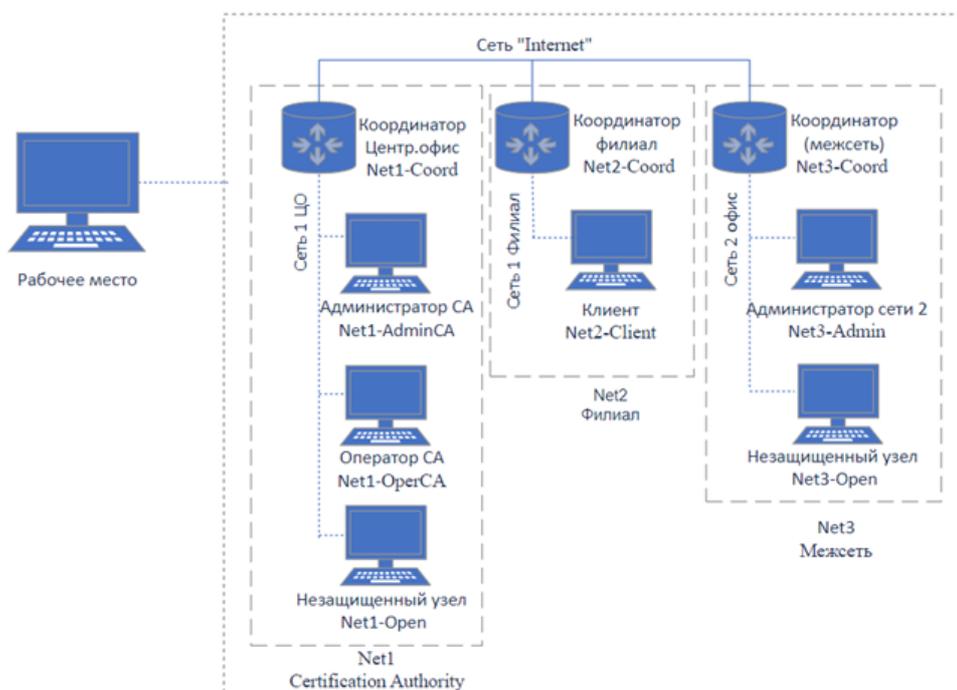


Рисунок 2 Схема межсетевого взаимодействия

Создать структуру второй сети: рабочее место администратора на виртуальной машине Net3-Admin (БД, ЦУС, УКЦ, Client), координатор (Net3-Coord-HW- VA). Установить и настроить необходимое ПО. Настроить межсетевое взаимодействие, с использованием ассиметричных межсетевых ключей, между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия. Проверить взаимодействие узлов, отправив сообщение чата и деловой почты с узла Администратор сети (Net1 - AdminCA) на Admin (Net3-Admin)

### 2.3. Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания

Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания в зависимости от вида аттестации, уровня ДЭ представлен в таблице № 10.

Перечень оборудования и оснащения, расходных материалов, средств обучения и воспитания может быть дополнен образовательной организацией с целью создания необходимых условий для участия в ДЭ обучающихся из числа лиц с ограниченными возможностями здоровья и обучающихся из числа детей-инвалидов и инвалидов.

Таблица № 8

1. Зоны площадки									
Наименование зоны площадки					Код зоны площадки				
Рабочее место участника					А				
Общая площадка					Б				
Рабочее место экспертов					В				
2. Инфраструктура рабочего места участника ДЭ									
№	Наименование	Минимальные (рамочные) технические характеристики	ОКПД-2	Расчет кол-ва (На 1 раб. место/На 1 участника)	Количество			Единица измерения	Код зоны площадки
					ПА	ГИА ДЭ БУ	ГИА ДЭ ПУ		
Перечень оборудования									
1.	Стул	На усмотрение организатора	31.01.11.15 0	На 1 раб.место	1	1	1	шт	А
2	Стол	На усмотрение организатора	31.01.12.11 0	На 1 раб.место	1	1	1	шт	А
3	Компьютер	Процессор не менее 3,2 ГГц с поддержкой виртуализации или аналог, не менее 6 физических ядер не менее 12 потоков, не менее 32 ГБ ОЗУ, не менее 500 ГБ SSD со свободным местом не менее 300 ГБ, не менее 100 ГБ свободного места на этом же или дополнительных носителях (HDD/SSD) для хранения резервных образов, в случае ноутбука необходим дополнительный монитор, ОС с графическим интерфейсом, ПО для виртуализации с поддержкой драйверов для операционных систем семейства UNIX, офисный пакет, текстовый редактор с подсветкой	26.20.15.11 0	На 1 раб.место	1	1	1	шт	А

		синтаксиса, браузер, ssh- клиент, sftp/scp-клиент, ftp- клиент, архиватор, программа просмотра pdf							
4	Монитор	Не менее 20" и разрешением не менее 1920x1080 пкс, можно устанавливать 2 шт (для удобства)	26.20.17.11 0	На 1 раб.место	1	1	1	шт	A
5	Клавиатура	Интерфейс подключения: USB	26.20.16.11 0	На 1 раб.место	1	1	1	шт	A
6	Мышь компьютерная	Интерфейс подключения: USB	26.20.16.17 0	На 1 раб.место	1	1	1	шт	A
7	Среда виртуализации	На усмотрение организатора	62.01.29.00 0	На 1 раб.место	1	1	1	шт	A
8	Виртуальная машина (сервер)	Предустановленная виртуальная машина совместимая с возможностью установки MSI пакетов, офисный пакет, текстовый редактор с подсветкой синтаксиса, браузер, ssh-клиент, sftp/scp-клиент, ftp- клиент, архиватор, программа просмотра pdf	58.29.11.00 0	На 1 раб.место	3	3	5	шт	A
9	Виртуальная машина (клиент)	Предустановленная виртуальная машина с возможностью подключения к домену или функциональный аналог с возможностью установки MSI пакетов или виртуальная машина с возможностью Установки deb-пакетов, офисный пакет, текстовый редактор с подсветкой синтаксиса, браузер, ssh- клиент, sftp/scp-клиент, ftp- клиент, архиватор, программа просмотра pdf	58.29.11.00 0	На 1 раб.место	2	3	4	шт	A
10	Программное обеспечение VPN для создания защищенных частных сетей в соответствии с рекомендациями	Программное обеспечение для создания защищенной виртуальной частной сети в составе Administrator, Coordinator (или программноаппаратный комплекс) не	62.01.29.00 0	На 1 раб.место	1	1	1	шт	A
	ФСТЭК с поддержкой программноаппаратных комплексов и шифрованием ГОСТ	менее 4 шт или аналоги, Client не менее 6 шт, лицензии на вышеуказанное ПО с возможностью установки межсетевого взаимодействия между двумя сетями, созданием туннелей, удаленного администрирования,							

		комплекс Удостоверяющий центр в составе Центр регистрации, сервис публикации, сервис информирования, поддержка шифрования ГОСТ								
<b>Перечень инструментов</b>										
1	Не требуется	-	-	-	-	-	-	-	-	-
<b>Перечень расходных материалов</b>										
1	Бумага	Белая, А4, плотность не менее 80г/м2	17.12.14.11 0	На 1 раб.место	3	3	3	лист	А	
2	Ручка канцелярская	Вид:шариковая или гелевая, цвет чернил:синий	32.99.12.11 0	На 1 раб.место	1	1	1	шт	А	
<b>Оснащение средствами, обеспечивающими охрану труда и технику безопасности</b>										
1	Не требуется	-	-	-	-	-	-	-	-	-
<b>3. Инфраструктура общего (коллективного) пользования участниками ДЭ</b>										
№	Наименование	Минимальные (рамочные) технические характеристики	ОКПД-2	Расчет кол-ва (На кол-во участников /На кол-во раб. мест/ На всю площадку)	Количество мест/ участников	Количество			Единица измерения	Код зоны площади
						ПА	ГИА ДЭ БУ	ГИА ДЭ ПУ		
<b>Перечень оборудования</b>										
1	Коммутатор	Не менее 12 Портов Gigabit Или аналог, управляемый, L2, настроены виртуальные сети до мест участников, серверной части, комнаты экспертов.	26.30.11.110	На всю площадку	-	1	1	1	шт	Б
2	Маршрутизатор или виртуальный аналог	Не менее 4 Портов Gigabit или аналог, настроены виртуальные сети (по 1 на участника, 1 на экспертов, 1 на серверную инфраструктуру) . Доступ между сетями участников запрещен, доступ с мест	26.30.11.120	На всю площадку	-	1	1	1	шт	Б

		участников к интернет/серверам и наоборот разрешен, доступ из сети								
		Экспертов к сетям участникам разрешен								
3	Точка доступа или возможность создания WiFi сетей на базе существующих в зонах проведения ДЭ с необходимыми характеристиками и подключением к локальной сети площадки	Поддержка диапазонов 2ГГц и 5ГГц, возможность подключения не менее 10 клиентов без потери пропускной способности, поддержка дополнительных виртуальных сетей	26.30.11.120	На всю площадку	-	1	1	1	шт	Б
4	Видеокамера (одна или более, при необходимости трансляции)	IP или USB, Разрешение не менее 1280x720 пкс, сжатие MP4, поддержка потока RTSP по ссылке, широкоугольный объектив, охват всей площадки	26.40.33.110	На всю площадку	-	1	1	1	шт	Б
5	Устройство для вещания трансляции в интернет(при необходимости)	Компьютер/ноутбук/прочее с возможностью передачи потока	26.20.15.110	На всю площадку	-	1	1	1	шт	Б
	трансляции) с предустановленным ПО	не менее 1280x720 25 к/с с возможностью аппаратного сжатия H264 сжатия и трансляции в реальном времени необходимого количества камер, программное обеспечение для обеспечения трансляции на необходимую площадку трансляций								

6	Устройство для вывода таймера	ТВ- панель/проектор /монитор не менее24", HDMI/VGA/Про чее, должен быть виден всем участникам	26.20.17.110	На всю площадку	-	1	1	1	шт	Б
7	Блок розеток	Тип: сетевой фильтр	27.33.13.190	На всю площадку	-	1	1	1	шт	Б
<b>Перечень инструментов</b>										
1.	Не требуется	-	-	-	-	-	-	-	-	-
<b>Перечень расходных материалов</b>										
1.	Не требуется	-	-	-	-	-	-	-	-	-
<b>Оснащение средствами, обеспечивающими охрану труда и технику безопасности</b>										
1.	Аптечка	Аптечка для оказания первой помощи работникам. Приказ Министерства здравоохранения Российской Федерации от 24 мая 2024 г. № 262Н «Об утверждении требований к комплектации медицинскими изделиями аптечки для оказания первой помощи работникам»	21.20.24.1 70	На всю площадку	-	1	1	1	шт	Б
2	Огнетушитель	Требования не менее, чем по приказу Федерального агентства по техническому регулированию и метрологии от 24 августа 2021 г. № 794-ст, в части ГОСТ Р 51057 Техника пожарная.	28.29.22.1 10	На всю площадку	-	1	1	1	шт	Б

		Огнетушители переносные. Общие технические требования								
3	Мусорная корзина	На усмотрение организатора	22.22.13.1 90	На всю площадь	-	1	1	1	шт	Б
<b>4. Инфраструктура рабочего места главного эксперта ДЭ</b>										
№	Наименование	Минимальные (рамочные) технические характеристики	ОКПД-2	Количество			Единица измерения	Код зоны площади		
				ПА	ГИА ДЭ БУ	ГИА ДЭ ПУ				
<b>Перечень оборудования</b>										
1.	Компьютер или сервер виртуализации для центральной инфраструктуры или необходимое количество ресурсов на сервере	Процессор не менее 3,2 ГГц с поддержкой виртуализации или аналог, не менее 6 физических ядер не менее 12 потоков, не менее 32 ГБ ОЗУ, не менее 500 ГБ SSD со свободным местом не менее 300 ГБ, не менее 2 сетевых интерфейса Gigabit или аналог, гипервизор, возможность импорта OVA/OVF пакетов	26.20.15.110	1	1	1	шт	В		
2	МФУ	МФУ формат А4 черно белый, возможность потокового цветного сканирования, картридж с расчетом на все потоки экзамена	26.20.18.110	1	1	1	шт	В		
3	Монитор	Не менее 20" и разрешением не менее 1920x1080 пкс, можно устанавливать 2 шт (для удобства)	26.20.17.110	1	1	1	шт	В		
4	Клавиатура	Интерфейс подключения: USB	26.20.16.110	1	1	1	шт	В		
5	Мышь компьютерная	Интерфейс подключения: USB	26.20.16.170	1	1	1	шт	В		
6	Стол	На усмотрение организаторов	31.01.12.110	1	1	1	шт	В		
7	Стул	На усмотрение организаторов	31.01.11.150	1	1	1	шт	В		
8	Блок розеток	Тип:сетевой фильтр, Количество розеток, штука:>2	27.33.13.190	1	1	1	шт	В		
<b>Перечень инструментов</b>										
1.	Степлер для бумаг	15 листов	25.99.22.130	1	1	1	шт	В		
<b>Перечень расходных материалов</b>										
1.	Картридж для МФУ	Картридж или дозаправка картриджа для МФУ из основного ИЛ, на усмотрение организатора	28.23.25.000	1	1	1	шт	В		

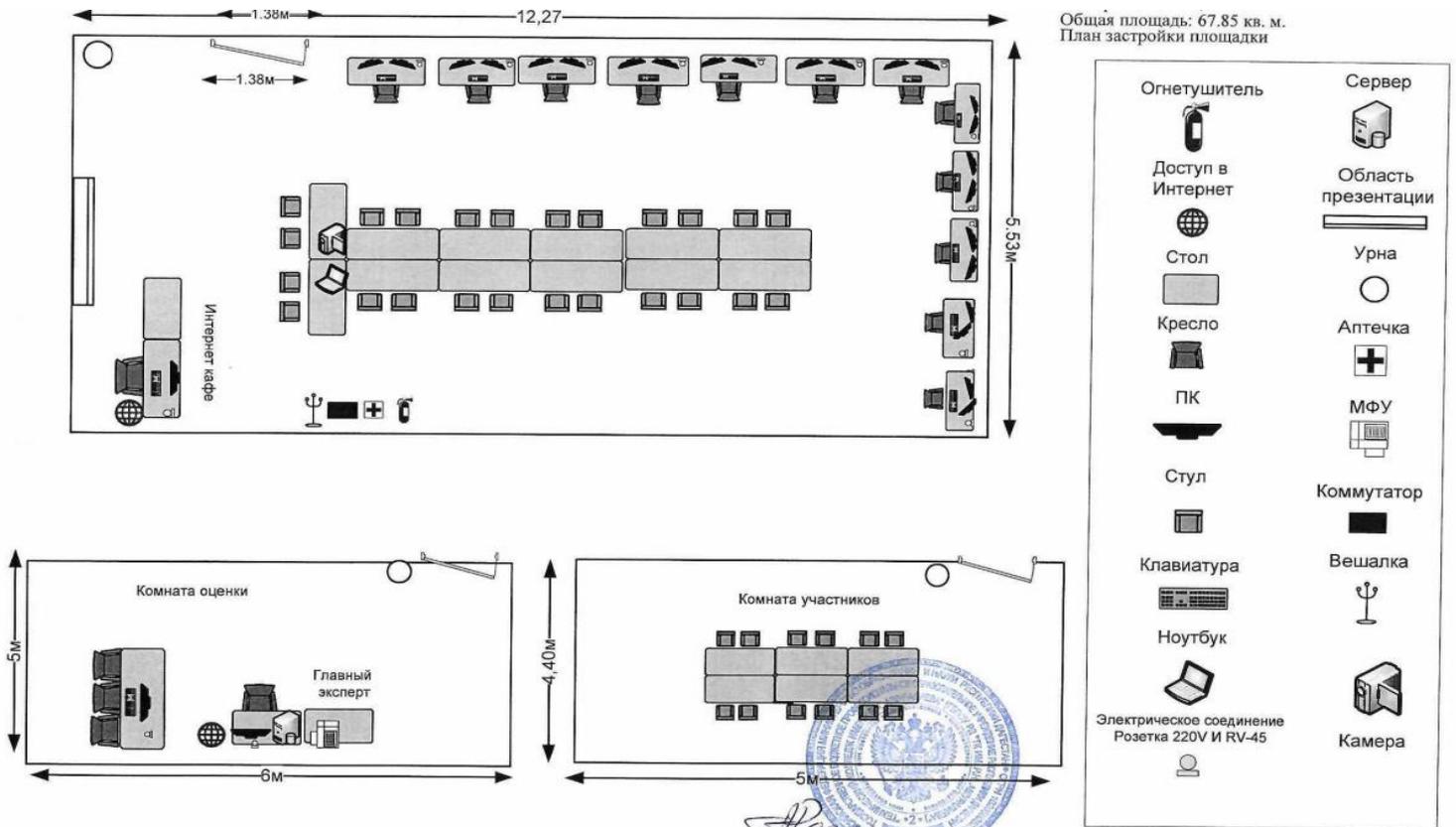
2	Ручка канцелярская	Вид:шариковая или гелевая, цвет чер- нил:синий	32.99.12.110	1	1	1	шт	В		
3	Файл-вкладыш	Формат:А4, количество файлов в упа- ковке (шт):100	22.29.25.000	1	1	1	упак	В		
4	Скобы для степлера	Совместимость со степлером	25.99.23.000	1	1	1	упак	В		
5	Бумага	А4, плотность не менее 80г/м2, ко- личество листов в пачке>=500	17.12.14.110	1	1	1	пачка	В		
6	Папка- скоросшиватель	Тип: папка-регистратор, меха- низм:арочный, формат:А4	17.23.13.193	1	1	1	шт	В		
<b>Оснащение средствами, обеспечивающими охрану труда и технику безопасности</b>										
1.	Мусорная корзина	На усмотрение организатора	22.22.13.190	1	1	1	шт	В		
<b>5. Инфраструктура рабочего места членов экспертной группы</b>										
№	Наименование	Минимальные (ра- мочные) технические характеристики	ОКПД-2	Расчет кол-ва (На 1 эксперта/ На кол-во экс- пертов/ На всех экспертов)	Количество экс- пертов	Количество			Единица из- мерен ия	Код зоны площа дки
						ПА	ГИА ДЭ БУ	ГИА ДЭ ПУ		
<b>Перечень оборудования</b>										
1.	Стол	На усмотрение орга- низаторов	31.01.12.110	На 1 эксперта	-	1	1	1	шт	В
2	Стул	На усмотрение орга- низаторов	31.01.11.150	На 1 эксперта	-	1	1	1	шт	В
<b>Перечень инструментов</b>										
1	Не требуется	-	-	-	-	-	-	-	-	-
<b>Перечень расходных материалов</b>										
1.	Бумага	А4, плотность не менее 80г/м2, ко- личество листов в пачке>=500	17.12.14.110	На 1 эксперта	-	1	1	1	пачка	В
2	Ручка канцелярская	Вид:шариковая или гелевая, цвет чер- нил:синий	32.99.12.110	На 1 эксперта	-	1	1	1	шт	В
<b>Оснащение средствами, обеспечивающими охрану труда и технику безопасности</b>										
1	Не требуется	-	-	-	-	-	-	-	-	-

## 2.4. План застройки площадки ЦПДЭ

### Код зоны площадки А

Общая площадь площадки: 67,85 м<sup>2</sup>

План застройки площадки для проведения демонстрационного экзамена



**2.5. Примерный план проведения демонстрационного экзамена в рамках государственной итоговой аттестации выпускников по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

**ПЛАН ПРОВЕДЕНИЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА  
в рамках государственной итоговой аттестации выпускников  
по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем**

<b>Наименование организации, на базе которой организован ЦПДЭ</b>	Государственное бюджетное профессиональное образовательное учреждение Республики Дагестан «Технический колледж имени Р.Н. Ашуралиева»
<b>Адрес ЦПДЭ</b>	Республика Дагестан, г. Махачкала, переулок Студенческий, д. 3.
<b>Код и наименование специальности среднего профессионального образования</b>	10.02.05 Обеспечение информационной безопасности автоматизированных систем
<b>Наименование квалификации</b>	Техник по защите информации
<b>Вид аттестации</b>	Государственная итоговая аттестация
<b>Уровень демонстрационного экзамена</b>	Профильный
<b>Шифр комплекта оценочной документации</b>	КОД 10.02.05-1-2025

**Место расположения ЦПДЭ:** г. Махачкала, переулок Студенческий 3, ГБПОУ РД «Технический колледж имени Р.Н. Ашуралиева», учебный корпус 2, Мастерская, оснащенная современной материально-технической базой по компетенции Корпоративная защита внутренних угроз информационной безопасности.

**Дата и время начала проведения демонстрационного экзамена: 26.05.2025, 09.00.00**

**Расписание сдачи демонстрационного экзамена в составе экзаменационных групп:**

<b>Экзаменационная группа</b>	<b>Подготовительный день</b>		<b>День 1</b>	
	<b>дата</b>	<b>время</b>	<b>дата</b>	<b>время</b>
1	26.05.2025	09:00:00	27.05.2025	08:30:00
2			28.06.2025	08:30:00
3			29.06.2025	08:30:00
4			30.06.2025	08:30:00
5			31.06.2025	08:30:00

**Планируемая продолжительность проведения демонстрационного экзамена** для каждой экзаменационной группы – 3 часа 30 минут часа.

**Технические перерывы в проведении демонстрационного экзамена** для каждой экзаменационной группы организованы на 15 минут через каждый час работы:

**10:10:00- 10:25:00**

**11:25:00-11:40:00**

**12:40:00-12:55:00**

Во время регламентированного перерыва с целью снижения нервно-эмоционального напряжения, утомления зрительного аппарата, необходимо выполнять комплексы физических упражнений.

Главный эксперт сообщает о течении времени выполнения задания ДЭ каждые 60 минут и за 30 и 5 минут до окончания времени выполнения задания

<b>План проведения демонстрационного экзамена для экзаменационных групп 1,2</b>		
<b>День экзамена</b>	<b>Время</b>	<b>Описание мероприятия</b>
<b>Дата: 26.05.2025</b>		
Подготовительный день	09:00:00-10:00:00	Проверка готовности ЦПДЭ главным экспертом в присутствии членов экспертной группы, участников ДЭ, а также технического эксперта. Заполнение и подпись Акта результатов проверки готовности ЦПДЭ.
	10:00:00-10:30:00	Загрузка главным экспертом копии Акта, паспорта ЦПДЭ, сведений о материально-техническом оснащении ЦПДЭ и сведений об обеспеченности ЦПДЭ расходными материалами в ИСО.
	10:30:00-11:00:00	Осмотр ЦПДЭ главным экспертом
	11:00:00-11:20:00	Регистрация присутствующих. Ознакомление их с планом проведения экзамена. Сверка состава экспертной группы в соответствии с подтвержденными в ИСО данными на основании документов, удостоверяющих личность
	11:20:00-11:40:00	Проведение техническим экспертом инструктажа об ознакомлении с требованиями охраны труда и безопасности производства в соответствии с типовой инструкцией по охране труда и безопасности производства. Оформление протокола. Знакомство экзаменуемых с условиями оказания первичной медицинской помощи в ЦПДЭ
	11:40:00-11:50:00	Распределение рабочих мест между экзаменуемыми с использованием способа случайной выборки. Оформление протокола распределения рабочих мест
	11:50:00-12:20:00	Знакомство экзаменуемых со своими рабочими местами
	12:20:00-12:30:00	Распределение обязанностей между членами экспертной группы по оценке выполнения заданий ДЭ. Оформление протокола распределения обязанностей между членами экспертной группы ДЭ
<b>Дата:</b>		
<ul style="list-style-type: none"> <li>– экзаменационная группа 1: 27.05.2025</li> <li>– экзаменационная группа 2: 28.05.2025</li> <li>– экзаменационная группа 3: 29.05.2025</li> <li>– экзаменационная группа 4: 30.05.2025</li> <li>– экзаменационная группа 5: 31.05.2025</li> </ul>		
День проведения экзамена	08:30:00-08:40:00	Допуск участников в ЦПДЭ главным экспертом на основании документов, удостоверяющих личность. Фиксация главным экспертом явки экзаменуемого, его рабочее место, в протоколе проведения ДЭ.
	08:40:00-08:50:00	Разъяснение главным экспертом перед началом экзамена участникам запрет на наличие материалов, инструментов или оборудования, запрещенных в соответствии с требованиями КОД и Порядка.
	08:50:00-09:10:00	Разъяснение главным экспертом правил поведения во время ДЭ Выдача главным экспертом экзаменационных заданий каждому участнику. Ознакомление участников с заданием ДЭ, обобщенной оценочной ведомостью (если применимо), дополнительными инструкциями к ним (при наличии) Оформление протокола ознакомления участников ДЭ с оценочными материалами и заданием
	09:10:00	Объявление главным экспертом о начале ДЭ. Фиксация времени начала ДЭ в протоколе проведения ДЭ
	09:10:00 - 10:10:00	Выполнение задания демонстрационного экзамена
	09:40:00, 10:05:00	Сообщение главным экспертом о течении времени выполнения задания ДЭ
	10:10:00- 10:25:00	Технический перерыв и проведение профилактических мероприятий
	10:25:00- 11:25:00	Выполнение задания демонстрационного экзамена
	11:25:00	Сообщение главным экспертом о течении времени выполнения задания ДЭ
	11:25:00-11:40:00	Технический перерыв и проведение профилактических мероприятий
	11:40:00-12:40:00	Выполнение задания демонстрационного экзамена

12:10:00	Сообщение главным экспертом о течении времени выполнения задания ДЭ
12:35:00	ДЭ
12:40:00-12:55:00	Технический перерыв и проведение профилактических мероприятий
12:55:00-13:25:00	Выполнение задания демонстрационного экзамена
13:25:00	Окончание ДЭ. Фиксация главным экспертом времени завершения выполнения задания ДЭ в протоколе проведения ДЭ
13:30:00-15:30:00	Оценивание результатов выполнения заданий ДЭ членами экспертной группы по 100-балльной системе в соответствии с требованиями КОД, с использованием предусмотренных в ИСО форм и оценочных ведомостей.
15:30:00-16:00:00	Перенос главным экспертом или техническим экспертом результатов выполнения заданий ДЭ из заполненных оценочных ведомостей в ИСО
16:00:00	Блокировка баллов в ИСО
16:00:00-16:30:00	Сверка главным экспертом и членами экспертной группы баллов, занесенных в ИСО, с формами оценивания, заполненными экспертами
	Направление главным экспертом запроса ответственным сотрудникам Оператора по работе с ИСО для разблокировки ИСО в соответствующем диапазоне в случае выявления в процессе сверки несоответствия внесенных в ИСО данных и форм внесения оценок
	Внесение необходимых корректировок
	Блокировка баллов в ИСО
16:30:00-16:40:00	Оформление протокола учета времени, технических остановок времени и нестандартных ситуаций, который подписывается главным экспертом и всеми экспертами, проводившими оценку
16:40:00-16:45:00	Выставление баллов в протоколе проведения ДЭ в присутствии члена ГЭК, не входящего в экспертную группу
16:45:00	Передача подписанного членами экспертной группы и утвержденного главным экспертом протокола проведения ДЭ в ГЭК для выставления оценок по итогам ГИА с учетом требований КОД
16:45:00	Передача оригинала протокола проведения ДЭ на хранение в образовательную организацию в составе архивных документов

### 3. ДИПЛОМНЫЙ ПРОЕКТ

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

Дипломный проект выполняется выпускником в соответствии с выбранной темой и требованиями, установленными Программой ГИА по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Тема дипломного проекта должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем:

- 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.

Темы дипломных проектов должны отражать современный уровень развития технических и программно-аппаратных средств защиты информации, иметь практико-ориентированный характер.

Дипломный проект может быть логическим продолжением курсовой работы, идеи и выводы которой реализуются на более высоком теоретическом и практическом уровне.

Дипломный проект представляет собой решение конкретной практической задачи (опытно-конструкторской, проектной, технологической), направленной на обеспечение информационной безопасности выбранного объекта. В качестве объекта защиты могут быть выбраны:

- компьютерная система;
- составная часть компьютерной системы;
- бизнес-процесс;
- предприятие, помещение или отдел организации;
- конфиденциальный документооборот;
- интеллектуальная собственность и пр.

Результатом дипломного проекта является разработанная и обоснованная выпускником система мер, обеспечивающая организацию и технологию защиты информации конкретного объекта, на основе использования различных защитных средств:

- организационно-правовых;
- инженерно-технических;
- программно-аппаратных.

### 3.1. Методика оценивания дипломных проектов

#### Процедура оценивания результатов освоения образовательной программы на защите дипломного проекта

Процедура оценивания результатов освоения образовательной программы включает в себя оценку уровня сформированности общих и профессиональных компетенций в процессе подготовки и защиты дипломного проекта.

Уровень сформированности общих и профессиональных компетенций в процессе подготовки и защиты дипломного проекта оценивается по результатам отзывов руководителя проекта, а также во время анализа членами ГЭК содержания, оформления, презентации дипломного проекта, умения выпускника участвовать в научной дискуссии.

Результаты проведения защиты дипломного проекта оцениваются с проставлением одной из отметок: "отлично", "хорошо", "удовлетворительно", "неудовлетворительно" - и объявляются в тот же день после оформления протоколов заседаний ГЭК.

Основные требования к содержанию оформлению и защите дипломных проектов выпускников:

Уровень проработки проблемы	
1.	Соответствие проекта содержания заявленной теме, заданию на проектирование (исследование)
2.	Раскрыта актуальность выбранной темы, взаимосвязь с современными тенденциями развития отрасли. Правильно определены объект, предмет, гипотеза исследования. Выделена проблема исследования и четко определены цель и задачи проекта
3.	Глубокая теоретическая проработка исследуемых вопросов на основе анализа используемых источников; критический подход к изучаемым фактическим материалам с целью поиска резервов повышения информационной безопасности
4.	Умелая систематизация данных в виде таблиц, графиков, схем с необходимым анализом, обобщением и выявлением угроз информационной безопасности. Даны практические рекомендации по повышению эффективности информационной безопасности.
5.	Адекватность применения современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности

6.	Логичное, последовательное изложение материала, взаимосвязь теоретической части работы с практической, обоснованность использования источников и этика цитирования.
7.	Самостоятельность выполнения проекта, творческий подход к изложению материала, обоснованность предложений и рекомендаций
8.	Выпускник при выполнении и защите дипломного проекта демонстрирует высокий уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности
Оформление работы	
9.	Правильность, четкость структуры проекта
10.	Соответствие оформления требованиям стандартов
Иллюстративность, качество презентации результатов работ	
11.	Доклад сопровождается мультимедиа презентацией. В презентации отражаются основные этапы и результаты проекта Качество иллюстративного материала, представленного в презентации к докладу: соответствие подбора иллюстративных материалов содержанию доклада, грамотность их оформления и упоминание в докладе, выразительность использованных средств
Навыки публичной дискуссии	
12.	Выпускник исчерпывающе, последовательно, грамотно и логически стройно излагает суть и решение проблемы, прослеживается умение делать выводы, обобщать знания и практический опыт. Выпускник показывает глубокие знания вопросов темы дипломного проекта, свободно оперирует профессиональной терминологией, материалами предметной области и средствами реализации; вносит обоснованные предложения по обеспечению информационной безопасности, эффективному использованию современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности хороший язык и стиль изложения
13.	Выпускник аргументировано, легко и технически грамотно отвечает на вопросы членов ГЭК, формулирует правильные, лаконичные и обоснованные ответы на поставленные вопросы с использованием профессиональной терминологии, имеет навыки публичной дискуссии
14.	Выдержан установленный регламент времени публичного выступления
Положительный отзыв руководителя проекта	
15.	Проект имеет положительный отзыв руководителя проекта

### **Критерии оценки содержания оформления и защиты дипломного проекта:**

Дипломный проект заслуживает оценки «**Отлично**»/компетенции сформированы на высоком уровне, если:

#### **Уровень проработки проблемы**

1. Содержание проекта соответствует заявленной теме, заданию на проектирование (исследование)
2. Раскрыта актуальность выбранной темы, взаимосвязь с современными тенденциями развития отрасли. Правильно определены объект, предмет, гипотеза исследования. Выделена проблема исследования и четко определены цель и задачи проекта.
3. Исследуемые вопросы глубоко проработаны на основе анализа используемых источников; сделан критический подход к изучаемым фактическим материалам с целью поиска резервов повышения информационной безопасности.
4. Выполнена умелая систематизация данных в виде таблиц, графиков, схем с необходимым анализом, обобщением и выявлением угроз информационной безопасности. Даны практические рекомендации по повышению эффективности информационной безопасности.

5. Обоснована необходимость применения современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности.
6. Изложение материала логичное, последовательное, прослеживается взаимосвязь теоретической части работы с практической. обоснованно использование источников.
7. Проект выполнен самостоятельно, выпускник творчески подошел к изложению материала, предложения и рекомендации обоснованны
8. Выпускник при выполнении и защите дипломного проекта демонстрирует высокий уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.

#### **Оформление работы**

9. Структура работы четкая, правильная.
10. Оформление соответствует требованиям стандартов.

#### **Иллюстративность, качество презентации результатов работ**

11. Выпускник сопровождает доклад мультимедиа презентацией. В презентации отражаются основные этапы и результаты проекта.  
Иллюстративные материалы соответствуют содержанию доклада, грамотно оформлены.

#### **Навыки публичной дискуссии**

12. Выпускник исчерпывающе, последовательно, грамотно и логически стройно излагает суть и решение проблемы, прослеживается умение делать выводы, обобщать знания и практический опыт;  
выпускник показывает глубокие знания вопросов темы дипломного проекта, свободно оперирует профессиональной терминологией, материалами предметной области и средствами реализации; вносит обоснованные предложения по обеспечению информационной безопасности, эффективному использованию современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности;  
хороший язык и стиль изложения
13. Выпускник аргументировано, легко и технически грамотно отвечает на вопросы членов ГЭК, формулирует правильные, лаконичные и обоснованные ответы на поставленные вопросы с использованием профессиональной терминологии, имеет навыки публичной дискуссии
14. Выдержан установленный регламент времени публичного выступления

#### **Положительный отзыв руководителя проекта**

15. Проект имеет положительный отзыв руководителя проекта

Дипломный проект заслуживает оценки «Хорошо»/компетенции сформированы на продвинутом уровне, если:

#### **Уровень проработки проблемы**

1. Содержание проекта в целом соответствует заявленной теме, заданию на проектирование (исследование). В проекте нет существенных ошибок.
2. В основном раскрыта актуальность выбранной темы, взаимосвязь с современными тенденциями развития отрасли. Определены объект, предмет, гипотеза исследования. Выделена проблема исследования и определены цель и задачи проекта.
3. Исследуемые вопросы проработаны на основе анализа используемых источников; сделан критический подход к изучаемым фактическим материалам с целью поиска резервов повышения информационной безопасности. Библиография в целом соответствует теме проекта.
4. Выполнена систематизация данных в виде таблиц, графиков, схем с необходимым анализом, обобщением и выявлением угроз информационной безопасности. Даны

практические рекомендации по повышению эффективности информационной безопасности.

5. В целом обоснована необходимость применения современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности.
6. Изложение материала логичное, последовательное, прослеживается взаимосвязь теоретической части работы с практической, обоснованно использование источников.
7. Проект выполнен самостоятельно, предложения и рекомендации обоснованны.
8. Выпускник при выполнении и защите дипломного проекта демонстрирует хороший уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.

#### **Оформление работы**

9. Структура проекта правильная
10. Оформление проекта в основном соответствует требованиям, но есть некоторые недочеты: работа недостаточно аккуратно оформлена, текст работы частично не соответствует нормам русского языка, недочеты в оформлении ссылок.

#### **Иллюстративность, качество презентации результатов работ**

11. Выпускник сопровождает доклад мультимедиа презентацией. Имеются замечания к оформлению презентации при защите. Иллюстрируемого материала недостаточно.

#### **Навыки публичной дискуссии**

12. Выпускник достаточно уверенно владеет содержанием работы, оперирует профессиональной терминологией, материалами предметной области и средствами реализации, но не всегда обоснованно и конкретно выражает свое мнение по поводу основных аспектов содержания проекта;
13. Выпускник дал ответы на большинство заданных вопросов.
14. Выдержан установленный регламент времени публичного выступления

#### **Положительный отзыв руководителя проекта**

15. Проект имеет положительный отзыв руководителя проекта, но содержащий некоторые рекомендации и несущественные замечания

Возможно наличие 2-3 незначительных недочетов, однако характер недочетов не должен иметь принципиальный характер

Дипломный проект заслуживает оценки «Удовлетворительно»/компетенции сформированы на базовом уровне, если:

#### **Уровень проработки проблемы**

1. Имеет место определенное несоответствие содержания работы заявленной теме.
2. Недостаточно обоснована актуальность темы. Имеются неточности в формулировках научного аппарата исследования. Не четко сформулированы предмет, объект исследования, цель, задачи, методы, используемые в работе.
3. В проекте недостаточно использована необходимая для раскрытия темы библиография. Проект отличается поверхностным анализом и недостаточно критическим разбором с целью поиска резервов повышения информационной безопасности. Теоретический анализ носит описательный характер, нет выводов.
4. Имеются замечания по содержанию и по глубине проведенного исследования, не обоснованы предложения по повышению эффективности информационной безопасности.
5. Недостаточно обоснована необходимость применения современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности.

6. Нарушена логика изложения материала. Некоторые части работы не связаны с целью и задачами работы, задачи раскрыты не полностью. Имеются замечания по соответствию содержания теоретической и практической частей проекта. Необоснованно использованы источники. Выбранные методы и технологии просты. Проект выполнен не в полном объеме, содержит незначительные ошибки.
7. Исследуемая проблема в основном раскрыта, но не отличается новизной, теоретической глубиной и аргументированностью. Отсутствует оригинальность в ее изложении материала и результатов, предложения, выводы расплывчаты, требуют уточняющих вопросов.
8. Выпускник при выполнении и защите дипломного проекта демонстрирует удовлетворительный уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.

#### **Оформление работы**

9. Имеются замечания к структуре проекта.
10. В оформлении проекта присутствуют ошибки (работа оформлена неаккуратно, содержит опечатки и другие технические и технологические погрешности).

#### **Иллюстративность, качество презентации результатов работ**

11. Имеются замечания к оформлению презентации при защите и к выступлению выпускника в ходе защиты.

#### **Навыки публичной дискуссии**

12. Доклад на тему представленного к защите дипломного проекта, содержит неточности в формулировке понятий, терминов. Изложение материала недостаточно связано и последовательно.
13. Выпускник испытывает затруднения в ответах на вопросы членов комиссии, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы.
14. Выдержан установленный регламент времени публичного выступления

#### **Положительный отзыв руководителя проекта**

15. В отзыве руководителя имеются рекомендации и замечания по содержанию, методике анализа и оформлению проекта.

Дипломный проект заслуживает оценки «**Неудовлетворительно**»/компетенции не сформированы, если:

#### **Уровень проработки проблемы**

1. Имеется определенное несоответствие содержания работы заявленной теме. Проект содержит существенные ошибки.
2. Не раскрыта актуальность выбранной темы. Допущены ошибки в формулировках научного аппарата исследования.
3. В проекте недостаточно использована необходимая для раскрытия темы библиография. Проект содержит существенные теоретико-методологические ошибки. Отсутствует тщательный анализ, критический разбор изучаемых фактических материалов.
4. Проект содержит слабую теоретическую базу, не содержит обоснованных расчетов. Аргументация основных положений проведенного исследования поверхностна, отсутствует анализ и обобщение результатов проекта, отсутствуют предложения по повышению эффективности информационной безопасности.
5. Полученные данные недостаточно обоснованы (слабо аргументированы, достоверность вызывает сомнения).
6. Работа изложена неубедительно, непоследовательно, нелогично. Не выдержана структурно-содержательная целостность работы. Выводы в целом не обоснованы, не соответствуют целями задачам. Выбранные методы и технологии просты.
7. Цели и задачи проекта не реализованы. Отсутствует новизна, оригинальность изложения материала и результатов.

8. Выпускник при выполнении и защите дипломного проекта демонстрирует неудовлетворительный уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.

#### **Оформление работы**

9. Не выдержана структура проекта.
10. Оформление не соответствует требованиям стандартов, низкая культура ссылок. не выполнены технические требования к оформлению печатного текста

#### **Иллюстративность, качество презентации результатов работ**

11. Имеются существенные замечания к содержанию и оформлению презентации и выступлению или презентация отсутствует.

#### **Навыки публичной дискуссии**

12. При защите выпускник не владеет материалом представленного к защите дипломного проекта, доклад на тему проекта содержит ошибки в формулировке понятий, терминов. Выпускник неуверенно излагает материал, работа доложена неубедительно. Выпускник с большими затруднениями демонстрирует работу приложения.
13. Выпускник затрудняется отвечать на поставленные вопросы, при ответе допускает существенные ошибки или не отвечает на вопросы членов ГЭК. Ответы на поставленные вопросы неубедительны
14. Не выдержан установленный регламент времени публичного выступления

#### **Положительный отзыв руководителя проекта**

15. В отзыве руководителя имеются существенные критические замечания по содержанию и оформлению проекта

## Критерии оценки содержания оформления и защиты дипломного проекта

	<b>Отлично</b> »/компетенции сформированы на высоком уровне	<b>«Хорошо»</b> /компетенции сформированы на продвинутом уровне (Возможно наличие 2-3 незначительных недочетов, однако характер недочетов не должен иметь принципиальный характер)	<b>«Удовлетворительно»</b> /компетенции сформированы на базовом уровне	<b>«Неудовлетворительно»</b> /компетенции не сформированы
<b>Уровень проработки проблемы</b>	Содержание проекта соответствует заявленной теме, заданию на проектирование (исследование)	Содержание проекта в целом соответствует заявленной теме, заданию на проектирование (исследование). В проекте нет существенных ошибок.	Имеет место определенное несоответствие содержания работы заявленной теме.	Имеется определенное несоответствие содержания работы заявленной теме. Проект содержит существенные ошибки.
	Раскрыта актуальность выбранной темы, взаимосвязь с современными тенденциями развития отрасли. Правильно определены объект, предмет, гипотеза исследования. Выделена проблема исследования и четко определены цель и задачи проекта.	В основном раскрыта актуальность выбранной темы, взаимосвязь с современными тенденциями развития отрасли. Определены объект, предмет, гипотеза исследования. Выделена проблема исследования и определены цель и задачи проекта.	Недостаточно обоснована актуальность темы. Имеются неточности в формулировках научного аппарата исследования. Не четко сформулированы предмет, объект исследования, цель, задачи, методы, используемые в работе.	Не раскрыта актуальность выбранной темы. Допущены ошибки в формулировках научного аппарата исследования.
	Исследуемые вопросы глубоко проработаны на основе анализа используемых источников; сделан критический подход к изучаемым фактическим материалам с целью поиска резервов повышения информационной безопасности.	Исследуемые вопросы проработаны на основе анализа используемых источников; сделан критический подход к изучаемым фактическим материалам с целью поиска резервов повышения информационной безопасности. Библиография в целом соответствует теме проекта.	В проекте недостаточно использована необходимая для раскрытия темы библиография. Проект отличается поверхностным анализом и недостаточно критическим разбором с целью поиска резервов повышения информационной безопасности. Теоретический анализ носит описательный характер, нет выводов.	В проекте недостаточно использована необходимая для раскрытия темы библиография. Проект содержит существенные теоретико-методологические ошибки. Отсутствует тщательный анализ, критический разбор изучаемых фактических материалов.
	Выполнена умелая систематизация данных в виде таблиц, графиков, схем с необходимым анализом, обобщением и выявлением угроз информационной безопасности. Даны практические рекомендации по повышению эффективности информационной безопасности.	Выполнена систематизация данных в виде таблиц, графиков, схем с необходимым анализом, обобщением и выявлением угроз информационной безопасности. Даны практические рекомендации по повышению эффективности информационной безопасности.	Имеются замечания по содержанию и по глубине проведенного исследования, не обоснованы предложения по повышению эффективности информационной безопасности.	Проект содержит слабую теоретическую базу, не содержит обоснованных расчетов. Аргументация основных положений проведенного исследования поверхностна, отсутствует анализ и обобщение результатов проекта, отсутствуют предложения по повышению эффективности информационной безопасности.
	Обоснована необходимость применения современных аппаратных и программно-аппаратных средств	В целом обоснована необходимость применения современных аппаратных и программно-аппаратных	Недостаточно обоснована необходимость применения современных аппаратных и программно-аппаратных	Полученные данные недостаточно обоснованы (слабо

	обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности.	средств обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности.	средств обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности.	аргументированы, достоверность вызывает сомнения).
	Изложение материала логичное, последовательное, прослеживается взаимосвязь теоретической части работы с практической. обоснованно использование источников.	Изложение материала логичное, последовательное, прослеживается взаимосвязь теоретической части работы с практической, обоснованно использование источников.	Нарушена логика изложения материала. Некоторые части работы не связаны с целью и задачами работы, задачи раскрыты не полностью. Имеются замечания по соответствию содержания теоретической и практической частей проекта. Необоснованно использованы источники. Выбранные методы и технологии просты. Проект выполнен не в полном объеме, содержит незначительные ошибки.	Работа изложена неубедительно, непоследовательно, нелогично. Не выдержана структурно-содержательная целостность работы. Выводы в целом не обоснованы, не соответствуют целями задачам. Выбранные методы и технологии просты.
	Проект выполнен самостоятельно, выпускник творчески подошел к изложению материала, предложения и рекомендации обоснованны	Проект выполнен самостоятельно, предложения и рекомендации обоснованны.	Исследуемая проблема в основном раскрыта, но не отличается новизной, теоретической глубиной и аргументированностью. Отсутствует оригинальность в ее изложении материала и результатов, предложения, выводы расплывчаты, требуют уточняющих вопросов.	Цели и задачи проекта не реализованы. Отсутствует новизна, оригинальность изложения материала и результатов.
	Выпускник при выполнении и защите дипломного проекта демонстрирует высокий уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.	Выпускник при выполнении и защите дипломного проекта демонстрирует хороший уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.	Выпускник при выполнении и защите дипломного проекта демонстрирует удовлетворительный уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.	Выпускник при выполнении и защите дипломного проекта демонстрирует неудовлетворительный уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности.
<b>Оформление работы</b>	Структура работы четкая, правильная.	Структура проекта правильная	Имеются замечания к структуре проекта.	Не выдержана структура проекта.
	Оформление соответствует требованиям стандартов	Оформление проекта в основном соответствует требованиям, но есть некоторые недочеты: работа недостаточно аккуратно оформлена, текст работы частично не соответствует нормам русского языка, недочеты в оформлении ссылок.	В оформлении проекта присутствуют ошибки (работа оформлена неаккуратно, содержит опечатки и другие технические и технологические погрешности)	Оформление не соответствует требованиям стандартов, низкая культура ссылок. не выполнены технические требования к оформлению печатного текста

<b>Иллюстративность, качество презентации результатов работ</b>	Выпускник сопровождает доклад мультимедиа презентацией. В презентации отражаются основные этапы и результаты проекта. Иллюстративные материалы соответствуют содержанию доклада, грамотно оформлены.	Выпускник сопровождает доклад мультимедиа презентацией. Имеются замечания к оформлению презентации при защите. Иллюстрируемого материала недостаточно.	Имеются замечания к оформлению презентации при защите и к выступлению выпускника в ходе защиты	Имеются существенные замечания к содержанию и оформлению презентации и выступлению или презентация отсутствует.
<b>Навыки публичной дискуссии</b>	Выпускник исчерпывающе, последовательно, грамотно и логически стройно излагает суть и решение проблемы, прослеживается умение делать выводы, обобщать знания и практический опыт; выпускник показывает глубокие знания вопросов темы дипломного проекта, свободно оперирует профессиональной терминологией, материалами предметной области и средствами реализации; вносит обоснованные предложения по обеспечению информационной безопасности, эффективному использованию современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности; хороший язык и стиль изложения	Выпускник достаточно уверенно владеет содержанием работы, оперирует профессиональной терминологией, материалами предметной области и средствами реализации, но не всегда обоснованно и конкретно выражает свое мнение по поводу основных аспектов содержания проекта;	Доклад на тему представленного к защите дипломного проекта, содержит неточности в формулировке понятий, терминов. Изложение материала недостаточно связано и последовательно.	При защите выпускник не владеет материалом представленного к защите дипломного проекта, доклад на тему проекта содержит ошибки в формулировке понятий, терминов. Выпускник неуверенно излагает материал, работа доложена неубедительно. Выпускник с большими затруднениями демонстрирует работу приложения.
	Выпускник аргументировано, легко и технически грамотно отвечает на вопросы членов ГЭК, формулирует правильные, лаконичные и обоснованные ответы на поставленные вопросы с использованием профессиональной терминологии, имеет навыки публичной дискуссии	Выпускник дал ответы на большинство заданных вопросов.	Выпускник испытывает затруднения в ответах на вопросы членов комиссии, не всегда дает исчерпывающие аргументированные ответы на заданные вопросы.	Выпускник затрудняется отвечать на поставленные вопросы, при ответе допускает существенные ошибки или не отвечает на вопросы членов ГЭК. Ответы на поставленные вопросы неубедительны
	Выдержан установленный регламент времени публичного выступления	Выдержан установленный регламент времени публичного выступления	Выдержан установленный регламент времени публичного выступления	Не выдержан установленный регламент времени публичного выступления
<b>Положительный отзыв руководителя проекта</b>	Проект имеет положительный отзыв руководителя проекта	Проект имеет положительный отзыв руководителя проекта, но содержащий некоторые рекомендации и не-существенные замечания	В отзыве руководителя имеются рекомендации и замечания по содержанию, методике анализа и оформлению проекта	В отзыве руководителя имеются существенные критические замечания по содержанию и оформлению проекта

## Индивидуальный лист оценки дипломного проекта

« \_\_\_\_\_ » \_\_\_\_\_ 202\_ г.

ФИО студента \_\_\_\_\_

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

№	Критерии оценивания	Оценка соответствия требованиям к дипломным проектам Количество баллов 0 – не соответствует 1 - частично 2 - соответствует
<b>Уровень проработки проблемы</b>		
16.	Соответствие проекта содержания заявленной теме, заданию на проектирование (исследование)	
17.	Раскрыта актуальность выбранной темы, взаимосвязь с современными тенденциями развития отрасли. Правильно определены объект, предмет, гипотеза исследования. Выделена проблема исследования и четко определены цель и задачи работы	
18.	Глубокая теоретическая проработка исследуемых вопросов на основе анализа используемых источников; критический подход к изучаемым фактическим материалам с целью поиска резервов повышения информационной безопасности	
19.	Умелая систематизация данных в виде таблиц, графиков, схем с необходимым анализом, обобщением и выявлением угроз информационной безопасности. Даны практические рекомендации по повышению эффективности и качества информационной безопасности.	
20.	Адекватность применения современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности, целесообразность использования конкретных средств обеспечения информационной безопасности	
21.	Логичное, последовательное изложение материала, взаимосвязь теоретической части работы с практической, обоснованность использования источников и этика цитирования.	
22.	Самостоятельность выполнения проекта, творческий подход к изложению материала, обоснованность предложений и рекомендаций	
23.	Выпускник при выполнении и защите дипломного проекта демонстрирует высокий уровень освоения общих и профессиональных компетенций, определенных ФГОС по специальности	
<b>Оформление работы</b>		
24.	Правильность, четкость структуры проекта	
25.	Соответствие оформления требованиям стандартов	
<b>Иллюстративность, качество презентации результатов работ</b>		
26.	Доклад сопровождается мультимедиа презентацией. В презентации отражаются основные этапы и результаты проекта Качество иллюстративного материала, представленного в презентации к докладу: соответствие подбора иллюстративных материалов содержанию доклада, грамотность их оформления и упоминание в докладе, выразительность использованных средств	
<b>Навыки публичной дискуссии</b>		

27.	Выпускник исчерпывающе, последовательно, грамотно и логически стройно излагает суть и решение проблемы, прослеживается умение делать выводы, обобщать знания и практический опыт. Выпускник показывает глубокие знания вопросов темы дипломного проекта, свободно оперирует профессиональной терминологией, материалами предметной области и средствами реализации; вносит обоснованные предложения по обеспечению информационной безопасности, эффективному использованию современных аппаратных и программно-аппаратных средств обеспечения информационной безопасности хороший язык и стиль изложения	
28.	Выпускник аргументировано, легко и технически грамотно отвечает на вопросы членов ГЭК, формулирует правильные, лаконичные и обоснованные ответы на поставленные вопросы с использованием профессиональной терминологии, имеет навыки публичной дискуссии	
29.	Выдержан установленный регламент времени публичного выступления	
<b>Положительный отзыв руководителя проекта</b>		
30.	Проект имеет положительный отзыв руководителя проекта	
		<b>Итого:</b>

#### Перевод фактической суммы баллов в оценку

Процент результативности	Балл (отметка)	оценка	
90%-100%	31-34 баллов	5	отлично
75%-89%	26-30 баллов	4	хорошо
65%-74%	22-25 баллов	3	удовлетворительно
Менее 65%	Менее 22 баллов	2	неудовлетворительно

### 3.2. Темы дипломных проектов

1. Модернизация локальной вычислительной сети в ГБПОУ РД «Технический колледж им. Р. Н. Ашуралиева»
2. Проектирование и внедрение VPN технологии для безопасности корпоративной сети предприятия ООО «ТехноСофт»
3. Усовершенствование системы информационной безопасности малого предприятия – на примере предприятия по выполнению ремонтно-строительных работ
4. Разработка комплексной системы защиты информации на предприятии ОАО «Дагэлектроавтомат»
5. Проектирование и организация беспроводной сети на основе технологии Wi-Fi для спортивного клуба «Атлет»
6. Проектирование системы комплексного обеспечения информационной безопасности для производственного предприятия
7. Совершенствование системы информационной безопасности в электромонтажной компании «Электросити»
8. Защита корпоративной почты ООО "Стройсервис-100"
9. Разработка комплекса защитных мер по обеспечению информационной безопасности при попытке доступа в удаленную систему организации
10. Проектирование комплексного обеспечения информационной безопасности для фирмы по розничной торговле
11. Проектирование и реализация локальной вычислительной сети кондитерской «Причуды Избушки»
12. Разработка и внедрение методов по обеспечению информационной безопасности баз данных
13. Проектирование и разработка системы безопасности персональных данных на примере организации здравоохранения

14. Построение и совершенствование системы защиты информации в издательстве
15. Развертывание и настройка системы мониторинга Zabbix на предприятии АО "Завод им. Гаджиева"
16. Установка и настройка тестового стенда с применением файрвола Континент 4 на предприятии ООО «Ама Континент»
17. Мониторинг событий информационной безопасности на предприятии ООО "ТУ-РАЛИ - КАСПИЙ"
18. Проектирование защищенной беспроводной сети склада временного хранения товаров
19. Разработка системы защиты информации для фирмы по производству металлоконструкций «МеталлДом»
20. Разработка системы безопасности информации для фирмы по проектированию и реализации программного обеспечения
21. Проектирование системы комплексного обеспечения информационной безопасности для медицинского центра
22. Разработка политики безопасности для обмена данными центрального офиса IT-компании «Интех-Софт»
23. Проектирование системы комплексного обеспечения информационной безопасности для головного офиса службы доставки еды
24. Совершенствование системы обеспечения информационной безопасности фирмы по производству и реализации стройматериалов
25. Проектирование корпоративной инфокоммуникационной сети на базе технологии ViPNet
26. Проектирование и реализация системы защиты информации на примере ООО «Дагнотех»
27. Разработка и внедрение методов использования биометрических технологий в системах безопасности организации
28. Построение и совершенствование системы защиты информации для хостинг-провайдера
29. Разработка и совершенствование комплексной системы обеспечения информационной безопасности в гостинице
30. Анализ и разработка системы информационной безопасности парфюмерно-косметической компании
31. Разработка программного модуля, реализующая функцию «Криптография данных» для операционной системы Windows
32. Проектирование и реализация системы уязвимостей в современных операционных системах
33. Проектирование комплексного обеспечения информационной безопасности для аудиторско-консалтинговой компании
34. Разработка рекомендаций по обеспечению безопасного электронного документооборота в фирме по созданию и реализации ювелирных изделий
35. Защита веб-сервера в Филиале ФГБОУ ВО «Санкт-Петербургский государственный экономический университет»
36. Выбор и обоснование мер по защите автоматизированной системы обработки персональных данных в фирме по подбору и продаже автомобилей
37. Разработка приложения криптографической защиты информации с помощью шифра Вернама для операционной системы Windows
38. Разработка рекомендаций по усовершенствованию системы защиты информации в частном охранном предприятии
39. Повышение защищенности сетевого подключения организации по предоставлению информационных технологий и услуг с помощью межсетевого экрана

40. Разработка рекомендаций по защите информационных систем от компьютерных атак, направленных на обход автоматических систем идентификации пользователей
41. Создание и реализация стратегии информационной безопасности для логистической компании
42. Разработка проекта для формирования защищенной корпоративной сети фирмы по оптовой продаже товаров с использованием технологий VPN
43. Разработка рекомендаций по совершенствованию системы защиты информации в отеле бизнес-класса
44. Разработка рекомендаций по обеспечению безопасности локальной вычислительной сети предприятия, занимающейся разработкой и продвижением веб-проектов
45. Управление безопасностью с на предприятии АО «Дагпродмаш» с применением системы комплексного мониторинга
46. Построение корпоративной сети предприятия ОАО «Завод стекловолокна» с помощью Cisco
47. Разработка комплексной защиты информации для магазина компьютерной техники «Импульс» г. Махачкалы
48. Проектирование и внедрение информационной безопасности в автоматизированной системе учета электроэнергии предприятия
49. Модернизация системы информационной безопасности для Бронницкого ювелирного завода
50. Разработка системы обеспечения информационной безопасности личных данных при проектировании системы «умный дом»