



Министерство образования Московской области
Государственное бюджетное профессиональное образовательное учреждение
Московской области

«Подольский колледж имени А.В. Никулина»

УТВЕРЖДАЮ

Директор ГБПОУ МО

«Подольский колледж имени А.В. Никулина»

_____ А.А.Гридюшко

«___» _____ 20__ г.

**Рассмотрено и утверждено на заседании
педагогического совета колледжа
протокол № ___ от «___» _____ 20__ г.**

СОГЛАСОВАНО

Председатель ГЭК по ППСЗ 10.02.04 «Обеспечение инфор-
мационной безопасности телекоммуникационных систем»

ПАО Группа Астра,

руководитель отдела образовательных проектов

_____ Е.Г. Попцова

«___» _____ 20__ г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ВЫПУСКНИКОВ

**по программе подготовки специалистов среднего звена по специальности:
10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»
(форма обучения – очная)**

Введено в действие приказом директора

№ _____ от «___» _____ 20__ г.

СОДЕРЖАНИЕ		стр.
1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА		2
2. ПАСПОРТ ПРОГРАММЫ ГИА.....		3
3. УСЛОВИЯ ПОДГОТОВКИ И ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТО- ГОВОЙ АТТЕСТАЦИИ (В ФОРМЕ ДЕМОСТРАЦИОННОГО ЭКЗАМЕНА)		5
4. КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ.....		8
5. ПЕРЕВОД БАЛЛОВ ДЕМОСТРАЦИОННОГО ЭКЗАМЕНА В ОЦЕНКУ.....		22
6. ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИИ.....		23
7. ОСОБЕННОСТИ ПРОВЕДЕНИЯ ГИА ДЛЯ ВЫПУСКНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ, ДЕТЕЙ-ИНВА- ЛИДОВ И ИНВАЛИДОВ.....		25
8. ГРАФИК ПОДГОТОВКИ И НАПИСАНИЯ ДИПЛОМНОГО ПРОЕКТА.....		26
9. ТЕМАТИКА ДИПЛОМНЫХ ПРОЕКТОВ.....		28
10. ДОКУМЕНТЫ ВЫПУСКНИКА.....		29

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1. Порядок проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования (далее соответственно - Порядок, ГИА) устанавливает правила организации и проведения организациями, осуществляющими образовательную деятельность по образовательным программам среднего профессионального образования (далее - образовательные организации), ГИА студентов (далее - выпускники), завершающей освоение имеющих государственную аккредитацию основных профессиональных образовательных программ среднего профессионального образования (программ подготовки квалифицированных рабочих, служащих и программ подготовки специалистов среднего звена) (далее - образовательные программы среднего профессионального образования), включая формы ГИА, требования к использованию средств обучения и воспитания, средств связи при проведении ГИА, требования, предъявляемые к лицам, привлекаемым к проведению ГИА, порядок подачи и рассмотрения апелляций, изменения и (или) аннулирования результатов ГИА, а также особенности проведения ГИА для выпускников из числа лиц с ограниченными возможностями здоровья, детей-инвалидов и инвалидов.

2. Обеспечение проведения ГИА осуществляется образовательной организацией.

3. Образовательные организации используют необходимые для организации образовательной деятельности средства обучения и воспитания при проведении ГИА выпускников.

4. Программа государственной итоговой аттестации разработана в соответствии:

– с порядком проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования, утвержденного приказом Министерства просвещения Российской Федерации от 08.11.2021 г. № 800 (в ред. Приказов Минпросвещения России от 05.05.2022 № 311, от 19.01.2023 № 37, от 24.04.2024 № 272, от 22.12.2024 № 812);

– со статьей 59 «Итоговая аттестация» Федерального закона Российской Федерации от 29.12.2012 года № 273 «Об образовании в Российской Федерации»;

– с приказом Министерства образования и науки Российской Федерации «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования» № 762 от 24.08.2022г.;

– с федеральным государственным образовательным стандартом среднего профессионального образования специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 №1551;

– с приказом Минпросвещения России от 01.09.2022 N 796 «О внесении изменений в федеральные государственные образовательные стандарты среднего профессионального образования»;

– с Положением о Государственной итоговой аттестации в ГБПОУ МО «Подольский колледж имени А.В. Никулина» и Методическими рекомендациями о проведении аттестации с использованием механизма демонстрационного экзамена (Распоряжение Министерства просвещения РФ от 01.2019 №Р-42);

– с оценочными материалами демонстрационного экзамена КОД 10.02.04-1-2026 Техник по защите информации, разработанными и утвержденными приказом ФГБОУ ДПО ИРПО от 29.09.2025 № 01-09-538/2025.

Целью государственной итоговой аттестации в форме демонстрационного экзамена является установление степени готовности обучающегося к самостоятельной деятельности, сформированности профессиональных компетенций в соответствии с федеральным государственным образовательным стандартом среднего профессионального образования (ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Программа государственной итоговой аттестации ежегодно обновляется и утверждается директором после ее рассмотрения и одобрения Педагогическим советом. Программа государственной итоговой аттестации согласовывается с работодателем.

Программа государственной итоговой аттестации разрабатывается и доводится до сведения студентов не позднее, чем за шесть месяцев до начала государственной итоговой аттестации.

В программе используются следующие сокращения:

ГИА - государственная итоговая аттестация;

ГЭК - государственная экзаменационная комиссия;

ДЭ – демонстрационный экзамен

СПО - среднее профессиональное образование;

ФГОС- федеральный государственный образовательный стандарт;

ЦПДЭ - центр проведения демонстрационного экзамена;

ЦПК - цифровой паспорт компетенций.

2. ПАСПОРТ ПРОГРАММЫ ГИА

2.1. Специальность/профессия СПО

10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

2.2. ФГОС СПО

Федеральный государственный стандарт среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 №1551, зарегистрирован в Минюсте РФ 26.12.2016 № 44944.

2.3. Квалификация

– Техник по защите информации

2.4. Срок получения среднего профессионального образования по программе подготовки специалистов среднего звена

3 года 10 месяцев

2.5. Исходные требования к подготовке и проведению государственной итоговой аттестации по программе подготовки квалифицированных рабочих, служащих

Форма государственной итоговой аттестации в соответствии с ФГОС СПО	Государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы (дипломная работа (дипломный проект)). По усмотрению образовательной организации демонстрационный экзамен (профильный уровень) включается в выпускную квалификационную работу
Объем времени на подготовку и проведение государственной итоговой аттестации	Подготовка 4 недели проведение 2 недели
Сроки подготовки и проведения государственной итоговой аттестации	Подготовка с «18» мая 2026 г. по «14» июня 2026г. Проведение с «15» июня 2026 г. по «28» июня 2026г.

2.6. Итоговые образовательные результаты по программе подготовки квалифицированных рабочих, служащих

Программа государственной итоговой аттестации разработана в соответствии с ФГОС СПО по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» в части освоения **видов деятельности (ВД) и соответствующих профессиональных компетенций (ПК):**

1. Эксплуатация информационно-телекоммуникационных систем и сетей:

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

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

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

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

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

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

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

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специ-

альных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

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

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

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

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

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

Общие компетенции

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. (п. 3.2 в ред. Приказа Минпросвещения России от 03.07.2024 N 464).

3. УСЛОВИЯ ПОДГОТОВКИ И ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ (В ФОРМЕ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА).

3.1. Формирование состава государственной экзаменационной комиссии

Итоговая аттестация выпускников по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» осуществляется государственной экзаменационной комиссией, состав которой формируется по каждой образовательной программе СПО. При необходимости могут создаваться несколько государственных экзаменационных комиссий по одной образовательной программе.

Государственная экзаменационная комиссия создается для проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования в соответствии с Порядком проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования.

Государственная экзаменационная комиссия руководствуется в своей деятельности, вышеописанным порядком и настоящей программой, разрабатываемой на основе федерального государственного образовательного стандарта в части требований к результатам освоения основной профессиональной образовательной программы по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

1. ГЭК формируется из числа педагогических работников образовательных организаций, лиц, приглашенных из сторонних организаций, в том числе: педагогических работников; представителей организаций-партнеров, направление деятельности которых соответствует области профессиональной деятельности, к которой готовятся выпускники.

2. При проведении демонстрационного экзамена в составе ГЭК создается экспертная группа из числа лиц, приглашенных из сторонних организаций и обладающих профессиональными знаниями, навыками и опытом в сфере, соответствующей профессии или специальности среднего профессионального образования или укрупненной группы профессий и специальностей, по которой проводится демонстрационный экзамен (далее соответственно - экспертная группа, эксперты).

3. Состав ГЭК утверждается распорядительным актом образовательной организации и действует в течение одного календарного года. В состав ГЭК входят председатель ГЭК, заместитель председателя ГЭК и члены ГЭК.

4. ГЭК возглавляет председатель, который организует и контролирует деятельность ГЭК, обеспечивает единство требований, предъявляемых к выпускникам.

5. Председатель ГЭК утверждается не позднее 20 декабря текущего года на следующий календарный год (с 1 января по 31 декабря) по представлению образовательной организации органом местного самоуправления муниципального района, муниципального округа, городского округа, органом исполнительной власти субъекта Российской Федерации, федеральным органом исполнительной власти, в ведении которого соответственно находится образовательная организация, а в случае, если функции и полномочия учредителя образовательной организации осуществляет Правительство Российской Федерации - по представлению указанной образовательной организации Министерством просвещения Российской Федерации.

6. Председателем ГЭК образовательной организации утверждается лицо, не работающее в образовательной организации, из числа: руководителей или заместителей руководителей организаций, осуществляющих образовательную деятельность, соответствующую области профессиональной деятельности, к которой готовятся выпускники; представителей работодателей или их объединений, организаций-партнеров, включая экспертов, при условии, что направление деятельности данных представителей соответствует области профессиональной деятельности, к которой готовятся выпускники.

7. Руководитель образовательной организации является заместителем председателя ГЭК.

В случае создания в образовательной организации нескольких ГЭК назначается несколько заместителей председателя ГЭК из числа заместителей руководителя образовательной организации или педагогических работников.

8. Экспертная группа создается по каждой профессии, специальности среднего профессионального образования или виду деятельности, по которому проводится демонстрационный экзамен.

9. Экспертную группу возглавляет главный эксперт, назначаемый из числа экспертов, включенных в состав ГЭК. Главный эксперт организует и контролирует деятельность возглавляемой экспертной группы, обеспечивает соблюдение всех требований к проведению демонстрационного экзамена и не участвует в оценивании результатов демонстрационного экзамена.

10. К ГИА допускаются выпускники, не имеющие академической задолженности и в полном объеме выполнившие учебный план или индивидуальный учебный план.

3.2. Общие требования к организации демонстрационного экзамена

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

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

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

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

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

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

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

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

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

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

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

распределения рабочих мест между обучающимися фиксируются главным экспертом в соответствующих протоколах.

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

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

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

4. КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ

4.1.Применимость КОД

Вид аттестации	Уровень ДЭ
ГИА	Профильный уровень

4.2.Требование к продолжительности ДЭ

Вид аттестации	Уровень ДЭ	Составная часть КОД (инвариантная/ вариативная)	Продолжительность ДЭ
ГИА	профильный	Инвариантная часть	3 ч. 30 мин.

4.3.Содержательная структура КОД

Вид деятельности (вид профессиональной деятельности)	Перечень оцениваемых ОК, ПК	Перечень оцениваемых уме- ний, навыков (практического опыта)
Эксплуатация информационно – телекоммуникационных систем и сетей	ПК: производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно – телекоммуникационных систем и сетей	Умение: настраивать, эксплуатировать и обслуживать оборудование ИТКС
		Практический опыт: монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС
	ОК. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии	Умения: применять средства информационных технологий для решения профессиональных задач

	<p>для выполнения задач профессиональной деятельности</p>	
	<p>ПК. Осуществлять контроль функционирования информационно- телекоммуникационных систем и сетей</p>	<p>Умение: проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС</p> <p>Практический опыт: текущем контроле функционирования оборудования ИТКС</p> <p>Умение: настраивать, эксплуатировать и обслуживать оборудование ИТКС</p> <p>Умение: производить испытания, проверку и приемку оборудования ИТКС</p>
<p>Защита информации в информационно – телекоммуникационных системах и сетях с использованием программно- аппаратных, в том числе криптографических средств защиты</p>	<p>ПК: производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно – телекоммуникационных систем и сетей</p>	<p>Умение: проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Умение: проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации</p> <p>Практический опыт: установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно- телекоммуникационных систем и сетей</p> <p>ПК: поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в</p> <p>Умение: проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации</p>

	информационно – телекоммуникационных системах и сетях	Практический опыт: поддержки бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях
		Умение: проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации
	ПК: осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	Практический опыт: защиты информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями
		Умение: проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации

4.4. Распределение баллов по критериям оценивания для ДЭ ПУ (инвариантная часть КОД) в рамках ГИА

№ п/п	Вид деятельности /Вид профессиональной деятельности	Критерий оценивания	Баллы
1	Эксплуатация информационно- телекоммуникационных систем и сетей	Производство монтажа, настройки, проверки функционирования и конфигурирование оборудования информационно- телекоммуникационных систем и сетей	9,00
		Осуществление контроля функционирования информационно-телекоммуникационных систем и сетей	16,00

		Использование современных средств поиска, анализа и интерпретации информации, и информационных технологий для выполнения задач профессиональной деятельности	2,00
	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	Производство установки, настройки, испытаний и конфигурирования программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетей	18,00
		Поддержка бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях	18,00
		Осуществление защиты информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями	12,00
ИТОГО			75,00

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 75 баллов

4.5. Образцы задания

Задание ДЭ представляет собой сочетание модулей в зависимости от вида аттестации и уровня ДЭ. Продолжительность выполнения каждого модуля задания представлена в таблице

Модули	Вид деятельности / Вид профессиональной деятельности	Продолжительность выполнения Модуля / совокупности Модулей и общее время на выполнение задания
		ГИА ДЭ ПУ (инвариантная часть)

Модуль 1	Эксплуатация информационно- телеком- муникационных систем и сетей	0 ч. 30 мин.
Модуль 2	Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно- аппаратных ,в том числе криптографических средств защиты	1 ч. 00 мин.
Модуль 3	Эксплуатация информационно- телеком- муникационных систем и сетей, Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно- аппаратных, в том числе криптографических средств защиты	1 ч. 00 мин.
Модуль 4	Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно- аппаратных, в том числе криптографических средств защиты	0 ч. 30 мин.
Модуль 5	Эксплуатация информационно- телеком- муникационных систем и сетей	0 ч. 30 мин.
Максимальная продолжительность демонстрационного экзамена:		3 ч. 30 мин.

Образец задания для ГИА ДЭ ПУ (инвариантная часть)

Модуль 1. Моделирование защищённой корпоративной сети в виртуальной среде

В рамках выполнения практического задания необходимо в среде виртуализации смоделировать защищённую корпоративную сеть организации, включающую два филиала:

- **главный офис** - реализуется на виртуальных машинах;
- **филиал** - реализуется на отдельных виртуальных машинах.

Ваша задача - произвести первичную настройку виртуальной инфраструктуры. В процессе выполнения работы необходимо:

- установить необходимое программное обеспечение на все рабочие станции защищённой сети;
- настроить учётные записи и задать пароли (для всех создаваемых учётных записей используйте пароль «ххХХ12345678». Указанный пароль необходимо применить без изменений и зафиксировать в отчёте в таблице учётных записей);
- выполнить базовую настройку сетевой среды (создать и настроить сетевые адаптеры виртуальных машин, назначить IP-адреса, задать имена хостов, настроить маршрутизацию).

По итогам работы вы должны подготовить отчёт в текстовом редакторе.

В отчёт включаются **скриншоты всех ключевых этапов настройки**, подтверждающие корректность выполненных действий.

Задача 1.1: Настройка сетевого окружения

Для обеспечения корректного взаимодействия между компонентами сети необходимо создать и настроить следующие сетевые адаптеры (используя режимы Host-only, Internal, NAT или

Bridge, в зависимости от платформы виртуализации). Для каждого сегмента создаётся отдельный адаптер указанного типа, при этом его имя в настройках виртуализации можно задать произвольно, при условии, что оно будет уникальным и отражать назначение сети:

- сеть Главного офиса (ЦО) - адаптер Host-only или Internal;
- сеть филиала - адаптер Host-only или Internal;
- сеть межсетевого взаимодействия между филиалами - адаптер Host-only или Internal;
- виртуальный доступ в Интернет - адаптер Host-only, NAT или Bridge.

Назначение адресов производится самостоятельно **в пределах указанных диапазонов:**

- сеть 1 Главного офиса (ЦО): 10.10.64/27;
- сеть 1 Филиала: 110.10.96/28;
- сеть 2 Офиса: 16.129.128/25;
- интернет-сегмент для всех координаторов: 100.102.0/24.

Внимание! Убедитесь, что при конфигурации IP-адресов не возникает пересечений, а выбранные IP соответствуют указанным подсетям.

Необходимые приложения: отсутствуют.

Модуль 2. Развёртывание защищённой корпоративной сети с помощью виртуальной инфраструктуры

Задание 2.1. Развёртывание рабочего места администратора с функциями центра сертификации

Разверните виртуальное рабочее место администратора на базе машины

Net1-Center-Admin (центральный офис). На данном узле необходимо:

- установить модуль управления защищённой сетью (ЦУС включает серверную и клиентскую части);
- установить программные средства удостоверяющего и ключевого центра, обеспечивающие выпуск сертификатов и управление ключевой инфраструктурой;
- проверить корректность установки и работоспособность компонентов.

Задание 2.2. Установка клиентского VPN-программного обеспечения

Выполните установку программного обеспечения для защищённого подключения на следующие виртуальные машины:

- **Net1-Center-Admin (центральный офис)** — установка серверной и клиентской части VPN-системы, на базе пользовательской или серверной операционной системы. Данная машина будет использоваться как рабочее место администратора защищённой сети;
- **Net2-Branch-Client (филиал)** — установка клиентской части на машину пользователя, обеспечивающую подключение к защищённой сети из филиала.

Задание 2.3. Инициализация координационных узлов защищённой сети

Выполните процедуру инициализации программных координаторов защищённого взаимодействия:

- на виртуальной машине Net1-Center-Coord (центральный офис) - произведите запуск и первичную настройку координационного узла типа HW-VA;
- на виртуальной машине Net2-Branch-Coord (филиал) - выполните аналогичную инициализацию для соответствующего координационного узла HW-VA в филиале.

Задание 2.4. Развёртывание защищённой сетевой инфраструктуры

Используя подготовленное ранее рабочее место администратора, выполните создание и запуск компонентов защищённой корпоративной сети. Реализация должна производиться в среде виртуальных машин. Все автоматизированные рабочие места (АРМ) следует настроить в соответствии с их сетевыми ролями, показанными на схеме ниже.

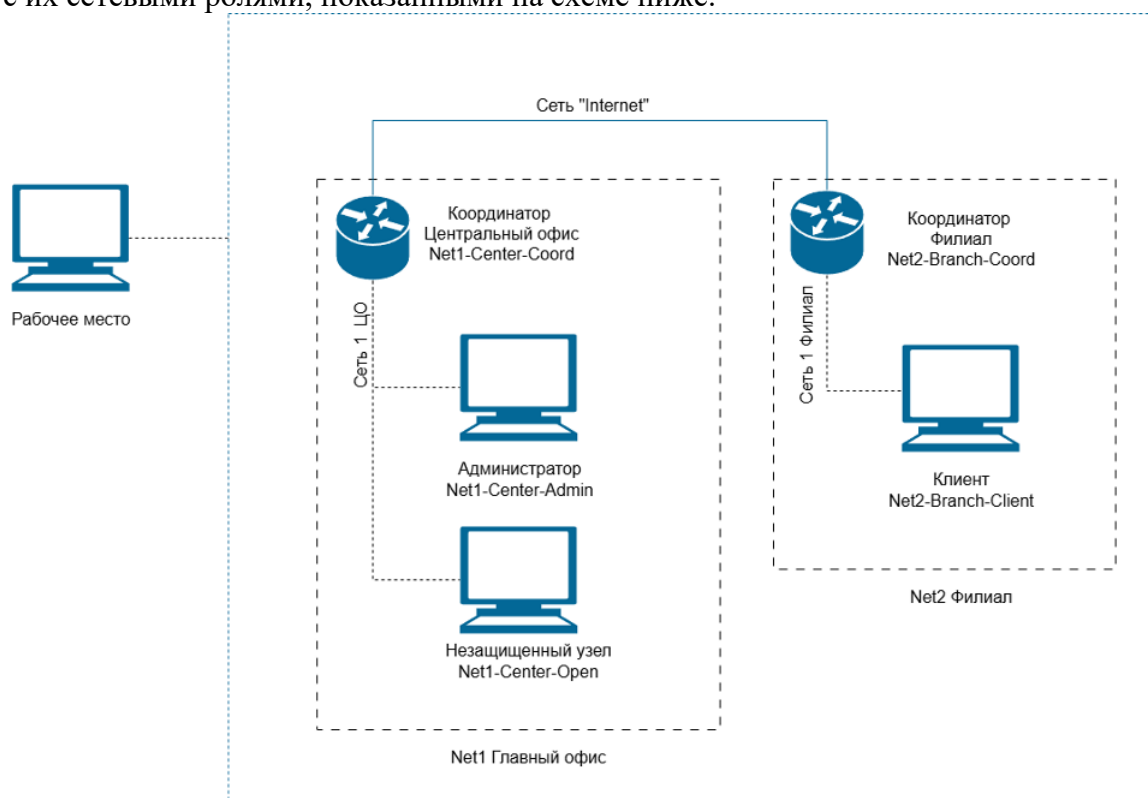


Рисунок 1 - Схема защищенной сети

В результате выполнения задания необходимо развернуть и сконфигурировать следующие узлы, описанные в таблице 1.

Таблица 1 - Сетевые узлы в защищённой инфраструктуре

Виртуальная машина	Назначение узла	Установленное ПО (по ролям)	Тип ОС	Имя пользователя
--------------------	-----------------	-----------------------------	--------	------------------

Net1-Center-Admin (Центр)	Сетевой администратор	Модуль управления защищённой сетью (ЦУС) и программные средства удостоверяющего и ключевого центра (УКЦ)	Пользовательская или серверная	AdmN1
Net1-Center-Coord (Центр)	Координационный узел офиса	Координатор защищённого сегмента	HW-VA	CoordN1
Net2-Branch-Coord (Филиал)	Координационный узел филиала	Координатор защищённого сегмента	HW-VA	CoordN2
Net2-Branch-Client (Филиал)	Клиентское АРМ	Клиент защищённой сети	Пользовательская или серверная	UserN2

Задание 2.5. Формирование логической структуры

Сформируйте в системе управления защищённой сетью структуру логических связей между узлами. Используйте схему на рисунке и информацию из таблицы ниже.

Таблица 2 - Схема логических связей между пользователями

Пользователь	AdmN1	CoordN1	CoordN2	UserN2
AdmN1	×	✓		■
CoordN1	✓	×	■	
CoordN2		■	×	✓
UserN2	■		■	×

Дополнительные действия:

1. Инициализируйте удостоверяющий центр;
2. Установите тип паролей для всех пользователей как «собственный»;
3. Сформируйте и экспортируйте дистрибутивы ключевой информации;
4. Разнесите ключи по соответствующим узлам сети;
5. Проведите первичную инициализацию каждого из АРМ;
6. Убедитесь в доступности всех защищённых узлов (проверка соединения);
7. Отправить текстовое сообщение пользователю AdmN1 от пользователя UserN
8. Подготовьте скриншоты, подтверждающие успешную настройку и работоспособность всех узлов.

Задание 2.6. Настройка резервного копирования

На узле Net1-Center-Admin (ЦО) выполните резервное копирование конфигурации сети с помощью возможностей системы управления защищённой сетью.

1. Ручное создание резервной копии: с помощью возможностей средств администрирования создайте резервную копию конфигурации сети.
2. Настройка автоматического резервного копирования: настройте автоматическое создание резервных копий конфигурации сети по расписанию - ежедневно в 23:00.

Шаблон отчета по практическому заданию Модуль 1 и Модуль 2

1. Общие сведения

- ФИО студента:
- Группа:
- Дата выполнения:
- Платформа виртуализации: (*например, VirtualBox / VMware / KVM*)
- ПО, использованное при выполнении задания.

1.1.9. Развертывание виртуальной среды

2.1. Сетевые адаптеры и IP-адресация

- таблица с перечнем виртуальных сетей и их назначением;
- скриншоты конфигурации адаптеров VM;
- обоснование выбора типа сети: NAT, Host-only и т.д.

2.2. Создание и настройка виртуальных машин

- таблица с VM: имя, ОС, роль, IP, логин пользователя;
- скриншоты диспетчера виртуальных машин и настроек.

1.1.10. Развертывание инфраструктуры управления

3.1. Установка программных компонентов на Net1-Center-Admin

- установка ЦУС: сервер и клиент;
- установка УКЦ;
- скриншоты установки и запуска сервисов.

3.2. Установка клиентов

- Net1-Center-Admin: установка VPN Client;
- Net2-Branch-Client: установка VPN Client;
- скриншоты подтверждающие установку.

3.3. Инициализация координаторов

- Net1-Center-Coord: настройка HW-VA;

- Net2-Branch-Coord: настройка HW-VA;
- скриншоты инициализации + присвоение имени узлу.

1.1.11. Настройка защищённой сети

4.1. Создание структуры в ЦУС

- таблица: сущности, их роли, связи (схема аналогичная Таблице 2);
- скриншот интерфейса ЦУС со структурой;
- обоснование связей пользователей.

4.2. Инициализация УКЦ

- пошагово: запуск УКЦ, генерация ключей, смена типа паролей;
- скриншоты ключевых операций;
- таблица с информацией об узлах и их ключах.

1.1.12. Разнесение дистрибутивов ключей и первичная инициализация

- скриншоты: импорт ключей на Net1-Center-Admin, Net1-Center-Coord, Net2-Branch-Coord, Net2-Branch-Client;
- проверка доступности: пинг, соединение, логи;
- список проверенных связей и краткое описание результатов.

6. Настройка резервного копирования

- пошагово: процесс ручного создания резервной копии
- настройки автоматического резервного копирования
- содержимое папки с созданными резервными копиями Журналы/логи при необходимости.

Необходимые приложения: отсутствуют.

Модуль 3. Настройка межсетевого взаимодействия защищённых сегментов

На базе виртуальной машины **Net3-Transit-Admin** необходимо развернуть дополнительное рабочее место администратора, которое будет представлять партнёрский защищённый сегмент. В составе этой новой логической сети также требуется создать координатор на узле **Net3-Transit-Coord** и незащищенный узел **Net3-Transit-Open**.

Состав устанавливаемого ПО:

- На Net3-Transit-Admin - система управления защищённой сетью и средства управления ключевой инфраструктурой
- На Net3-Transit-Coord - программный или виртуальный координационный узел
- На Net3-Transit-Open - клиентское программное обеспечение для защищённого подключения

После установки и настройки необходимого программного обеспечения, следует:

- сформировать архитектуру второго защищённого сегмента в соответствии со схемой (см. рисунок 2),
- настройте межсетевой обмен между доменом основной сети (Net1) и доменом партнёрской сети (Net3),
- обеспечить взаимодействие между узлами защищённых сетей с применением **асимметричных межсетевых ключей**.

Схематическая структура межсетевого взаимодействия приведена на **рисунке 2**.

После завершения конфигурации необходимо убедиться в работоспособности межсетевого обмена, отправив электронное сообщение с узла **Net1-Center-Admin** (администратор основной сети) на **Net3-Transit-Admin** (администратор партнёрской сети) средствами почтового модуля клиентского ПО для защищённых сетей.

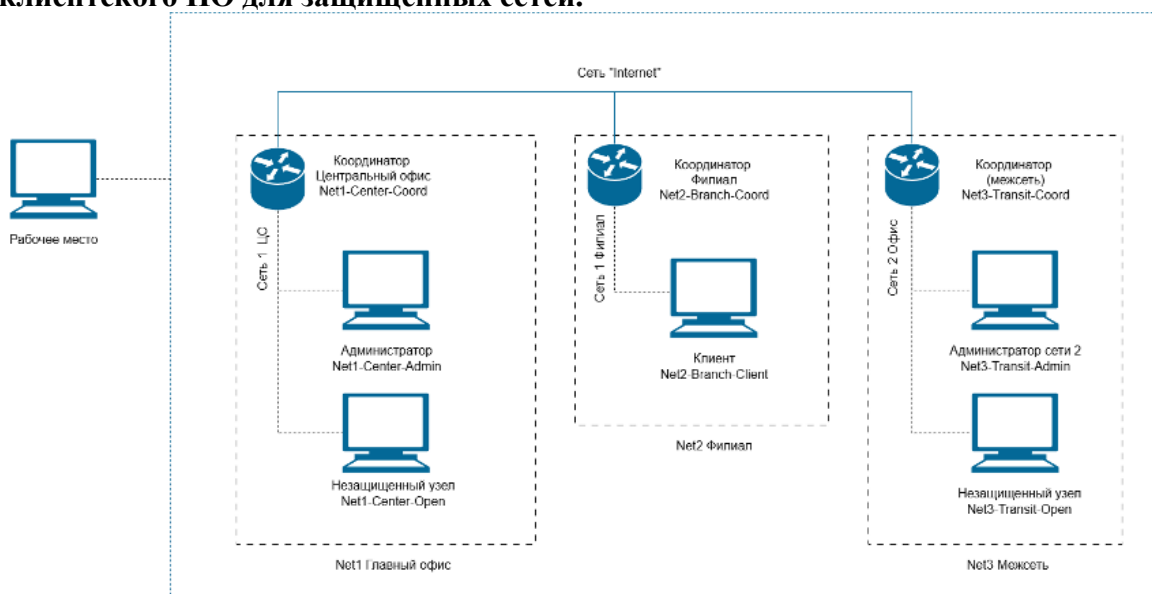


Рисунок 2 - Схема межсетевого взаимодействия

Шаблон отчета по Модулю 3:

Развёртывание и настройка Net3-Transit-Admin:

- установка ПО системы управления защищённой сетью и средств управления ключевой инфраструктурой;
- первичная инициализация;
- создание пользователя и объекта координатора.

Скриншот 1 - установка ПО

Скриншот 2 - создание узла администратора в ЦУС

Создание координатора Net3-Transit-Coord:

- назначение роли координатора;
- привязка к сегменту Net3.

Скриншот 3 - добавление координатора

Скриншот 4 - параметры инициализации

Обмен межсетевыми ключами:

- генерация асимметричных межсетевых ключей;
- передача и установка ключей между Net1 и Net3.

Скриншот 5 - создание межсетевых связей

Скриншот 6 - подтверждение ключей на стороне Net1

Скриншот 7 - подтверждение ключей на стороне Net3

Настройка межсетевых связей в ЦУС:

- объединение сетей в межсетевой домен (Net1 и Net3);
- назначение политик доверия (правила обмена трафиком между доменами);
- проверка таблиц маршрутов (допустимы отличия при использовании NAT/проброса портов, при условии успешной проверки связи). **Скриншот 8** - настройка доверия

Скриншот 9 - готовая таблица маршрутов

Отправка сообщения между администраторами:

- отправка электронного письма с Net1-Center-Admin на Net3-Transit-Admin.

Скриншот 10 - подготовка сообщения

Скриншот 11 - подтверждение доставки

Необходимые приложения: отсутствуют.

Модуль 4. Настройка фильтрации трафика и межсетевого доступа в защищённой ИТ-инфраструктуре

Задание 4.1. Реализация политик ограничения интернет-доступа и администрирования устройств

В рамках данного задания необходимо использовать встроенные функции ранее инициализированного и настроенного координатора Net2- Branch-Coord для фильтрации трафика и ограничения интернет-доступа в филиале. Координатор будет выполнять роль устройства безопасности, обеспечивающего контроль доступа к ресурсам сети и интернету.

Требования по настройке:

- 1) активировать веб-интерфейс администрирования на порту 8080 для узла Net1-Center-Open;
- 2) разрешить прохождение ICMP-пакетов для соответствующих подсетей узла Net1-Center-Open;
- 3) запретить доступ к ресурсам: vk.com, ok.ru, google.com.

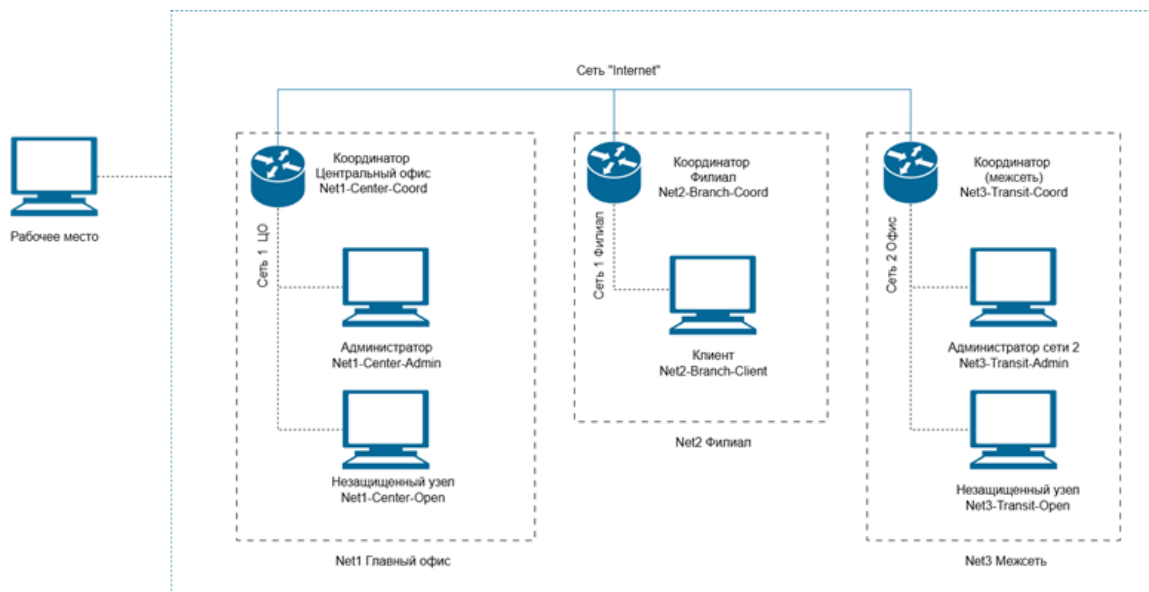


Рисунок 3 - Схема защищённой сети с межсетевым экраном

Внимание: все этапы настройки должны быть зафиксированы при помощи скриншотов и включены в итоговый отчёт.

Задание 4.2. Конфигурация правил доступа в сети

Вам необходимо настроить правила межсетевого взаимодействия на координаторе Net2-Branch-Coord, обеспечив:

- 1) удалённый доступ по RDP с узла Net2-Branch-Client (филиал) на Net1-Center-Open (незащищённый узел центрального офиса);
- 2) разрешение доступа по SSH к координатору Net1-Center-Coord со стороны узла Net2-Branch-Client.

При необходимости установка SSH-клиента на соответствующие виртуальные машины осуществляется самостоятельно.

Таблица 1 - Конфигурация фильтров

№	Протокол	Источник	Назначение	Порт	Действие
1	RDP	Net2-Branch-Client	Net1-Center-Open	3389	Разрешить
2	SSH	Net2-Branch-Client	Net1-Center-Coord	22	Разрешить

Правило 1 - Разрешить RDP от Net2-Branch-Client → Net1-Center-Open:

- протокол: RDP
- источник: Net2-Branch-Client

- назначение: Net1-Center-Open
- порт: 3389 (TCP)

Правило 2 - Разрешить SSH от Net2-Branch-Client→ Net1-Center-Coord:

- протокол: SSH
- источник: Net2-Branch-Client
- назначение: Net1-Center-Coord
- порт: 22 (TCP)

Контроль: убедитесь в корректной работе заданных фильтров и приложите скриншоты с подтверждением подключения по RDP и SSH.

Структура отчета:

Скриншот 1 - Настройка доступа к веб-интерфейсу (порт 8080) от Net1- Center-Open

Скриншот 2 - Разрешение ICMP-трафика к узлу Net1-Center-Open Скриншот 3- Блокировка запрещённых доменов

Скриншот 4- Проверка фильтрации (ping и доступ к сайтам) Скриншот 5 - Настройка фильтров на Net2-Branch-Coord Скриншот 6 - Подключение по RDP

Скриншот 7 - Подключение по SSH

Необходимые приложения: отсутствуют.

Модуль 5. Настройка туннелирования для зашифрованного обмена между открытыми узлами разных сегментов сети

Задача 5.1. Реализация туннелирования в межсетевом взаимодействии

Подключите открытый (незащищённый) узел в сети 3, используя виртуальную машину **Net3-Transit-Open**. В качестве второго открытого узла задействуйте **Net1-Center-Open**, расположенный в сети 1. Необходимо настроить туннельное соединение с использованием встроенных механизмов системы защищённой сети таким образом, чтобы обмен данными между этими двумя машинами происходил через **шифрованный защищённый канал**, несмотря на то, что они сами находятся вне периметра защищённой сети.

После настройки выполните проверку доступности узлов друг для друга:

- с помощью ICMP (ping);
- с применением другого протокола (например, SMB — доступ к сетевому ресурсу), либо любого другого по выбору студента, за исключением ICMP.

Дополнительно проведите **анализ журналов IP-пакетов** на координаторах соответствующих сетей и зафиксируйте факты установленного туннелирования.

Шаблон отчета:

Настройка туннелирования

1. Настройка узла Net1-Center-Open:

- IP-адрес: _____
- интерфейс: _____

- команды/скрипты настройки (пример):

Скриншот 1 - Настройка туннеля на Net1-Center-Open

2. Настройка узла Net3-Transit-Open:

- IP-адрес: _____

- интерфейс: _____

- команды/скрипты настройки:

Скриншот 2 - Настройка туннеля на Net3-Transit-Open Проверка связи с помощью ICMP (ping):

Скриншот 3 - Успешный ping Net3-Transit-Open с Net1-Center-Open Скриншот 4 - Успешный ping Net1-Center-Open с Net3-Transit-Open

3. Проверка по другому протоколу (например, SMB):

- используемый протокол: _____

- метод тестирования: _____

Скриншот 5 - Доступ к общей папке через туннель (или аналогичная проверка)

Анализ журналов координаторов Координатор сети 1 (Net1-Center-Coord):

Скриншот 6 - Журнал IP-пакетов, подтверждающий прохождение туннелированного трафика

Координатор сети 3 (Net3-Transit-Coord):

Скриншот 7 - Журнал IP-пакетов, подтверждающий обратное направление трафика

Необходимые приложения: отсутствуют.

5. ПЕРЕВОД БАЛЛОВ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА В ОЦЕНКУ

Результаты проведения ГИА оцениваются с проставлением одной из отметок: "отлично", "хорошо", "удовлетворительно", "неудовлетворительно" - и объявляются в тот же день после оформления протоколов заседаний ГЭК. Процедура оценивания результатов выполнения заданий демонстрационного экзамена осуществляется членами экспертной группы по 100-балльной системе в соответствии с требованиями комплекта оценочной документации. Баллы выставляются в протоколе проведения демонстрационного экзамена, который подписывается каждым членом экспертной группы и утверждается главным экспертом после завершения экзамена для экзаменационной группы.

При выставлении баллов присутствует член ГЭК, не входящий в экспертную группу, присутствие других лиц запрещено. Подписанный членами экспертной группы и утвержденный главным экспертом протокол проведения демонстрационного экзамена далее передается в ГЭК для выставления оценок по итогам ГИА. Оригинал протокола проведения демонстрационного экзамена передается на хранение в образовательную организацию в составе архивных документов.

При проведении оценки выполнения демонстрационного экзамена обучающимися может быть применена следующая схема перевода результатов ДЭ в пятибалльную шкалу:

Уровень ДЭ	«2»	«3»	«4»	«5»
Базовый уровень	0,00-24,99	25,00-32,49	32,50-44,99	45,00-50,00
Профильный уровень	0,00-37,49	37,50-38,69	48,70-67,49	67,50-75,00
Отношение полученного количества баллов к максимально возможному (в процентах)	0,00% - 49,99%	50,00% - 64,99%	70,00% - 89,99%	90,00% - 100,00%

Статус победителя, призера финала Чемпионата по профессиональному мастерству «Профессионалы» и финала Чемпионата высоких технологий по профилю осваиваемой образовательной программы среднего профессионального образования засчитывается выпускнику в качестве оценки «отлично» по демонстрационному экзамену в рамках проведения ГИА по данной образовательной программе среднего профессионального образования.

6. ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИИ

По результатам ГИА выпускник имеет право подать в апелляционную комиссию письменную апелляцию о нарушении, по его мнению, Порядка и (или) несогласии с результатами ГИА (далее - апелляция).

1. Апелляция подается лично выпускником или родителями (законными представителями) несовершеннолетнего выпускника в апелляционную комиссию образовательной организации. Апелляция о нарушении Порядка подается непосредственно в день проведения ГИА, в том числе до выхода из центра проведения экзамена. Апелляция о несогласии с результатами ГИА подается не позднее следующего рабочего дня после объявления результатов ГИА.

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

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

4. Апелляция рассматривается на заседании апелляционной комиссии с участием не менее двух третей ее состава. На заседание апелляционной комиссии приглашается председатель соответствующей ГЭК, а также главный эксперт при проведении ГИА в форме демонстрационного экзамена. При проведении ГИА в форме демонстрационного экзамена по решению председателя апелляционной комиссии к участию в заседании комиссии могут быть также привлечены члены экспертной группы, технический эксперт. По решению председателя апелляционной комиссии заседание апелляционной комиссии может пройти с применением средств видео, конференц-связи, а равно посредством представления письменных пояснений по поставленным апелляционной комиссией вопросам. Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции. С несовершеннолетним выпускником имеет право присутствовать один из родителей (законных представителей). Указанные лица должны при себе иметь документы, удостоверяющие личность.

5. Рассмотрение апелляции не является передачей ГИА.

6. При рассмотрении апелляции о нарушении Порядка апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из следующих решений: об отклонении апелляции, если изложенные в ней сведения о нарушениях Порядка не подтвердились и (или) не повлияли на результат ГИА; об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях Порядка подтвердились и повлияли на результат ГИА.

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

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

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

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

8. В результате рассмотрения апелляции о несогласии с результатами ГИА апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата ГИА

либо об удовлетворении апелляции и выставлении иного результата ГИА. Решение апелляционной комиссии не позднее следующего рабочего дня передается в ГЭК. Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов ГИА выпускника и выставления новых результатов в соответствии с мнением апелляционной комиссии.

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

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

10. Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

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

7. ОСОБЕННОСТИ ПРОВЕДЕНИЯ ГИА ДЛЯ ВЫПУСКНИКОВ ИЗ ЧИСЛА ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ, ДЕТЕЙ-ИНВАЛИДОВ И ИНВАЛИДОВ

1. Для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов проводится ГИА с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких выпускников (далее - индивидуальные особенности).

2. При проведении ГИА обеспечивается соблюдение следующих общих требований: проведение ГИА для выпускников с ограниченными возможностями здоровья, выпускников из числа детей-инвалидов и инвалидов в одной аудитории совместно с выпускниками, не имеющими ограниченных возможностей здоровья, если это не создает трудностей для выпускников при прохождении ГИА; присутствие в аудитории, центре проведения экзамена тьютора, ассистента, оказывающих выпускникам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с членами ГЭК, членами экспертной группы); пользование необходимыми выпускникам техническими средствами при прохождении ГИА с учетом их индивидуальных особенностей; обеспечение возможности беспрепятственного доступа выпускников в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов, лифтов, при отсутствии лифтов аудитория должна располагаться на первом этаже, наличие специальных кресел и других приспособлений).

3. Дополнительно при проведении ГИА обеспечивается соблюдение следующих требований в зависимости от категорий выпускников с ограниченными возможностями здоровья, выпускников из числа детей-инвалидов и инвалидов:

а) для слепых: задания для выполнения, а также инструкция о порядке ГИА, комплект

оценочной документации, задания демонстрационного экзамена оформляются рельефно-точечным шрифтом по системе Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, или зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом по системе Брайля или на компьютере со специализированным программным обеспечением для слепых, или надиктовываются ассистенту; выпускникам для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих: обеспечивается индивидуальное равномерное освещение не менее 300 люкс; выпускникам для выполнения задания при необходимости предоставляется увеличивающее устройство; задания для выполнения, а также инструкция о порядке проведения государственной аттестации оформляются увеличенным шрифтом;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи: обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости предоставляется звукоусиливающая аппаратура индивидуального пользования; по их желанию государственный экзамен может проводиться в письменной форме; г) для лиц с нарушениями опорно-двигательного аппарата (с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей): письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; по их желанию государственный экзамен может проводиться в устной форме;

д) также для выпускников из числа лиц с ограниченными возможностями здоровья и выпускников из числа детей-инвалидов и инвалидов создаются иные специальные условия проведения ГИА в соответствии с рекомендациями психолого-медико-педагогической комиссии (далее - ПМПК), справкой, подтверждающей факт установления инвалидности, выданной федеральным государственным учреждением медико-социальной экспертизы (далее - справка).

4. Выпускники или родители (законные представители) несовершеннолетних выпускников не позднее чем за 3 месяца до начала ГИА подают в образовательную организацию письменное заявление о необходимости создания для них специальных условий при проведении ГИА с приложением копии рекомендаций ПМПК, а дети-инвалиды, инвалиды - оригинала или заверенной копии справки, а также копии рекомендаций ПМПК при наличии.

8. ГРАФИК ПОДГОТОВКИ И НАПИСАНИЯ ДИПЛОМНОГО ПРОЕКТА

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

Дипломный проект (работа) выпускников, осваивающих образовательные программы в области искусств, предполагает различные виды подготовки, в том числе исполнение сольной программы/сольного номера, исполнение концертной программы с участием в сольных и ансамблевых/ансамблевых и хоровых номерах, дирижирование и работа с хором, участие в спектакле или иное, в соответствии с требованиями, установленными ФГОС СПО по соответствующей специальности.

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

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

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

Целесообразно начать разработку и написание дипломного проекта с начала прохождения преддипломной практики, т.к. преддипломная практика, как часть образовательной программы, является завершающим этапом обучения и проводится после освоения студентами программы теоретического и практического обучения для накопления ими первоначального профессионального опыта, проверки готовности будущего выпускника к самостоятельной трудовой деятельности.

Также преддипломная практика одновременно используется студентом для сбора фактического материала о производственной деятельности предприятия, учреждения, организации, необходимого для написания дипломного проекта.

№ п/п	Наименование вида работ	Сроки исполнения ¹
1.	Подбор, изучение и обработка литературы по проблематике дипломного проекта.	20 апреля т.г. 24 апреля т.г.
2.	Постановка задачи, составление плана и утверждение его руководителем дипломного проекта.	27 апреля т.г. 29 апреля т.г.
3.	Написание и представление руководителю первого раздела (обзор и постановка задачи)	30 апреля т.г. 05 мая т.г.
4.	Разработка и представление руководителю второго раздела (результаты проведенного исследования)	05 мая т.г. 19 мая т.г.
5.	Предоставление на утверждение готового чертежа по своему проекту	19 мая т.г.
6.	Анализ результатов, формирование выводов и разработка предложений.	19 мая т.г.
7.	Доработка дипломного проекта в соответствии с замечаниями руководителя.	02 июня т.г.
8.	Подготовка тезисов доклада для защиты дипломного проекта и обсуждение их с руководителем.	05 июня т.г.

¹ Даты написания дипломного проекта являются условными, дипломный руководитель имеет право сам корректировать даты.

9.	Ознакомление студента-дипломника с отзывом и рецензией на дипломный проект.	10 июня т.г.
10.	Подготовка к защите с учетом замечаний, сделанных в отзыве и рецензии, изготовление иллюстрированных плакатов.	11 июня т.г.
11.	Защита дипломного проекта	Согласно приказу

9. ТЕМАТИКА ДИПЛОМНЫХ ПРОЕКТОВ

1. Разработка сценариев для проверки безопасности веб-приложений методом тестирования на проникновение.
2. Разработка кейсов для тестирования на проникновение, связанных с криптографическими уязвимостями.
3. Разработка заданий для отработки методов обратной разработки (reverse engineering) в рамках пентеста.
4. Разработка кейсов для тестирования на проникновение, связанных с анализом стеганографии.
5. Разработка заданий для пентеста, основанных на методах проактивной безопасности (форензика).
6. Разработка заданий, моделирующих атаку внешнего злоумышленника (BlackBox-тестирование).
7. Построение архитектуры сети предприятия с применением NGFW для обеспечения многоуровневой безопасности.
8. Анализ методов обеспечения отказоустойчивости инфраструктуры в условиях распределенных атак типа «отказ в обслуживании» (DDoS).
9. Исследование методов защиты документированной информации ограниченного доступа от несанкционированного доступа.
10. Проектирование архитектуры системы информационной безопасности на базе программно-аппаратного комплекса VipNet.
11. Исследование применения алгоритмов шифрования на основе эллиптических кривых для защиты данных.
12. Сравнительный анализ эффективности протоколов транспортного уровня сетевой модели OSI.
13. Сравнительное моделирование и анализ стандартов спутникового вещания DVB-S и DVB-S2.
14. Внедрение и адаптация российской операционной системы Astra Linux в корпоративную сетевую инфраструктуру.
15. Анализ технологий туннелирования для организации защищенных каналов связи между распределенными филиалами предприятия.
16. Разработка и внедрение комплексной системы предотвращения утечек конфиденциальной информации (DLP) в организации.
17. Проектирование защищенной сетевой архитектуры предприятия с использованием межсетевых экранов нового поколения (NGFW).
18. Исследование методов и средств защиты информации в корпоративных локальных вычислительных сетях.

19. Разработка системы корпоративной безопасности для защиты центра обработки данных от внешних киберугроз.
20. Анализ криптографических механизмов защиты информации в системах электронной почты.
21. Разработка плана сетевой инфраструктуры предприятия с целью модернизации локальной вычислительной сети
22. Обеспечение конфиденциальности пользователей в сети Интернет через внедрение политик информационной безопасности.
23. Создание программного обеспечения для организации защищенного канала передачи данных.
24. Реализация алгоритма асимметричного шифрования RSA для криптографической защиты информации.
25. Имитационное моделирование и анализ характеристик беспроводных сетей стандарта Bluetooth.
26. Обеспечение защиты рабочих станций от современных киберугроз.
27. Анализ защищенности и уязвимостей криптографических протоколов SSL/TLS.
28. Исследование алгоритмов безопасного обмена данными с применением электронной цифровой подписи.
29. Анализ механизмов обеспечения безопасной передачи данных между конечными узлами сети.
30. Использование программных решений безопасности для защиты информационных систем организации.
31. Оценка рисков и исследование методов защиты информации при использовании облачных технологий.
32. Изучение современных и перспективных криптографических алгоритмов шифрования данных.
33. Проектирование защищенной корпоративной сети с применением межсетевых экранов.
34. Моделирование и исследование работы беспроводных сетей стандарта IEEE 802.11 (Wi-Fi).
35. Разработка дорожной карты по переходу предприятия на отечественное (импорто-независимое) программное обеспечение

10. ДОКУМЕНТЫ ВЫПУСКНИКА

Документы выпускника: диплом о среднем профессиональном образовании и Цифровой паспорт компетенций (ЦПК). Он формируется по итогам прохождения аттестации в форме демонстрационного экзамена.

Цифровой паспорт компетенций (ЦПК) – электронный документ, подтверждающий уровень владения профессиональными умениями и навыками. Документ формируется по итогам прохождения аттестации по образовательным программам среднего профессионального образования в форме демонстрационного экзамена (ДЭ). Результаты экзамена отражаются в ЦПК в виде набранных баллов в разрезе критериев/модулей задания.