

Министерство образования Белгородской области
Областное государственное автономное профессиональное
образовательное учреждение
«Белгородский индустриальный колледж»

Рассмотрена
На заседании педагогического
совета колледжа
Протокол № 3 от «01» октября 2024 г.

«Утверждаю»
Директор ОГАПОУ
«Белгородский индустриальный
колледж»
О. А. Шаталов
«01» октября 2024 г.
приказ № 339 от 01.10.2024г.

Программа государственной итоговой аттестации
2024–2025 учебного года по специальности
10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем
(базовый уровень)

Квалификация – Техник по защите информации

Белгород, 2024

Программа государственной итоговой аттестации разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем примерной основной образовательной программы (разработчик ПООП: Федеральное учебно-методическое объединение в системе среднего профессионального образования по укрупненной группе специальностей 10.00.00 «Информационная безопасность», 2017 год).

Согласовано:

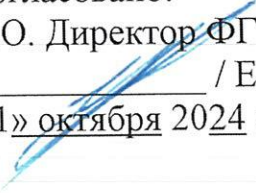
Заместитель директора по учебной работе колледжа

 /Н.В.Выручаева/

«01» октября 2024 г.

Согласовано:

И.О. Директор ФГУП филиал РТРС «Белгородский ОРТПЦ»

 / Е.Е. Щетинина /

«01» октября 2024 г.

Принята на заседании цикловой комиссии «Радивещание и системы диспетчерского управления»

Протокол № 2 от «30» сентября 2024г.

Председатель ЦК «Радивещание и системы диспетчерского управления»

 /Л.А.Чобану/

1 Общие положения

Программа государственной итоговой аттестации (далее ГИА) является частью основной профессиональной образовательной программы (далее – ОПОП) в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее ФГОС СПО) №1551, утвержденным 09.12.2016 г. по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» и является обязательной процедурой для выпускников, завершающих освоение ОПОП СПО в ОГАПОУ «Белгородский индустриальный колледж».

Целью государственной итоговой аттестации является установление соответствия уровня освоения компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся ФГОС СПО по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Программа ГИА по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» разработана цикловой комиссией электротехнических дисциплин и принята на заседании цикловой комиссии «30» сентября 2024 г., протокол № 2.

В соответствии с требованиями ФГОС СПО по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы, которая выполняется в виде дипломного проекта и демонстрационного экзамена.

К ГИА допускаются лица, выполнившие требования, предусмотренные курсом обучения по программе подготовки специалистов среднего звена по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» и успешно прошедшие все промежуточные аттестационные испытания по теоретическому и практическому этапам обучения, предусмотренные рабочим учебным планом, утвержденным директором колледжа, и согласованным с работодателем.

ГИА проводится с целью выявления соответствия уровня и качества подготовки выпускника требованиям ФГОС СПО, дополнительным требованиям к выпускнику по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» в ОГАПОУ «Белгородский индустриальный колледж» (далее Колледж) и готовности выпускника к профессиональной деятельности.

Основными целями выпускной квалификационной работы являются:

- систематизация и углубление теоретических и практических знаний, умений по специальности, полученных выпускником по программе подготовки специалистов среднего звена (ППССЗ) среднего профессионального образования в соответствии с ФГОС СПО, их применение при решении конкретных профессиональных задач;
- умение применять систематизированный опыт, знания и практические умения по избранной специальности при решении частных научно-исследовательских или практических задач;
- развитие навыков самостоятельной работы;

– овладение методикой исследования и экспериментирования при решении практических задач.

Общими требованиями к выпускной квалификационной работе являются:

- соответствие названию работы ее содержанию, целевая направленность;
- четкость построения, логическая последовательность изложения материала;
- глубина исследования и полнота освещения вопроса, убедительность аргументаций;
- краткость и точность формулировок, конкретность изложения результатов работы;
- доказательность выводов и обоснованность рекомендаций;
- грамотное оформление работы, согласно методическим указаниям к выпускной квалификационной работе, установленным ОГАПОУ «Белгородский индустриальный колледж».

Демонстрационный экзамен в рамках государственной итоговой аттестации обучающихся является независимой оценкой качества подготовки кадров, целью проведения данных аттестационных процедур является оценка освоения обучающимися образовательной программы (или её части) и соответствия уровня освоения общих и профессиональных компетенций требованиям:

- федеральных государственных образовательных стандартов СПО;
- профессиональных стандартов.

Организация процедур демонстрационного экзамена реализуется с учетом базовых принципов объективной оценки результатов подготовки рабочих кадров.

Предметом ГИА выпускников по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» в Колледже является:

- уровень образованности обучающегося, оцениваемый через систему индивидуальных образовательных достижений, включающих: учебные достижения в части освоения учебных дисциплин, МДК, профессиональных модулей;
- квалификацию как систему освоенных компетенций (общих и профессиональных), т.е. готовность выпускника к профессиональной деятельности.

Выпускник базовой подготовки с квалификацией техник готов к следующим видам профессиональной деятельности:

- Организовывать простые работы по техническому обслуживанию и ремонту электрического и электромеханического оборудования.
- Выполнять сервисное обслуживание бытовых машин и приборов
- Организовывать деятельность производственного подразделения.
- Выполнять работы по одной или нескольким профессиям рабочих, должностям служащих (приложение к ФГОС).

Выпускник должен обладать следующими общими и профессиональными компетенциями:

Код компетенции	Способности
Общие компетенции	
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, 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	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере.
Профессиональные компетенции в зависимости от видов профессиональной деятельности	
Эксплуатация информационно-телекоммуникационных систем и сетей	
ПК 1.1	Производить монтаж, настройку, проверку функционирования и конфигурирования 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.
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 несанкционированного доступа и специальных воздействий в оборудовании информационно-телекоммуникационных систем и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.
Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических 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.
Выполнение работ по профессии 14601 «Монтажник оборудования связи»	
ПК 4.1	Выполнять монтаж и настройку сетей проводного и беспроводного абонентского доступа в соответствии с действующими отраслевыми стандартами
ПК 4.2	Выполнять монтаж, демонтаж и техническое обслуживание кабелей связи и оконечных структурированных кабельных устройств в соответствии с действующими
ПК 4.3	Выполнять монтаж, демонтаж, первичную установку, мониторинг, диагностику инфокоммуникационных систем передачи в соответствии с действующими отраслевыми стандартами

Обучающиеся выпускного курса должны быть ознакомлены с программой ГИА не позднее 15 декабря (за 6 месяцев до защиты ВКР).

2 Нормативные ссылки

2.1 Федеральный закон РФ от 29.12.2012 г. №273-ФЗ «Об образовании в Российской Федерации».

2.2 Приказ Министерства просвещения Российской Федерации от 08 ноября 2021 г. №800 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования».

2.3 Приказ союза «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы» (Ворлдскиллс Россия)» от 26 марта 2019 г. N 26.03.2019-1 «Об утверждении перечня чемпионатов профессионального мастерства, проводимых союзом «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы» (Ворлдскиллс Россия)» либо международной организацией «WorldSkills International», результаты которых засчитываются в качестве оценки «отлично» по демонстрационному экзамену в рамках государственной итоговой аттестации» (в действующей редакции).

2.4 Приказ союза «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы» (Ворлдскиллс Россия)» от 28 февраля 2020 г. N 28.02.2020-1 «Об утверждении перечня компетенций ВСР».

2.5 Приказ союза «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы» (Ворлдскиллс Россия)» от 31 января 2019 г. N 31.01.2019-1 «Об утверждении Методики организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия» (в действующей редакции).

2.6 Приказ союза «Агентство развития профессиональных сообществ и рабочих кадров «Молодые профессионалы» (Ворлдскиллс Россия)» от 20 марта 2019 г. N 20.03.2019-1 «Об утверждении Положения об аккредитации центров проведения демонстрационного экзамена».

2.7 Распоряжение Министерства просвещения Российской Федерации от 1 апреля 2019 года № Р-42 «Об утверждении методических рекомендаций о проведении аттестации с использованием механизма демонстрационного экзамена (с изменениями на 1 апреля 2020 года);

2.8 Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» базовый уровень от 09.12.2016 г., регистрационный №1551.

2.9 Приказ Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н «Об утверждении профессионального стандарта 06.030 Специалист по защите информации в телекоммуникационных системах и сетях» (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449);

2.10 Постановление Правительства Российской Федерации от 14.06.2013 г. №464 «Об утверждении Типового положения об образовательном учреждении среднего профессионального образования (среднем специальном учебном заведении)».

2.11 Порядок проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования выпускников ОГАПОУ «Белгородский индустриальный колледж».

3 Виды государственной итоговой аттестации

Государственная итоговая аттестация проводится в форме защиты выпускной квалификационной работы, которая выполняется в виде дипломного проекта и демонстрационного экзамена.

4 Объем времени на подготовку и проведение государственной итоговой аттестации

На подготовку и проведение ГИА согласно ФГОС СПО по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» и в соответствии с календарным учебным графиком отводится 6 недель, в том числе:

- на подготовку выпускной квалификационной работы – 4 недели.
- на проведение защиты выпускной квалификационной работы – 2 недели.

Подготовка к выполнению заданий демонстрационного экзамена осуществляется в течение всего срока освоения образовательной программы.

5 Сроки проведения государственной итоговой аттестации

На государственную итоговую аттестацию отводится 216 часов (6 недель) из них 72 часа (2 недели) на защиту дипломного проекта.

Выполнение ВКР осуществляется с 19 мая по 14 июня 2025 г. (всего 4 недели.)

Защита ВКР проводится с 16.06.2025 по 28.06.2025 г. (всего 2 недели.)

Выполнение заданий демонстрационного экзамена проводится с 02.06.2025 по 14.06.2025 г. (всего 2 недели.)

6 Тематика и объем выпускной квалификационной работы

Тематика выпускной квалификационной работы должна иметь актуальность, новизну и практическую значимость в прикладной отрасли, отвечать современным требованиям развития науки, техники, производства, экономики, культуры и образования.

Темы ВКР должны подбираться по предложениям (заказам) предприятий, организаций отрасли, разрабатываться ведущими преподавателями ЦК специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» или могут быть предложены обучающимся при условии обоснования целесообразности разработки.

Тематика ВКР по специальности, исходные данные, структура, содержание определенной темы представлены в Приложении А.

Темы ВКР должны обсуждаться на заседании ЦК и утверждаться приказом директора Колледжа не позднее 07 апреля 2025 г.

Пояснительная записка должна иметь объем не менее 50 страниц формата А4, включая приложения.

По структуре ВКР состоит из теоретической и графической частей. В теоретической части дается теоретическое освещение темы на основе анализа имеющейся литературы.

Графическая часть может быть представлена методикой, расчетами, анализом экспериментальных данных в соответствии с видами профессиональной деятельности не менее 3-х листов формата А1. Содержание теоретической и графической частей определяется в зависимости от темы ВКР.

7 Необходимые материалы для выполнения ВКР

Приказ директора Колледжа об утверждении тем ВКР и назначении руководителей ВКР из числа работников отраслевых предприятий и организаций, ведущих преподавателей ЦК, а также консультантов по разделам и нормоконтроля

на основании протоколов заседания ЦК специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» не позднее 07 апреля 2025 г.

Индивидуальное задание, разработанное руководителем ВКР по утвержденной теме, где, в соответствующих разделах, консультантами формулируются конкретные требования этой части применительно к общей тематике данной ВКР. Задание на ВКР рассматривается ЦК, подписывается руководителем, заведующим отделением специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» и утверждается заместителем директора Колледжа по учебной работе не позднее 07 апреля 2025 г.

Выдача задания на ВКР студенту должна состояться не позднее 07 апреля 2025 г. (за две недели до начала преддипломной практики) и должна сопровождаться консультацией со стороны руководителя, в ходе которой разъясняются задачи, структура, объем работы, принцип разработки и оформления.

Бланк задания на ВКР по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» представлен в Приложении Б.

Календарный план работы над ВКР, составленный дипломником и утвержденный руководителем, где предусмотрены сроки выполнения всех отдельных частей ВКР, а также прохождение нормоконтроля, смотра ВКР и предварительной защиты. Пример заполнения календарного плана представлен в Приложении В.

Методические рекомендации по выполнению ВКР по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем», разработанные ведущими преподавателями – консультантами выпускающей ЦК.

При выполнении ВКР по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» рекомендуется использовать учебную и справочную литературу, перечень которой представлен в Приложении Д.

8 Условия подготовки и процедура проведения государственной итоговой аттестации

К государственной итоговой аттестации допускаются обучающиеся, не имеющие академических задолженностей и в полном объеме выполнившие учебный план или индивидуальный план по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Необходимым условием допуска к государственной итоговой аттестации является предоставление документов, подтверждающих освоение обучающимися общих и профессиональных компетенций при изучении теоретического материала и прохождения практик по каждому из основных видов деятельности.

Расписание государственной итоговой аттестации по специальности составляется ежегодно председателем ЦК и утверждается заместителем директора.

Расписание государственной итоговой аттестации включает в себя:

- график предзащиты дипломного проекта;
- график защиты дипломного проекта;
- график проведения демонстрационного экзамена.

8.1 Организация проведения демонстрационного экзамена

Демонстрационный экзамен является первым этапом ГИА. Оценку выполнения заданий ДЭ осуществляет экспертная группа, возглавляемая главным экспертом. Количество экспертов, входящих в состав экспертной группы, составляет 3 человека и определяется на основе условий, указанных в комплекте оценочной документации для ДЭ по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности», соответствующей профильному уровню.

Не допускается участие в оценивании заданий ДЭ экспертов, принимавших участие в обучении обучающихся или представляющих с ними одну образовательную организацию.

ДЭ проводится на площадке, аккредитованной в качестве центра проведения демонстрационного экзамена (далее - ЦПДЭ). Образовательная организация обеспечивает реализацию процедур ДЭ как части образовательной программы, в том числе выполнение требований охраны труда, безопасности жизнедеятельности, пожарной безопасности, соответствие санитарным нормам и правилам.

Общая информация для демонстрационного экзамена по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности» (КОД 1.1.) размещена на официальном сайте (<https://om.firpo.ru>)

Комплект оценочной документации (КОД) № 1.1 (приложение Г) разработан в целях организации и проведения демонстрационного экзамена по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности» и рассчитан на выполнение заданий продолжительностью 6 часов.

Демонстрационный экзамен по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности» включает в себя выполнение четырех модулей:

Модуль 1: Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз

Модуль 2: Технологии защиты узла и агентского мониторинга

Модуль 3: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

Модуль 4: Предотвращение инцидентов и управление событиями информационной безопасности

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 54,00.

Проведение ДЭ делится на несколько этапов.

Организационный и подготовительный этап. Образовательной организацией осуществляется определение и включение в состав программ государственной итоговой аттестации конкретных комплектов оценочной документации демонстрационного экзамена в рамках профессии, специальности среднего профессионального образования.

После утверждения программ государственной итоговой аттестации образовательным организациям необходимо провести оперативную работу по приведению центров проведения демонстрационного экзамена в соответствие с требованиями комплекта оценочной документации.

Разработка и утверждение плана проведения демонстрационного экзамена осуществляется в разрезе экзаменационных групп, профессий и специальностей среднего профессионального образования.

При проведении проверки центра проведения демонстрационного экзамена в подготовительный день осуществляется распределение рабочих мест между участниками демонстрационного экзамена методом случайной выборки (рекомендуется использовать алгоритм случайной подборки чисел в присутствии участников демонстрационного экзамена). Результаты распределения рабочих мест фиксируются в протоколе распределения рабочих мест, составляемом главным экспертом. Участники демонстрационного экзамена знакомятся с протоколом распределения рабочих мест под личную роспись. После осуществленного распределения рабочих мест следует проводить ознакомление участников демонстрационного экзамена непосредственно со своими рабочими местами.

После ознакомления участников демонстрационного экзамена со своими рабочими местами техническому эксперту следует проводить ознакомление участников демонстрационного экзамена с условиями оказания первичной медицинской помощи и требованиями охраны труда и безопасности производства. Факт ознакомления фиксируется личной подписью участника демонстрационного экзамена в протоколе распределения рабочих мест.

Проведение демонстрационного экзамена. Допуск к экзамену осуществляется главным экспертом на основании документа, удостоверяющего личность.

К демонстрационному экзамену допускаются участники демонстрационного экзамена, прошедшие ознакомление с требованиями охраны труда и безопасности производства, а также ознакомившиеся с рабочими местами.

К оценке выполнения заданий демонстрационного экзамена допускаются члены Экспертной группы, прошедшие ознакомление с требованиями охраны труда и техники безопасности, а также ознакомившиеся с распределением обязанностей.

Перед началом экзамена членами Экспертной группы, участникам демонстрационного экзамена разъясняются их права и обязанности, обращается внимание на установленные запреты и ограничения в период проведения демонстрационного экзамена, включая необходимость недопущения у указанных лиц запрещенных средств и предметов и необходимость их сдачи на период нахождения в центре проведения демонстрационного экзамена во время проведения демонстрационного экзамена.

Главным экспертом выдаются задания демонстрационного экзамена каждому участнику в бумажном виде, членам экспертной группы дополнительно критерии оценивания в разрезе установленного распределения обязанностей и состава экзаменационных групп, дополнительные инструкции к ним (при наличии), а также разъясняются правила поведения во время демонстрационного экзамена.

После получения экзаменационного задания и дополнительных материалов к нему, участникам предоставляется время на ознакомление и возникающие вопросы, которое не включается в общее время проведения экзамена и составляет не менее 15 минут.

По завершению процедуры ознакомления с заданием участники подписывают протокол распределения рабочих мест и ознакомления участников с документацией, оборудованием и рабочими местами, оформляемый по каждой экзаменационной группе. Протокол проведения демонстрационного экзамена подписывается главным экспертом и экспертами после завершения демонстрационного экзамена, участники демонстрационного экзамена протокол проведения демонстрационного экзамена не подписывают.

К выполнению экзаменационных заданий участники приступают после указания главного эксперта и фиксации времени начала проведения демонстрационного экзамена в протоколе проведения демонстрационного экзамена.

Организация деятельности экспертной группы по оценке выполнения заданий демонстрационного экзамена осуществляется главным экспертом.

Главный эксперт обязан находиться в центре проведения демонстрационного экзамена в течение всего времени проведения демонстрационного экзамена и завершения процедуры оценивания результатов демонстрационного экзамена.

В ходе проведения экзамена участникам запрещаются контакты с другими участниками или членами экспертной группы без разрешения главного эксперта если иное не предусмотрено требованиями комплекта оценочной документации и не связано с обеспечением выполнения требований охраны труда и производственной безопасности.

В случае возникновения несчастного случая или болезни экзаменуемого главным экспертом незамедлительно принимаются действия по привлечению ответственных лиц от ЦПДЭ для оказания медицинской помощи и уведомляется представитель образовательной организации, которую представляет экзаменуемый (далее - сопровождающее лицо). Далее с привлечением сопровождающего лица принимается решение об отстранении экзаменуемого от дальнейшего участия в экзамене или назначении ему дополнительного времени в пределах времени, предусмотренного планом проведения демонстрационного экзамена и требованиями комплекта оценочной документации.

В случае отстранения, экзаменуемого от дальнейшего участия в экзамене ввиду болезни или несчастного случая, ему начисляются баллы за любую завершённую работу по его желанию.

Вышеуказанные случаи подлежат обязательной регистрации в Протоколе проведения демонстрационного экзамена.

Участник, нарушивший правила поведения на экзамене и чье поведение мешает процедуре проведения экзамена, получает предупреждение с занесением в протокол проведения демонстрационного экзамена. Потерянное время при этом не компенсируется участнику, нарушившему правило.

После повторного предупреждения участник может быть удален из центра проведения демонстрационного экзамена если его действия (бездействия) влекут нарушение объективности демонстрационного экзамена, мешают другим участникам демонстрационного экзамена, нарушают требования охраны труда и безопасности производства.

В процессе выполнения заданий экзаменуемые обязаны неукоснительно соблюдать требования охраны труда и безопасности производства. Несоблюдение экзаменуемыми указанных требований может привести к потере баллов в соответствии с критериями оценки. Систематическое и грубое нарушение норм безопасности может привести к временному или окончательному отстранению экзаменуемого от выполнения экзаменационных заданий.

Процедура проведения демонстрационного экзамена проходит с соблюдением принципов объективности, справедливости и открытости. Вся информация и инструкции по выполнению заданий экзамена от главного эксперта и членов экспертной группы, в том числе с целью оказания необходимой помощи, должны

быть четкими и недвусмысленными, не дающими преимущества тому или иному участнику.

Обеспечение соблюдения требований охраны труда и безопасности производства, сохранение жизни и здоровья участников демонстрационного экзамена и других лиц, привлеченных к организации и проведению демонстрационного экзамена, являются высшим приоритетом и не могут уступать в пользу каких-либо иных факторов и обстоятельств.

Вмешательство иных лиц, которое может помешать участникам завершить экзаменационное задание, не допускается.

Оценка не должна выставляться в присутствии участника демонстрационного экзамена, если иное не предусмотрено комплектом оценочной документации.

Процедура оценивания результатов выполнения экзаменационных заданий осуществляется в соответствии требованиями комплекта оценочной документации, критериями оценивания.

Баллы выставляются членами Экспертной группы вручную с использованием предоставленных главным экспертом ведомостей.

Одно из главных требований при выполнении оценки заданий демонстрационного экзамена - это обеспечение равных условий для всех участников демонстрационного экзамена.

После всех оценочных процедур, главным экспертом и членами экспертной группы производится сверка баллов, их внесение в протокол проведения демонстрационного экзамена

Если демонстрационный экзамен проводится как форма государственной итоговой аттестации, к сверке привлекается член государственной экзаменационной комиссии, присутствовавший в центре проведения демонстрационного экзамена и не входящий в состав экзаменационной группы.

Оригинал протокола проведения демонстрационного экзамена передается в государственную экзаменационную комиссию для выставления итоговых оценок по результатам государственной итоговой аттестации, в дальнейшем хранится в образовательной организации.

8.2 Выполнение ВКР

Выполнение ВКР осуществляется обучающимся с соблюдением сроков, установленных в календарном плане. В случае нарушения сроков выполнения одного из этапов ВКР руководитель ставит в известность заведующего отделением по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Общее руководство и контроль за ходом выполнения осуществляет заведующий отделением специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» преподаватели ЦК и руководитель ВКР.

Руководитель и консультанты составных частей ВКР проводят консультации обучающихся в соответствии с разработанным графиком консультаций и индивидуальным календарным планом обучающегося. Для консультирования одного обучающегося должно быть предусмотрено не более двух часов в неделю.

Завершающим этапом выполнения ВКР является нормоконтроль. Его целью является соблюдение обучающимися всех требований ЕСКД, ЕСТД, ЕСТП и

ЕСДП при оформлении ВКР. Нормоконтроль проводится при 100%-ной готовности ВКР. При успешном прохождении нормоконтроля контролер ставит подписи на титульном листе, на первом листе пояснительной записки и на всех листах графической части с приложениями. Дипломные проекты, не прошедшие нормоконтроль, к защите не допускаются.

Срок прохождения нормоконтроля – до 05 июня 2025 г.

После прохождения нормоконтроля консультанты знакомятся с содержанием соответствующих разделов выполненной ВКР и при отсутствии замечаний подписывают титульный лист пояснительной записки.

Срок получения подписей консультантов – до 05 июня 2025 г.

ВКР, выполненная в полном объеме в соответствии с заданием, подписанная выпускником, нормоконтролем, консультантами по отдельным разделам, передается руководителю ВКР для заключительного просмотра. Руководитель ставит подписи на титульном листе, на первом листе пояснительной записки и на всех чертежах с приложениями, затем пишет отзыв, где отражает качество содержания выполненной ВКР, проводит анализ хода ее выполнения, дает характеристику работы выпускника и выставляет оценку уровня подготовленности студента к защите ВКР.

Отзыв руководителя ВКР о работе выпускника над дипломным проектом является основанием для допуска студента к рецензированию ВКР.

Срок получения обучающимся отзыва руководителя ВКР – до 07 июня 2025 г.

Решением ЦК в соответствии с приказом директора Колледжа об утверждении рецензентов ВКР обучающийся передает выполненный дипломный проект на рецензию.

Рецензирование выполненных ВКР осуществляется специалистами из числа работников отраслевых предприятий и организаций, а также преподавателей, хорошо владеющих вопросами, связанными с тематикой ВКР.

Рецензия должна включать:

- заключение о соответствии ВКР заданию на нее;
- оценку качества выполнения каждого раздела ВКР;
- оценку степени разработки перспективных вопросов, оригинальности и практической значимости ВКР;
- оценку ВКР.

Срок сдачи ВКР на рецензию – 09 июня 2025 г.

Срок рецензирования ВКР – три дня (до 11 июня 2025 г.).

Рецензент тщательно знакомится с пояснительной запиской и графическими материалами ВКР, ставит подписи на титульном листе. Затем составляет обоснованную критическую рецензию, где отражает соответствие и качество содержания выполненной ВКР, проводит анализ обоснованности предлагаемых технических решений, указывает достоинства и недостатки ВКР, выставляет оценку по стандартной шкале («отлично», «хорошо», «удовлетворительно» и «неудовлетворительно») и дает заключение о возможности присвоения автору ВКР соответствующей квалификации.

По окончании срока рецензирования (11 июня) обучающийся знакомится с содержанием рецензии, забирает ВКР у рецензента и проходит процедуру предварительной защиты дипломного проекта. Внесение изменений в ВКР после получения рецензии не допускается. Во время защиты обучающийся вправе согласиться или не согласиться с рецензией, обосновав свой выбор.

Проведение предзащит и обзорных лекций по профилирующим дисциплинам планируется за неделю до начала работы ГЭК – **9-14 июня 2025 г.**

Допуск к ГИА оформляется приказом директора Колледжа на основании результатов учебной деятельности, прохождения учебной, производственной, преддипломной практики и готовности ВКР.

На организационном собрании обучающиеся выпускного курса знакомятся с графиком работы Государственной экзаменационной комиссии (далее ГЭК) для проведения ГИА, составленным заведующим отделением по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» согласованным с заместителем директора Колледжа по учебной работе и утвержденным директором Колледжа – **9 июня** (за 5 дней до защиты ВКР).

Обучающиеся выпускного курса сдают отзыв руководителя ВКР и рецензию на ВКР заведующему отделением специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» для предоставления их в ГЭК до **14 июня 2025 г.**

8.3 Необходимые материалы для проведения государственной итоговой аттестации (защита ВКР)

1. Программа ГИА;
2. Приказ учредителя Колледжа о назначении председателя ГЭК;
3. Приказ директора Колледжа об утверждении состава ГЭК;
4. Приказ директора Колледжа о допуске к защите ВКР обучающихся специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» успешно завершивших обучение по программе подготовки специалистов среднего звена (по результатам промежуточных аттестаций по дисциплинам, профессиональным модулям, междисциплинарным курсам и прохождения всех видов производственной практики, предусмотренных учебным планом).
5. График защиты ВКР, составленный заведующим отделением по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» согласованный с заместителем директора Колледжа по учебной работе и утвержденный директором Колледжа к **31 мая 2025 г.** (за две недели до защиты ВКР).
6. Протоколы заседаний ГЭК.
7. Выписку из учебной части об оценках каждого выпускника по всем дисциплинам, профессиональным модулям, междисциплинарным курсам, практикам, курсовым проектам.
8. В ГЭК обучающимся предоставляются следующие материалы и документы:
 - 8.1 Задание на дипломное проектирование.
 - 8.2 Пояснительная записка ВКР.
 - 8.3 Графическая часть ВКР.
 - 8.4 Отзыв руководителя ВКР о работе обучающегося над дипломной работой (сданный ранее заведующему отделением специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».
 - 8.5 Рецензия на ВКР (сданная ранее заведующему отделению специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

8.4 Проведение государственной итоговой аттестации (защита ВКР)

Для проведения ГИА (защиты ВКР) создается государственная аттестационная комиссия численностью не менее 5 человек. В состав ГЭК по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» входят:

- председатель ГЭК;
- заместитель председателя ГЭК;
- члены комиссии;
- заведующий отделением;
- преподаватели специальных дисциплин выпускающей ЦК специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»
- ответственный секретарь ГЭК.

Председатель ГЭК утверждается приказом учредителя Колледжа за 6 месяцев до начала работы ГЭК. Остальной состав ГЭК утверждается приказом директора Колледжа за 2 месяца до начала работы ГЭК.

Расписание проведения ГИА выпускников утверждается директором Колледжа и доводится до сведения обучающихся не позднее, чем за две недели до начала работы ГЭК.

Работа ГЭК начинается в первый день проведения ГИА и заканчивается в последний день проведения ГИА. На первом заседании ГЭК председатель представляет комиссию и объявляет начало и порядок проведения ГИА

Защита ВКР производится на открытом заседании ГЭК.

На защиту ВКР обучающемуся отводится до 45 минут. Процедура ГИА включает доклад обучающегося (не более 15-20 минут), вопросы членов комиссии, ответы обучающегося на поставленные вопросы, чтение отзыва и рецензии. Может быть предусмотрено выступление руководителя ВКР, рецензента, если они присутствуют на заседании ГЭК.

Решение ГЭК принимается на закрытом заседании большинством голосов членов комиссии, участвующих в заседании (при равном числе голосов голос председателя является решающим).

Заседания ГЭК протоколируются. В протоколе записываются: итоговая оценка ВКР, присуждение квалификации и особое мнение членов комиссии. Протоколы заседаний ГЭК подписываются председателем, всеми членами и секретарем комиссии. Ведение протоколов осуществляется в прошнурованных книгах, листы которых пронумерованы. Книга протоколов заседаний ГЭК хранится в делах колледжа в течение установленного срока.

По окончании каждого заседания ГИА выпускники приглашаются в аудиторию, где председателем оглашается решение ГЭК.

Система оценок ГИА

– пятибалльная.

Присвоение соответствующей квалификации выпускнику и выдача ему документа о среднем профессиональном образовании осуществляется при условии успешного прохождения государственной итоговой аттестации.

Студенту, имеющему оценку «отлично» не менее чем по 75 процентам дисциплин учебного плана, оценку «хорошо» по остальным дисциплинам и

прошедшему все установленные учебным планом виды аттестационных испытаний, входящих в итоговую государственную аттестацию:

- демонстрационный экзамен с оценкой «хорошо» или «отлично»;
- защита ВКР с оценкой «отлично» выдается диплом с отличием.

При оценке «неудовлетворительно» обучающийся получает академическую справку установленного образца. ГЭК принимает решение о возможности повторной защиты обучающимся той же ВКР, либо признать целесообразным закрепление за ним нового задания на ВКР и определить срок новой защиты, но не ранее, чем через год.

Решение ГЭК о присвоении квалификации выпускникам, прошедшим ГИА, и выдаче соответствующего документа об образовании объявляется приказом директора колледжа.

По окончании защит ВКР ГЭК составляет ежегодный отчет о работе, который обсуждается на заседании выпускающей ЦК.

В отчете отражается следующая информация:

- общие положения;
 - качественный состав ГЭК;
 - вид ГИА обучающихся по ОПОП СПО;
 - характеристика общего уровня подготовки обучающегося по специальности
- 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем»

- анализ результатов по ГИА;
- недостатки в подготовке обучающихся по специальности;
- выводы и предложения.

Во время защиты ВКР обучающийся может использовать:

- выполненную графическую часть ВКР;
- пояснительную записку ВКР;
- составленный ранее доклад или тезисы своего выступления.

Проверка уровня профессиональной подготовленности обучающегося осуществляется через ответы на дополнительные вопросы по теме ВКР.

При определении окончательной оценки по защите ВКР учитываются:

- сообщение (доклад) по теме ВКР;
- ответы на вопросы;
- оценка рецензента;
- отзыв руководителя;
- выступления рецензента и руководителя (по желанию).

9 Критерии оценки

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

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

Перевод полученного количества баллов в оценки осуществляется государственной экзаменационной комиссией с обязательным участием главного эксперта.

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100%. Перевод баллов в оценку осуществляется на основании Приказа ОГАПОУ «Белгородский индустриальный колледж» «О переводной шкале баллов».

В основе оценки ВКР лежит пятибалльная система. При проведении процедуры защиты ВКР необходимо учитывать следующие критерии:

- уровень освоения обучающимся материала, предусмотренного рабочими программами дисциплин;
- уровень практических умений, продемонстрированных выпускником при выполнении ВКР;
- уровень знаний и умений, позволяющий решать производственные задачи при выполнении ВКР;
- обоснованность, чёткость, лаконичность изложения сущности темы ВКР;
- гибкость и быстрота мышления при ответах на поставленные при защите ВКР вопросы.

Оценка уровня сформированных компетенций в целом по основной профессиональной образовательной программе выпускника колледжа проводится ГЭК поэтапно с учетом оценок:

- общих и профессиональных компетенций выпускника колледжа, продемонстрированных при выполнении ВКР;
- общих и профессиональных компетенций по ведомости успеваемости за весь период обучения, подготовленной заведующим отделением, на основании результатов промежуточной аттестации по учебным дисциплинам, МДК, профессиональным модулям, практикам;
- общих и профессиональных компетенций выпускника, представленных в портфолио студентов на заседании предметно-цикловой комиссии специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем» и оформленные в ведомости с указанием набранных баллов.

Уровень знаний обучающегося определяется следующими оценками:

- «отлично»;
- «хорошо»;
- «удовлетворительно»;
- «неудовлетворительно».

Оценка «отлично» ставится при соблюдении следующих условий:

- представленная на ГИА ВКР выполнена в полном соответствии с техническим заданием согласно Рекомендациям по оформлению выпускной квалификационной работы для обучающихся ОГАПОУ «Белгородский индустриальный колледж», имеет подписи выпускника, руководителя ВКР, консультантов по разделам ВКР, нормоконтроля и рецензента в основных надписях всех входящих в ВКР документов;
- изложение (доклад) поставленной задачи и способов ее решения в представленной к защите ВКР дано обучающимся грамотно, четко и аргументировано;
- на все поставленные по тематике данной ВКР вопросы даны исчерпывающие ответы. При этом речь обучающегося отличается логической последовательностью, четкостью, прослеживается умение делать выводы, обобщать знания и практический опыт;

- во время защиты обучающийся демонстрирует знание проблемы, раскрывает пути решения производственных задач, имеет свои суждения по различным аспектам представленной ВКР.

Оценка «хорошо» ставится при соблюдении следующих условий:

- представленная на ГИА ВКР выполнена в полном соответствии с техническим заданием согласно Рекомендациям по оформлению выпускной квалификационной работы для обучающихся ОГАПОУ «Белгородский индустриальный колледж», имеет подписи выпускника, руководителя ВКР, консультантов по разделам ВКР, нормоконтроля и рецензента в основных надписях всех входящих в ВКР документов;

- изложение (доклад) поставленной задачи и способов ее решения в представленной на защите ВКР дано обучающимся грамотно, четко и аргументировано;

- на все поставленные по тематике данной ВКР вопросы даны ответы. При этом речь обучающегося отличается логической последовательностью, четкостью, прослеживается умение делать выводы, обобщать знания и практический опыт;

- возможны некоторые упущения при ответах, однако основное содержание вопроса раскрыто полно.

Оценка «удовлетворительно» ставится при соблюдении следующих условий:

- представленная на ГИА ВКР выполнена в полном соответствии с техническим заданием согласно Рекомендациям по оформлению выпускной квалификационной работы для обучающихся ОГАПОУ «Белгородский индустриальный колледж», имеет подписи выпускника, руководителя ВКР, консультантов по разделам ВКР, нормоконтроля и рецензента в основных надписях всех входящих в ВКР документов; ВКР документов;

- доклад на тему представленной на защите ВКР не раскрывает сути поставленной задачи и не отражает способов ее решения;

- на поставленные по тематике данной ВКР вопросы даны неполные, слабо аргументированные ответы;

- не даны ответы на некоторые вопросы, требующие элементарных знаний учебных дисциплин;

- отказ от ответов демонстрирует неумение обучающегося применять теоретические знания при решении производственных задач.

Оценка «неудовлетворительно» ставится в том случае, если:

- представленная на ГИА ВКР выполнена в полном соответствии с заданием согласно Порядку проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования выпускников ОГАПОУ «Белгородский индустриальный колледж», имеет подписи выпускника, руководителя ВКР, консультантов по разделам ВКР, нормоконтроля и рецензента в основных надписях всех входящих в ВКР документов;

- доклад на тему представленной на защите ВКР не раскрывает сути поставленной задачи и не отражает способов ее решения;

- обучающийся не понимает вопросов по тематике данной ВКР и не знает ответы на теоретические вопросы, требующие элементарных знаний учебных дисциплин.

При выставлении общей оценки за выполнение и защиту ВКР комиссия учитывает отзыв руководителя проекта о ходе работы обучающегося над темой и оценку ВКР рецензентом.

10 Структура выпускной квалификационной работы

Темы ВКР должны иметь практико-ориентированный характер и соответствовать содержанию одного или нескольких профессиональных модулей. Перечень тем по ВКР:

- разрабатывается преподавателями МДК в рамках профессиональных модулей;
- рассматривается на заседаниях цикловой комиссии;
- утверждается после предварительного положительного заключения работодателей (п.8.6 ФГОС СПО).

Структура выпускной квалификационной работы:

Введение

1. Общая часть

- теоретическая часть

2. Расчетная часть

- расчетно-конструкторская часть
- организационная часть
- экономическая часть
- мероприятия по техники безопасности

Заключение, рекомендации по использованию полученных результатов

Список используемых источников

Приложения

Во введении обосновывается актуальность и практическая значимость выбранной темы, формулируются цель и задачи.

При работе над **теоретической частью** определяются объект и предмет ВКР, круг рассматриваемых проблем. Проводится обзор используемых источников, обосновывается выбор применяемых методов, технологий и др. Работа выпускника над теоретической частью позволяет руководителю оценить следующие общие компетенции:

- понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес;
- осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;
- самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации

Работа над вторым разделом должна позволить руководителю оценить уровень развития следующих общих компетенций:

- организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество;
- принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность;

- владеть информационной культурой, анализировать и оценивать информацию с использованием информационно-коммуникационных технологий
- ориентироваться в условиях частой смены технологий в профессиональной деятельности

Заключение содержит выводы и предложения с их кратким обоснованием в соответствии с поставленной целью и задачами, раскрывает значимость полученных результатов.

11 Условия реализации программы итоговой государственной аттестации

11.1 Требования к минимальному материально-техническому обеспечению при подготовке и защите выпускной квалификационной работы

- **при выполнении выпускной квалификационной работы** реализация программы ГИА предполагает наличие кабинета подготовки к итоговой аттестации.

Оборудование кабинета:

- рабочее место для консультанта-преподавателя;
- компьютер, принтер;
- рабочие места для обучающихся;
- лицензионное программное обеспечение общего и специального назначения;
- график проведения консультаций по выпускным квалификационным работам;
- график поэтапного выполнения выпускных квалификационных работ;
- комплект учебно-методической документации.

- **при защите выпускной квалификационной работы** отводится специально подготовленный кабинет.

Оснащение кабинета:

- рабочее место для членов Государственной аттестационной комиссии;
- компьютер, мультимедийный проектор, экран;
- лицензионное программное обеспечение общего и специального назначения.

11.2 Требования к минимальному материально-техническому обеспечению при подготовке и процедуре выполнения заданий демонстрационного экзамена

Инфраструктура и материально-техническое оснащение мастерской по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности» должны соответствовать инфраструктурным листам по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности» и планам застройки мастерской. Инфраструктурные листы по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности» и планы застройки мастерских актуализированы Институтом развития профессионального образования и размещаются на сайте, расположенном по адресу <https://om.firpo.ru/competencies> в информационно-телекоммуникационной сети

"Интернет", не позднее чем за 6 месяцев до проведения демонстрационного экзамена.

12 Информационное обеспечение ГИА

1. Программа итоговой государственной аттестации.
2. Методические рекомендации по разработке выпускных квалификационных работ.
3. Федеральные законы и нормативные документы.
4. Оценочные материалы для демонстрационного экзамена.
5. Стандарты на справочные материалы.
6. Литература по специальности.
7. Периодические издания по специальности.

13 Кадровое обеспечение ГИА

Требования к квалификации педагогических кадров, обеспечивающих руководство выполнением выпускных квалификационных работ: наличие высшего профессионального образования, соответствующего профилю специальности.

Требование к квалификации руководителей ГИА от организации (предприятия): наличие высшего профессионального образования, соответствующего профилю специальности.

Оценку выполнения заданий демонстрационного экзамена осуществляют эксперты по компетенции F7 «Корпоративная защита от внутренних угроз информационной безопасности», владеющие методикой оценки демонстрационного экзамена и внесенные в реестр экспертов демонстрационного экзамена.

14 Апелляция результатов ГИА

По результатам государственной итоговой аттестации, проводимой с применением механизма демонстрационного экзамена, выпускник имеет право подать в апелляционную комиссию письменное апелляционное заявление о нарушении, по его мнению, установленного порядка проведения государственной итоговой аттестации и (или) несогласии с ее результатами.

Апелляция подается лично выпускником или родителями (законными представителями) несовершеннолетнего выпускника в апелляционную комиссию образовательной организации.

Апелляция о несогласии с результатами государственной итоговой аттестации выдается не позднее следующего рабочего дня после объявления результатов государственной итоговой аттестации.

Апелляция рассматривается апелляционной комиссией не позднее трех рабочих дней с момента ее поступления. На заседание апелляционной комиссии приглашается председатель соответствующей государственной экзаменационной комиссии. Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции. С несовершеннолетним выпускником имеет право присутствовать один из родителей (законных представителей). Указанные лица должны иметь при себе документы, удостоверяющие личность.

Рассмотрение апелляции не является пересдачей государственной итоговой аттестации. В результате рассмотрения апелляции о несогласии с результатами

государственной итоговой аттестации апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата государственной итоговой аттестации либо об удовлетворении апелляции и выставлении иного результата государственной итоговой аттестации. Решение апелляционной комиссии не позднее следующего рабочего дня передается в государственную экзаменационную комиссию.

Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов государственной итоговой аттестации выпускника и выставления новых.

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

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

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

Состав апелляционной комиссии утверждается образовательной организацией одновременно с утверждением состава государственной экзаменационной комиссии. На заседание апелляционной комиссии приглашается председатель соответствующей государственной экзаменационной комиссии.

Примерная тематика ВКР

- разработка модели угроз НСД на предприятии;
- разработка модели угроз безопасности ИС персональных данных на предприятии;
- проектирование комплексной модели защиты информации на предприятии;
- оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов;
- проектирование комплексной системы защиты информации на предприятии;
- разработка комплексной системы безопасности персональных данных;
- проектирование подсистемы технической защиты информации;
- организация защиты информации от утечки по техническим каналам;
- разработка системы безопасности АС;
- проектирование комплексной (интегрированной) системы безопасности для объекта;
- проектирования общей системы оповещения пожарной сигнализации;
- проектирование системы охранно-пожарной сигнализации для объекта;
- проектирование системы пожарной сигнализации для объекта;
- проектирование системы видеонаблюдения для объекта;
- проектирование системы автоматического пожаротушения для объекта;
- проектирование системы контроля и управления доступом для объекта;
- проектирование системы сбора и обработки информации для объекта;
- организация предоставления мультисервисных услуг на сети связи;
- реализация концепции NGN на ССОП.

Министерство образования Белгородской области
Областное государственное автономное профессиональное
образовательное учреждение
«Белгородский индустриальный колледж»

УТВЕРЖДАЮ
Заместитель директора
по учебной работе
«___» _____ 20__ г.
_____/Н.В. Выручаева/

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ДИПЛОМНЫЙ ПРОЕКТ (ДИПЛОМНУЮ РАБОТУ)

Обучающемуся _____ группы _____
Специальность 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Тема проекта (работы) _____ утве
ржденная приказом директора от «__» _____ 20__ г. № _____

1. Исходные данные к проекту (работе)

2.

Перечень вопросов, подлежащих разработке

3. Перечень графического материала проекта (с указанием обязательных чертежей)

Пример оформления календарного плана
КАЛЕНДАРНЫЙ ПЛАН

ВКР обучающегося _____

№ п/п	Наименование этапов ВКР	Срок выполнения этапов	Примечания
1	Ознакомление с заданием на ВКР		
2	Составление плана ВКР. Определение цели, задач, гипотез, объекта, предмета исследования		
3	Работа над теоретической частью ВКР. Анализ литературы по проблеме		
4	Работа над практической частью ВКР. Сбор информации и систематизация материала во время прохождения преддипломной практики		
5	Оформление пояснительной записки		
6	Проверка содержания полностью выполненной ВКР руководителем		
7	Утверждение (на подпись) ВКР руководителем. Получение отзыва руководителя ВКР		
8	Нормоконтроль		
9	Предварительная защита, получение допуска на защиту ВКР		
10	Рецензирование ВКР. Утверждение (на подпись) ВКР зав. отделением и зам. директора по УР.		

Дата выдачи задания «__» ____ 20__ г.

Срок сдачи законченного проекта «__» ____ 20__ г.

Задание принял к исполнению «__» ____ 20__ г.

Студент дипломник _____ /

Руководитель _____ /

Рассмотрено на заседании ЦК протокол № ____ от ____ 20__ г.

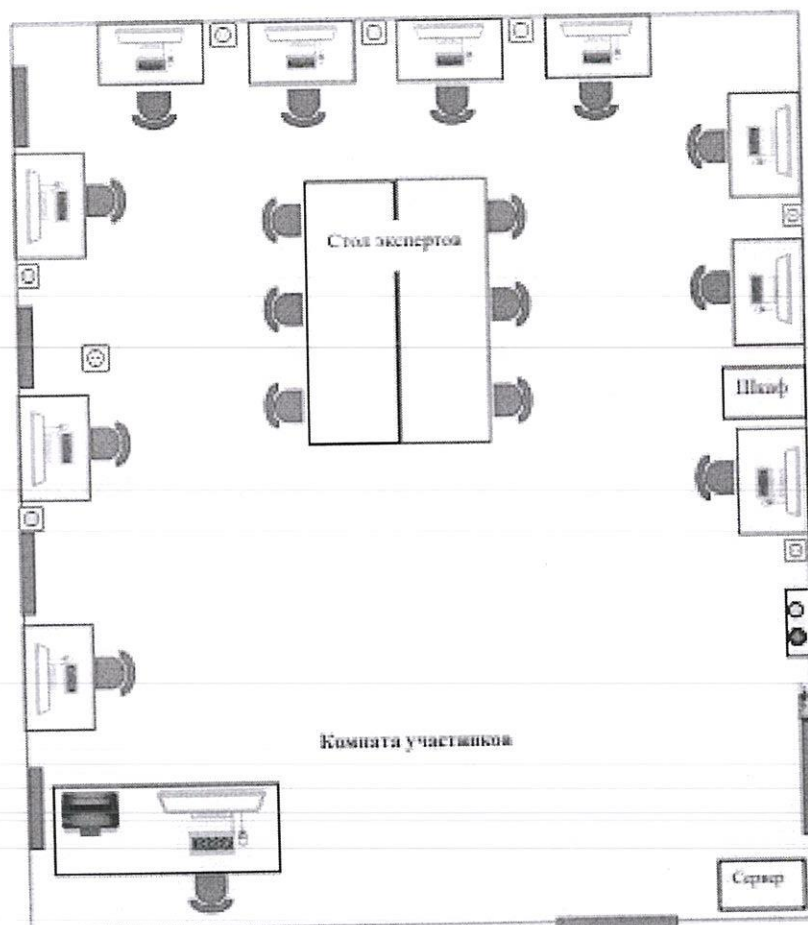
Председатель ЦК _____ /

Заведующий отделением _____ /

Комплект оценочной документации по коду 1.1-2023-2025

Образец задания

Образец задания для демонстрационного экзамена по комплекту оценочной документации 1.1-2023-2025.



Общие требования.

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.

После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 1».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задача 1–1 и т. д.)

Задания на разработку политик можно выполнять в любом порядке.

При выполнении задания ставятся следующие цели:

Настроить систему предотвращения утечек для правильного функционирования политик безопасности.

Произвести настройку технологий, используемых в политиках безопасности, а именно: лингвистический анализ, регулярные выражения, эталонные документы, графические объекты, выгрузки из баз данных.

Произвести верную настройку объектов защиты, верно выстроить логику срабатывания.

Разработать политики безопасности для корректного срабатывания политик, указать направления передачи, уровень нарушений, вердикты, теги.

Произвести проверку работоспособности политик.

Задание модуля 1.

Задача 1 Выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты. Стоит учесть, что стандартные политики и объекты можно модифицировать под свои нужды.

Задача 2 Создать локальную группу пользователей «Сотрудники под наблюдением». Добавьте в нее трех любых пользователей.

Задача 3 Создать список веб-ресурсов «Доверенные домены». Добавить в список следующие сайты: filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Список рекомендуемых источников для написания
выпускной квалификационной работы

Федеральные законы и нормативные документы

1. ГОСТ 12.1.004-91. ССБТ. Пожарная безопасность. Общие требования

- | | |
|---------------------------|---|
| 2. <u>РД-ССПБ-1</u> | Требования к органам по сертификации и порядок их аккредитации |
| 3. <u>РД-ССПБ-3</u> | Требования к экспертам и порядок их аттестации |
| 4. <u>РД-ССПБ-4</u> | Требования к порядку ведения государственного реестра участников и объектов системы сертификации в области пожарной безопасности в Российской Федерации |
| 5. <u>РД-ССПБ-5</u> | Формы основных документов, применяемых в системе сертификации в области пожарной безопасности в Российской Федерации |
| 6. <u>РД-ССПБ-6</u> | Положение о центральном органе системы сертификации в области пожарной безопасности в Российской Федерации |
| 7. <u>РД 009-01-96</u> | Установки пожарной автоматики. Правила технического содержания |
| 8. <u>РД 009-02-96</u> | Установки пожарной автоматики техническое обслуживание и планово-предупредительный ремонт |
| 9. <u>РД 03-410-01</u> | Инструкция по проведению комплексного технического освидетельствования изотермических резервуаров сжиженных газов |
| 10. <u>РД 03-418-01</u> | Методические указания по проведению анализа риска опасных производственных объектов |
| 11. <u>РД 25.952-90</u> | Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Порядок разработки задания на проектирование. |
| 12. <u>РД 25.953-90</u> | Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Обозначения условные графические элементов связи. |
| 13. <u>Р 78.36.002-99</u> | Выбор и применение телевизионных систем видеоконтроля. |
| 14. <u>Р 78.36.007-99</u> | Рекомендации
Выбор и применение средств охранно-пожарной сигнализации и средств технической укреплённости для оборудования объектов |

Основные источники

1. Антоненко А.А., Буцынская Т.А. Членов А.Н. Основы эксплуатации систем комплексного обеспечения безопасности объектов. Под общей ред. А.Н.Членова. М.: ООО "Издательство "Пожнаука", 2020.

2. Бабуров В.П., Бабуринов В.В., Фомин В.И. Технические средства систем охранной и пожарной сигнализации. М.: ООО "Издательство "Пожнаука", 2020.
3. Ворона В.А., Тихонов В.А. Концептуальные основы создания и применения системы защиты объектов. М.: ООО Горячая линия телеком, 2020 г.
4. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. М.: ООО Горячая линия телеком, 2021 г.
5. Ворона В.А., Тихонов В.А. Комплексные (интегрированные) системы обеспечения безопасности. – М.: Горячая линия–Телеком, 2021. – 160 с.
6. Ворона В. А., Тихонов В. А. Технические средства наблюдения в охране объектов. – М.: Горячая линия–Телеком, 2019. – 184 с.
7. Ворона В. А., Тихонов В. А. Технические системы охранной и пожарной сигнализации. – М.: Горячая линия–Телеком, 2019. – 376 с.:
8. Бубнов, А.А. Основы информационной безопасности [Текст]: учеб. пособие для студентов учреждений среднего проф. образования / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. - 3-е изд., стер. - М.: Академия, 2017. - 256 с. - (Профессиональное образование. Информационная безопасность).
9. Защита информационных технологий. Справочник: справочник / Ю.И. Коваленко. - М.: Русайнс, 2016. - 321 с. - <http://www.book.ru/book/921524>
10. Информационная безопасность.: учебник / Мельников В.П. под ред., Куприянов А.И. — Москва: КноРус, 2019. — 267 с. — (СПО).
11. Информационная безопасность: учебник / Мельников В.П. под ред., Куприянов А.И. — Москва: КноРус, 2019. — 267 с. — (СПО). — URL: <https://book.ru/book/932059> (дата обращения: 01.11.2019). — Текст: электронный.
12. Новикова Е. Л. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи [Текст]: учебник для использования в образовательном процессе образовательных организаций, реализующих программы среднего профессионального образования по специальности "Инфокоммуникационные сети и системы связи" / Е. Л. Новикова. - Москва: Академия, 2018. – 192 с.
13. Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017. – 336с

Дополнительные источники

1. Бабаш, А.В. Криптографические методы защиты информации: учебник / Бабаш А.В., Баранова Е.К. — Москва: КноРус, 2021. — 189 с. — URL: <https://book.ru/book/933943>. — Текст: электронный.
2. Баранова, Е.К. Криптографические методы защиты информации. Лабораторный практикум +CD: учебное пособие / Баранова Е.К., Бабаш А.В. — Москва: КноРус, 2021. — 196 с. — URL: <https://book.ru/book/920017>. — Текст: электронный
3. Голиков А.М. Кодирование в телекоммуникационных системах [Электронный ресурс]: учебное пособие Курс лекций, компьютерный практикум, задание на самостоятельную работу / А.М. Голиков. - Электрон. текстовые данные. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2020. - 338 с.- Режим доступа: <http://www.iprbookshop.ru/72111.html>
4. Горбенко А.О. Основы информационной безопасности (введение в профессию) [Электронный ресурс]: учебное пособие / А.О. Горбенко. - Электрон. текстовые данные.

— СПб.: Интермедия, 2021. - 335 с. - Режим доступа:
<http://www.iprbookshop.ru/66797.html>

5. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

6. Креопалов, В. В. Технические средства и методы защиты информации: учебное пособие / В. В. Креопалов. — М.: Евразийский открытый институт, 2021. — 278 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/10871.html>.

7. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

8. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи: учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов: Ай Пи Эр Медиа, 2021. — 227 с. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: <http://www.iprbookshop.ru/80290.html>

Периодическая литература

Журналы «Системы безопасности», «Мир безопасности», «Электросвязь», «Вестник связи», «Сети и системы связи», «Системы и средства связи, телевидения и радиовещания», «Мобильные системы», «Технологии и средства связи», «Информкуррьер-связь», «Журнал сетевых решений».

Internet-ресурсы

Сайты ведущих телекоммуникационных компаний и систем безопасности и производителей оборудования:

<http://bolid.ru/> Научно-внедренческое предприятие «Болид»

<http://video.yandex.ru/> - видеонаблюдение

<http://www.mpn-sb.ru/> - видеонаблюдение

<http://www.mooml.com/> - Нормы и правила, ГОСТы, СНИПы. Нормативно-техническая документация

<http://snipov.net/> - Нормативные документы по противопожарной безопасности и по системам безопасности

<http://www.polyset.ru/GOST/> - Нормативные документы по противопожарной безопасности и по системам безопасности

<http://www.hited.ru> - Автоматизированные системные устройства

<http://ru.teplowiki.org> - Системы автоматизации, диспетчеризации и удаленного управления

<http://www.osp.ru/>

Приложение Д

Образец задания для проведения демонстрационного экзамена профильного уровня (КОД 10.02.04-1-2025)

Модуль № 1:

Эксплуатация информационно – телекоммуникационных систем и сетей

Текст задания:

С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах (Главный офис — виртуальные машины, Офис филиал — виртуальные машины). При выполнении заданий необходимо при помощи текстового редактора, сформировать отчет, в котором представить скриншоты ключевых настроек. В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети, задать пароли.

Задача 1.1 Произвести настройки сетевого окружения.

Для правильной работы сети надо создать или убедиться в наличии сетей:

Host only или внутренняя сеть адаптер для сети центрального офиса,
Host only или внутренняя сеть адаптер для сети филиала,
Host only или внутренняя сеть адаптер для сети межсетевого взаимодействия,
Host only адаптер, NAT или Bridge для виртуального «Интернета».

IP адреса защищенных сетей:

Центральный офис «Сеть 1 ЦО»:192.10.10.0/27
Офис филиал «Сеть 1 Филиал»:110.110.10.64/28
Офис сеть 2 «Сеть 2 Офис»: 172.16.128.128/25
«Интернет» для всех координаторов:200.100.100.0/24

Адреса выбираются самостоятельно из указанного диапазона.

Необходимые приложения: отсутствуют.

Модуль № 2:

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

Текст задания:

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

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

На виртуальной машине Net1-Admin (ЦО) установить ПО Client

(Пользовательская или серверная ОС), рабочее место администратора;

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

Необходимые приложения: отсутствуют.

Модуль № 1:

Эксплуатация информационно – телекоммуникационных систем и сетей

Текст задания:

Задача 1.2. Инициализация VPN Coordinator

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

Необходимые приложения: отсутствуют.

Модуль № 2:

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

Текст задания:

Задача 2.3. Развертывание защищенной сети

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

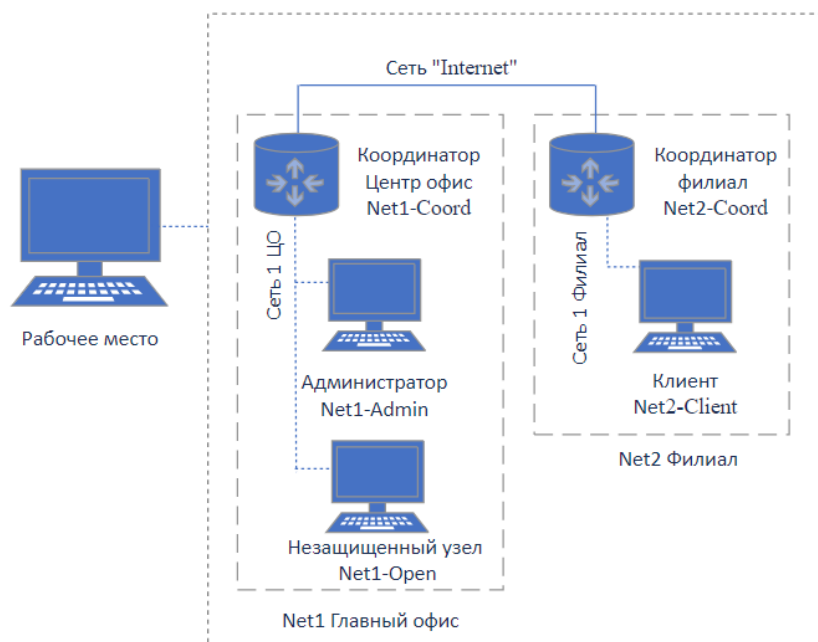


Рисунок 1 Схема защищенной сети

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

Таблица 1 - Узлы защищенной сети

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

Задача 2.4. Создание структуры защищенной сети

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

Таблица 2 - Схема связей пользователей

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

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

Задача 2.5. Отправить письмо по Деловой почте пользователю UserB с узла Администратора сети, отправить текстовое сообщение пользователю AdmN от пользователя UserB.

В отчете необходимо зафиксировать: скриншоты текстового сообщения и деловой почты на отправителе и получателе, скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторов.

Необходимые приложения: отсутствуют.

Модуль № 2:

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

Текст задания:

Задача 2.6. Реализовать межсетевое взаимодействие защищённых сетей (связями «все со всеми»), развернув на виртуальной машине Net3-Admin рабочее место Администратора партнёрской сети. Схема межсетевого взаимодействия представлена на рисунке 2.

Создать структуру второй сети: рабочее место администратора на виртуальной машине Net3-Admin, координатор (Net3-Coord-HW-VA).

Установить и настроить необходимое ПО. Настроить межсетевое взаимодействие, с использованием ассиметричных межсетевых ключей, между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

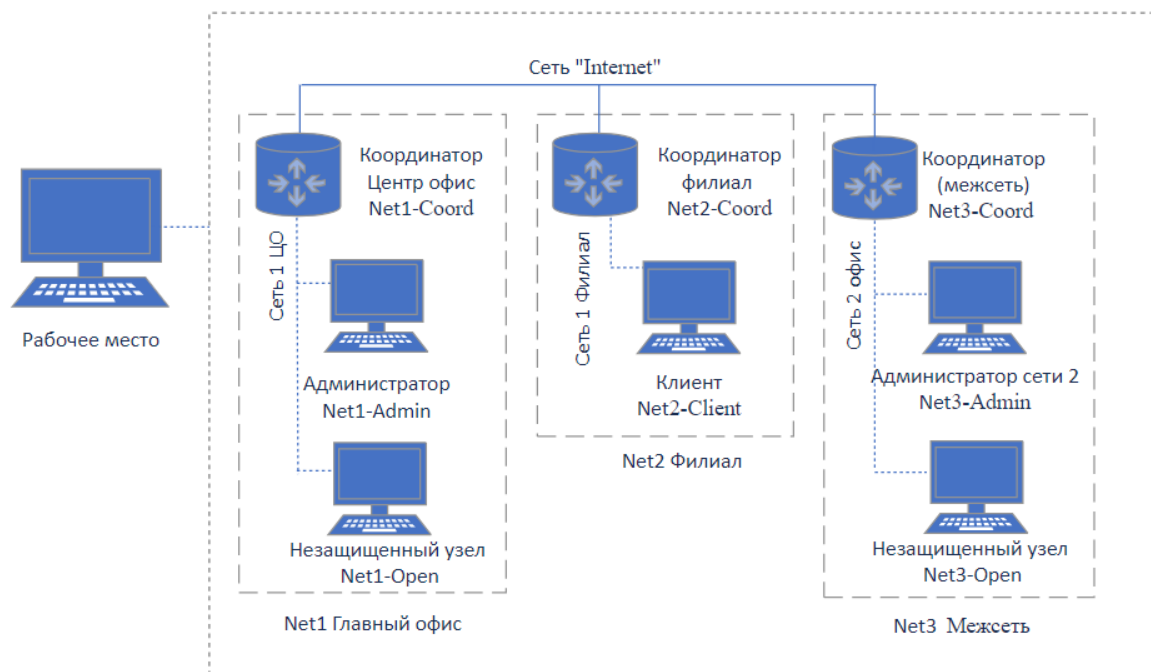


Рисунок 2 - Схема межсетевого взаимодействия

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

Необходимые приложения: отсутствуют.

Модуль № 2:

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

Текст задания:

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

User

администратору. В отчете необходимо зафиксировать процесс настройки скриншотами.

Задача 2.8. Настройка правил в сети.

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

Необходимые приложения: отсутствуют.

Модуль № 1:

Эксплуатация информационно – телекоммуникационных систем и сетей

Текст задания:

Задача 1.3. Туннелирование в рамках межсетевого взаимодействия

Подключить незащищенную машину в сети 3 (Net3-Open). Для второй открытой машины использовать Net1-Open узел в сети 1. Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по зашифрованному каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping), а также любым другим протоколом, например smb (общая сетевая папка) или другим удобным (кроме ICMP); проанализировать журналы IP-пакетов на координаторах.

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

Необходимые приложения: отсутствуют.