Приложение № 4
к образовательной программе среднего профессионального образования – программе подготовки специалистов среднего звена по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)

РАБОЧАЯ ПРОГРАММА ИТОГОВОЙ АТТЕСТАЦИИ

1. Общая характеристика итоговой аттестации

1.1. Цель итоговой аттестации: установление уровня подготовки выпускника образовательной программы среднего профессионального образования к выполнению задач профессиональной деятельности по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

1.2. Задачи итоговой аттестации:

– проверка уровня сформированности компетенций и степени владения выпускником теоретическими знаниями, умениями и практическими навыками для профессиональной деятельности с учетом типов задач профессиональной деятельности и планируемых результатов образовательной программы среднего профессионального образования;

– принятие решения о присвоении квалификации «Техник по защите информации» по результатам итоговой аттестации и выдаче документа о среднем профессиональном образовании.

1.3. Итоговая аттестация выпускников, завершающих обучение по образовательной программе среднего профессионального образования, является заключительным и обязательным этапом оценки содержания и качества освоения студентами образовательной программы среднего профессионального образования.

К итоговой аттестации допускается обучающийся, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по образовательной программе среднего профессионального образования.

1.4. Выпускник, освоивший образовательную программу среднего профессионального образования, должен обладать следующими компетенциями:

Личностные компетенции (общие)

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**
ЛК-01. Выбирает способы решения задач профессиональной деятельности применительно к различным контекстам	ИЛК-01.1. Анализирует профессиональный и социальный контекст, распознает задачу/проблему, выделяет её составные части и определяет значимые внешние и внутренние факторы
	ИЛК-01.2. Определяет этапы решения задачи, составляет структурированный план действий (с учетом алгоритмов выполнения работ) и обосновывает выбор необходимых ресурсов
	ИЛК-01.3. Применяет актуальные методы работы в профессиональной и смежных сферах, следуя установленным алгоритмам выполнения работ
	ИЛК-01.4. Адаптируется к изменяющимся условиям и новым идеям, корректирует способы действий на основе переоценки накопленного опыта и прогнозирования изменений
	ИЛК-01.5. Реализует составленный план, эффективно выполняя несколько разноплановых профессиональных задач без потери качества

	ИЛК-01.6. Оценивает результат решения задачи и последствия своих действий (самостоятельно или с помощью наставника), применяя установленный порядок оценки результатов профессиональной деятельности
	ИЛК-01.7. Применяет математический аппарат для постановки, анализа и решения профессиональных задач в различных контекстах
	ИЛК-01.8. Анализирует и оценивает процесс становления и развития мировой и отечественной науки и техники, технологической модернизации.
	ИЛК-01.9. Обобщает, анализирует и оценивает информацию: теории, концепции, факты, имеющие отношение к общественному развитию и роли личности в нем, с целью проверки гипотез и интерпретации данных различных источников
ЛК-02. Использует современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	ИЛК-02.1. Применяет номенклатуру информационных источников в профессиональной деятельности
	ИЛК-02.2. Формулирует поисковый запрос, выделяет и оценивает практическую значимость полученных результатов, структурирует и оформляет результаты поиска
	ИЛК-02.3. Организует собственную деятельность для решения стандартных профессиональных задач, действуя в рамках целей и способов, определенных руководителем
	ИЛК-02.4. Выделяет основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте
	ИЛК-02.5. Использует системные исторические знания, служащие основой для понимания места и роли России в мировой истории, соотносит (синхронизирует) события и процессы всемирной истории
	ИЛК-02.6. Самостоятельно анализирует документальную базу по исторической тематике, работает с историческими источниками
	ИЛК-02.7. Применяет методологии проектирования, разработки и поддержки на всех этапах жизненного цикла проекта
	ИЛК-02.8. Знает и применяет информационные технологии (системы счисления, кодирование, алгебра логики, теория информации) для представления, преобразования и обработки данных в профессиональной деятельности
ЛК-03. Планирует и	ИЛК-03.1. Определяет и выстраивает индивидуальную траекторию

реализует собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использует знания по правовой и финансовой грамотности в различных жизненных ситуациях	профессионального развития и самообразования с учетом актуальных требований отрасли и перспективных направлений цифровой экономики
	ИЛК-03.2. Рационально планирует, организует, своевременно корректирует и совершенствует процесс профессионального развития и самообразования на основе самостоятельной оценки результатов своей учебной и будущей профессиональной деятельности
	ИЛК-03.3. Анализирует результаты полученной работы и делает обоснованные выводы
	ИЛК-03.4. Выделяет перечень проблемных вопросов, информацией по которым не владеет
	ИЛК-03.5. Знает правовые нормы и требования законодательства в профессиональной деятельности и различных жизненных ситуациях
	ИЛК-03.6. Владеет инструментами финансовой грамотности для управления личными и профессиональными финансами, включая планирование бюджета, налоговые вопросы, оценку финансовых рисков и инвестиционные решения в рамках своей компетенции
	ИЛК-03.7. Анализирует взаимовлияние общественных, политических, экономических, социо-культурных процессов и технологического прогресса
	ИЛК-03.8. Развивает интеллектуальные, творческие способности и критическое мышление в ходе проведения простейших исследований, анализа явлений, восприятия и интерпретации естественно-научной информации
	ИЛК-03.9. Использует знания основ философии для формирования научного мировоззрения
ЛК-04. Эффективно взаимодействует и работает в коллективе и команде	ИЛК-04.1. Владеет основами проектной деятельности
	ИЛК-04.2. Организует работу коллектива и команды; взаимодействует с коллегами, руководством, клиентами в ходе профессиональной деятельности
	ИЛК-04.3. Знает психологические основы деятельности коллектива и психологические особенности личности
	ИЛК-04.4. Участвует в разработке мероприятий по улучшению условий работы команды
	ИЛК-04.5. Включается в коллективное обсуждение рабочей ситуации
	ИЛК-04.6. Анализирует производственную ситуацию и называет

	противоречия между реальными и идеальными условиями реализации технологического процесса
ЛК-05. Осуществляет устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	ИЛК-05.1. Применяет современную терминологию на государственном языке, относящуюся к описанию предметов, средств и процессов профессиональной деятельности
	ИЛК-05.2. Анализирует языковые единицы с точки зрения правильности, точности и уместности их употребления
	ИЛК-05.3. Грамотно излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке
	ИЛК-05.4. Знает особенности социального и культурного контекста, проявляет толерантность в рабочем коллективе
	ИЛК-05.5. Оценивает устные и письменные высказывания с точки зрения языкового оформления, эффективности достижения поставленных коммуникативных задач
	ИЛК-05.6. Понимает проблему, выдвигает гипотезу, структурирует материал, подбирает аргументы для подтверждения собственной позиции, выделяет причинно-следственные связи в устных и письменных высказываниях, формулирует выводы
	ИЛК-05.7. Осознает тесную связь между языковым, литературным, интеллектуальным, духовно- нравственным развитием личности и ее социальным ростом
ЛК-06. Проявляет гражданско-патриотическую позицию, демонстрирует осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применяет стандарты антикоррупционного	ИЛК-06.1. Знает сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности; стандарты антикоррупционного поведения и последствия его нарушения
	ИЛК-06.2. Демонстрирует осознанное поведение, руководствуясь традиционными российскими духовно-нравственными ценностями, проявляет уважение к культурному многообразию и учитывает принципы гармонизации межнациональных и межрелигиозных отношений
	ИЛК-06.3. Проявляет гражданско-патриотическую позицию в профессиональной и социальной деятельности и осознает свою роль в развитии общества и государства
	ИЛК-06.4. Умеет высказывать мнение относительно заданной ситуации, содержащей ту или иную нравственную коллизию

поведения	
ЛК-07. Содействует сохранению окружающей среды, ресурсосбережению, применяет знания об изменении климата, принципы бережливого производства, эффективно действует в чрезвычайных ситуациях	ИЛК-07.1. Выбирает верные алгоритмы действий в чрезвычайных ситуациях
	ИЛК-07.2. Соблюдает правила и нормы экологической безопасности при ведении социальной и профессиональной деятельности
	ИЛК-07.3. Организовывает профессиональную деятельность с учетом знаний об изменении климатических условий региона
	ИЛК-07.4. Осознает значимость компетенций в области естественных наук для человека и общества, использует технологические достижения в области химии, биологии, географии, экологии для повышения собственного интеллектуального развития в выбранной профессиональной деятельности
ЛК-08. Использует средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности	ИЛК-08.1. Понимает роль физической культуры в общекультурном, профессиональном и социальном развитии человека, осознает ценность здорового образа жизни для достижения жизненных и профессиональных целей
	ИЛК-08.2. Использует средства физкультурно-оздоровительной деятельности для сохранения и укрепления здоровья, поддержания необходимого уровня физической подготовленности
	ИЛК-08.3. Идентифицирует зоны риска физического здоровья, характерные для специальности
	ИЛК-08.4. Знает и применяет средства профилактики перенапряжения в процессе профессиональной деятельности
ЛК-09. Использует профессиональную документацию на государственном и иностранном языке	ИЛК-09.1. Владеет лексическим минимумом профессиональной и общей направленности: понимает и использует терминологию, относящуюся к описанию предметов, средств и процессов профессиональной деятельности, в устной и письменной речи
	ИЛК-09.2. Правильно читает, понимает общий смысл и переводит (самостоятельно и со словарем) тексты профессиональной и общей направленности, включая инструкции, нормативные документы и техническую литературу
	ИЛК-09.3. Составляет тексты профессиональной и общей направленности: грамматически правильно строит простые и сложные предложения, ведет письменную переписку на профессиональные и общие темы, оформляет документацию на государственном и иностранном языках

	ИЛК-09.4. Участвует в устной коммуникации на профессиональные и общие темы: воспринимает общий смысл высказываний, участвует в диалогах, представляет информацию на государственном и иностранном языках
	ИЛК-09.5. Самостоятельно развивает языковые компетенции, совершенствует устную и письменную речь, расширяет словарный запас, адаптирует языковые средства под изменяющиеся профессиональные задачи

Профессиональные компетенции

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**
ПК-01. Выполняет монтаж, настройку и администрирование сетевого оборудования и систем обеспечения информационной безопасности	ИПК-01.1. Выполняет установку и конфигурирование аппаратного обеспечения ПК, серверов и периферийного оборудования
	ИПК-01.2. Выполняет монтаж и подключение линейных сооружений связи и кабельных систем
	ИПК-01.3. Администрирует сетевые устройства (маршрутизаторы, коммутаторы)
	ИПК-01.4. Реализует сетевую безопасность (межсетевые экраны, VPN, ACL, IDS/IPS)
	ИПК-01.5. Осуществляет аудит безопасности и контроль целостности вычислительной системы
ПК-02. Обеспечивает бесперебойное функционирование, мониторинг и защиту сетевой инфраструктуры	ИПК-02.1. Обеспечивает мониторинг доступности сетевых устройств и каналов связи
	ИПК-02.2. Настраивает протоколы динамической маршрутизации (OSPF, RIP) и управление пропускной способностью каналов связи
	ИПК-02.3.Проводит анализ журналов событий (syslog, SNMP) для выявления сбоев
	ИПК-02.4. Обеспечивает резервирование и отказоустойчивость сетевой инфраструктуры
	ИПК-02.5. Анализирует сетевой трафик и выявляет инциденты информационной безопасности
ПК-03. Применять	ИПК-03.1. Применяет криптографические средства и методы защиты информации

программно-аппаратные средства и методы обеспечения информационной безопасности, включая тестирование на проникновение и анализ защищённости	ИПК-03.2. Устанавливает и конфигурирует программно-аппаратные средства защиты информации
	ИПК-03.3. Выполняет тестирование на проникновение и анализ защищённости
	ИПК-03.4. Анализирует уязвимости и составляет отчёты по результатам тестирования
	ИПК-03.5. Обеспечивает антивирусную защиту и контроль программного обеспечения
ПК-04. Применять средства автоматизации для администрирования, управления инцидентами и настройки систем информационной безопасности	ИПК-04.1. Разрабатывает скрипты для автоматизации задач администрирования и безопасности
	ИПК-04.2. Осуществляет мониторинг и управление инцидентами в ИТ-системах
	ИПК-04.3. Работает в системах Service Desk и управления конфигурациями
	ИПК-04.4. Применяет инструменты автоматизации для настройки средств защиты
ПК-05. Обеспечивать физическую и техническую защиту объектов информатизации, включая выявление и блокирование каналов утечки информации	ИПК-05.1. Организует физическую защиту объектов информатизации (СКУД, видеонаблюдение)
	ИПК-05.2. Выявляет и блокирует технические каналы утечки информации
	ИПК-05.3. Обеспечивает электробезопасность и защиту от электромагнитных излучений
	ИПК-05.4. Эксплуатирует инженерно-технические средства охраны
ПК-06. Использует знания в области информатики и информационных технологий в профессиональной деятельности	ИПК-06.1. Применяет прикладные офисные пакеты в профессиональной деятельности
	ИПК-06.2. Использует блок-схемы для описания алгоритмов
	ИПК-06.3. Знает и использует операции алгебры логики в профессиональной деятельности
	ИПК-06.4. Работает с численными значениями, представленными в разных системах счисления

	ИПК-06.5. Знает и использует основные понятия теории информации
ПК-07. Применяет методы математического анализа, дискретной математики и математической логики для построения моделей, разработки алгоритмов и анализа информационных систем в профессиональной деятельности	ИПК-07.1. Выполняет операции над матрицами, решает системы линейных уравнений и использует элементы теории множеств и комбинаторики для формализации задач обработки данных и разработки алгоритмов.
	ИПК-07.2. Применяет методы дифференциального и интегрального исчисления для анализа характеристик процессов (скорость передачи данных, оптимизация алгоритмов, моделирование систем).
	ИПК-07.3. Использует алгебру логики для построения сложных условий, оптимизации логических выражений, формирования запросов к базам данных и разработки алгоритмов принятия решений.
	ИПК-07.4. Применяет теорию графов для моделирования структур данных (сети, деревья решений, схемы баз данных, иерархии) и оптимизации маршрутов обработки информации.
	ИПК-07.5. Использует методы теории вероятностей и математической статистики для оценки надежности программных средств, обработки результатов экспериментов и анализа рисков в информационных системах.
ПК-08. Устанавливает и производит конфигурацию персональных компьютеров и устройств	ИПК-08.1. Устанавливает и производит конфигурацию ИТ-систем и подключает периферийные устройства
	ИПК-08.2. Производит конфигурацию и установку персональных рабочих станций, техническую поддержку работы оборудования и программ
	ИПК-08.3. Собирает ПК из комплектующих, исходя из их совместимости
	ИПК-08.4. Проводит инсталляцию, конфигурирование и настройку операционной системы, драйверов, резидентных программ
ПК-09. Выполняет проектирование топологии и архитектуры ИТ-систем	ИПК-09.1. Использует в работе общие принципы построения сетей
	ИПК-09.2. Знает топологии и архитектуры компьютерных сетей
	ИПК-09.3. Уверенно распознает уровневые модели открытых систем OSI и TCP
	ИПК-09.4. Разрабатывает архитектуру корпоративных и частных сетей
ПК-10. Разрабатывает	ИПК-10.1. Программирует на языке Python
	ИПК-10.2.Интегрирует программные модули в приложение

системы, комплексы, средства и технологии обеспечения информационной безопасности	ИПК-10.3. Разрабатывает модели угроз, проводит оценку рисков и разрабатывает компенсирующие меры
ПК-11. Проектирует базу данных и разрабатывает в ней объекты на основе анализа предметной области	ИПК-11.1. Знает структуры данных СУБД
	ИПК-11.2. Применяет в работе основные принципы построения концептуальной, логической и физической модели данных
	ИПК-11.3. Работает с современными инструментальными средствами проектирования схемы базы данных
	ИПК-11.4. Знает понятие транзакции и языки для написания хранимых процедур
	ИПК-11.5. Создает объекты баз данных в современных СУБД
ПК-12. Проводит тестирование, отладку и приёмо-сдаточные испытания ИТ-систем и программного обеспечения	ИПК-12.1. Проводит инсталляцию, конфигурирование и настройку операционной системы, драйверов, резидентных программ
	ИПК-12.2. Использует средства и встроенные программы тестирования
	ИПК-12.3. Проводит автоматизированное функциональное тестирование
	ИПК-12.4. Проводит модульное, интеграционное, системное и приёмочное тестирование в разных методологиях разработки
	ИПК-12.5. Пишет тестовые сценарии
ПК-13. Проводит анализ защищенности информационных систем через тестирование на проникновение	ИПК-13.1. Применяет автоматизированные средства сбора информации и разведки в киберпространстве
	ИПК-13.2. Применяет сканеры уязвимостей на сетевом уровне
	ИПК-13.3. Применяет сканеры уязвимостей на уровне операционной системы
	ИПК-13.4. Применяет сканеры уязвимостей на уровне прикладного ПО
	ИПК-13.5. Разрабатывает методологию описания уязвимостей и формирует отчеты
	ИПК-13.6. Разрабатывает программы и методики испытаний средств и систем обеспечения информационной безопасности
	ИПК-13.7. Применяет автоматизированные средства сбора информации и разведки в киберпространстве

2. Объем, формы и срок итоговой аттестации

2.1. Объем итоговой аттестации составляет 216 ак.часа.

2.2. На проведение итоговой аттестации выделяется 8 недель.

2.3. Итоговая аттестация по образовательной программе среднего профессионального образования проводится в форме сдачи итогового (демонстрационного) экзамена, подготовки и защиты дипломного проекта (работы).

2.4. Итоговая аттестация проводится в сроки, установленные календарным учебным графиком образовательной программы среднего профессионального образования. Расписание проведения защиты дипломного проекта (работы) доводится до сведения обучающихся не позднее чем за 1 месяц до начала периода итоговой аттестации.

3. Итоговый (демонстрационный) экзамен

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

3.2. Задания демонстрационного экзамена разрабатываются на основе профессиональных стандартов: «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н, «Специалист по безопасности компьютерных систем и сетей», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н, «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н, «Специалист по защите информации в автоматизированных системах», утвержденного Приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 599н и с учетом примерной основной образовательной программы.

Примерные задания к итоговому (демонстрационному) экзамену представляются обучающимся для ознакомления не позднее чем за 1 месяц до его проведения.

Примерный перечень заданий к итоговому (демонстрационному) экзамену:

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.

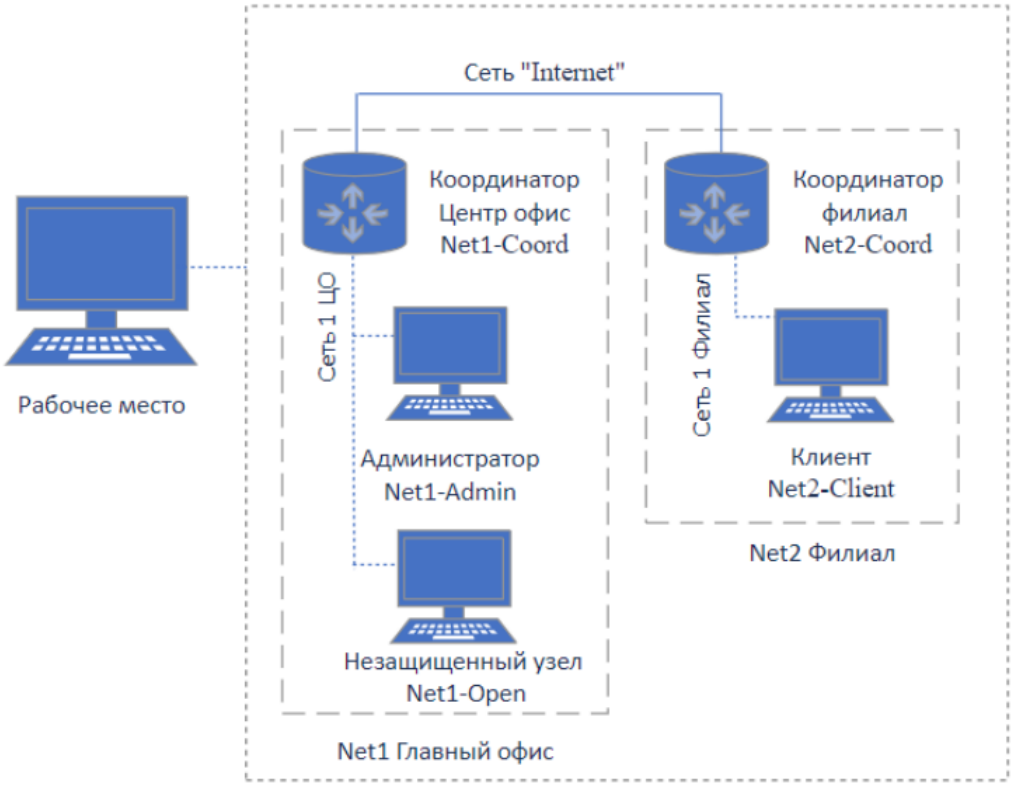

Рисунок 1 Схема защищенной сети

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, УКЦ), Client	Пользовательская или серверная ОС	AdmN
Net1-Coord (ЦО)	Координатор офиса	Coordinator	HW-VA	CoordO
Net2-Coord (филиал)	Координатор филиала	Coordinator	HW-VA	CoordB
Net2-Client (филиал)	Пользователь филиала	Client	Пользовательская или серверная ОС	UserB

Задача 2.4. Создание структуры защищенной сети

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

Таблица 2 - Схема связей пользователей

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

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

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

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

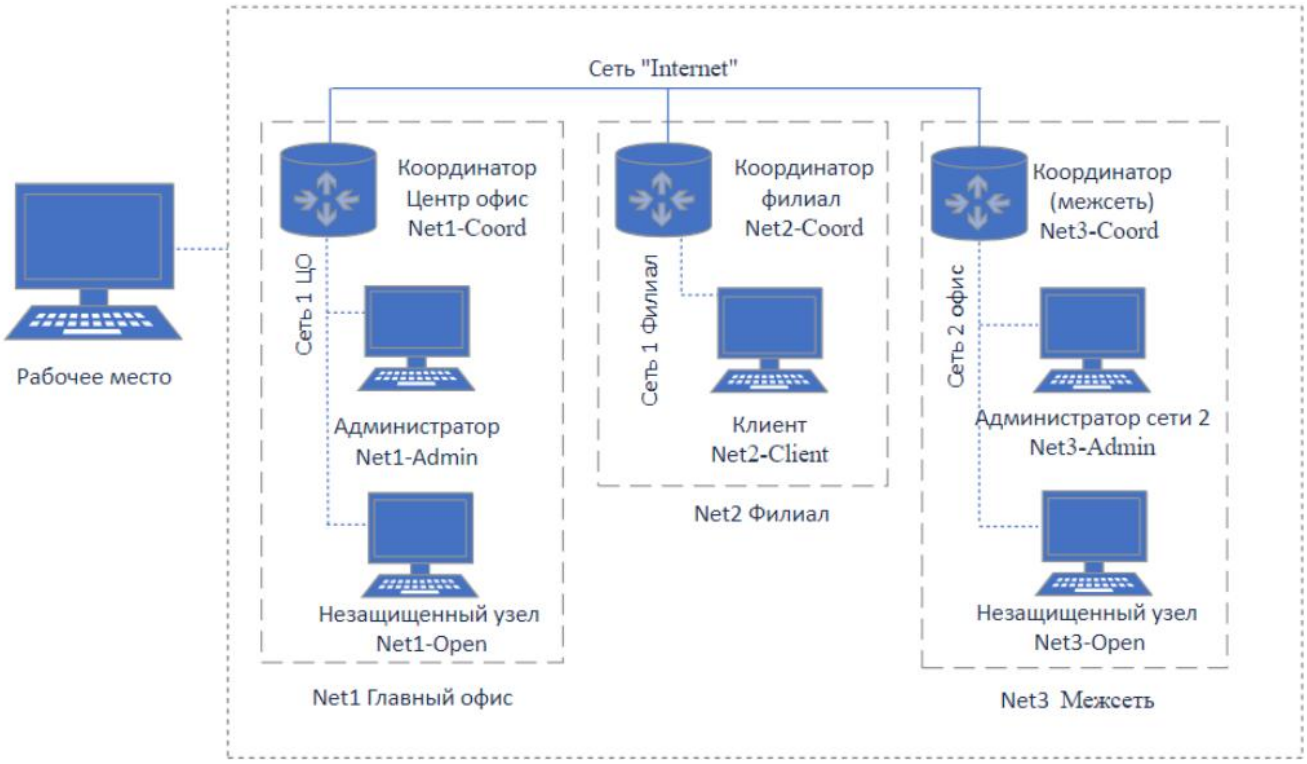

Рисунок 2 - Схема межсетевого взаимодействия

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 SSHдоступ 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 шифрованному

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 проверкиработоспособности механизма туннелирования.

Необходимые приложения: отсутствуют.

3.3. Порядок проведения итогового (демонстрационного) экзамена (далее – ДЭ)

Не позднее чем за один рабочий день до даты проведения ДЭ главным экспертом проводится проверка готовности площадки ДЭ в присутствии 5 членов экспертной группы, обучающихся, а также технического эксперта, назначаемого организацией, на территории которой расположена площадка ДЭ, ответственного за соблюдение установленных норм и правил охраны труда и техники безопасности.

Главным экспертом осуществляется осмотр площадки ДЭ, 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.

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

Допуск обучающихся на площадку ДЭ осуществляется главным экспертом на основании документов, удостоверяющих личность.

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

Выпускники вправе:

- пользоваться оборудованием площадки проведения экзамена, необходимыми материалами, средствами обучения и воспитания в соответствии с требованиями комплекта оценочной документации, задания демонстрационного экзамена;
- получать разъяснения технического эксперта по вопросам безопасной и бесперебойной эксплуатации оборудования площадки проведения экзамена;
- получить копию задания демонстрационного экзамена на бумажном носителе.

Выпускники обязаны:

- во время проведения демонстрационного экзамена не пользоваться и не иметь при себе средства связи, носители информации, средства её передачи и хранения, если это прямо не предусмотрено комплектом оценочной документации;
- во время проведения демонстрационного экзамена использовать только средства обучения и воспитания, разрешённые комплектом оценочной документации;
- во время проведения демонстрационного экзамена не взаимодействовать с другими выпускниками, экспертами, иными лицами, находящимися на площадке ДЭ, если это не предусмотрено комплектом оценочной документации и заданием демонстрационного экзамена.

Выпускники могут иметь при себе лекарственные средства и питание, приём которых осуществляется в специально отведённом для этого помещении согласно плану проведения демонстрационного экзамена за пределами площадки ДЭ.

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

В соответствии с планом проведения демонстрационного экзамена главный эксперт ознакамливает выпускников с заданиями, передает им копии заданий демонстрационного экзамена.

После ознакомления с заданиями демонстрационного экзамена выпускники занимают свои рабочие места в соответствии с протоколом распределения рабочих мест.

После того, как все выпускники и лица, привлеченные к проведению демонстрационного экзамена, займут свои рабочие места в соответствии с требованиями охраны труда и производственной безопасности, главный эксперт объявляет о начале демонстрационного экзамена.

Время начала демонстрационного экзамена фиксируется в протоколе проведения демонстрационного экзамена, составляемом главным экспертом по каждой экзаменационной группе.

После объявления главным экспертом начала демонстрационного экзамена выпускники приступают к выполнению заданий демонстрационного экзамена.

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

Явка выпускника, его рабочее место, время завершения выполнения задания демонстрационного экзамена подлежат фиксации главным экспертом в протоколе проведения демонстрационного экзамена.

В случае удаления из центра проведения экзамена выпускника, лица, привлеченного к проведению демонстрационного экзамена, или присутствующего в центре проведения экзамена, главным экспертом составляется акт об удалении. Результаты ИА выпускника, удаленного из центра проведения экзамена, аннулируются ЭК, и такой выпускник признаётся ЭК не прошедшим ИА по неуважительной причине.

Главный эксперт сообщает выпускникам о течении времени выполнения задания демонстрационного экзамена каждые 60 минут, а также за 30 и 5 минут до окончания времени выполнения задания.

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

Выпускник по собственному желанию может завершить выполнение задания досрочно, уведомив об этом главного эксперта.

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

Результаты проведения ИА оцениваются с проставлением одной из отметок: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» - и объявляются в тот же день после оформления протоколов заседаний ЭК.

Процедура оценивания результатов выполнения заданий демонстрационного экзамена осуществляется членами экспертной группы по 100-балльной системе в соответствии с требованиями комплекта оценочной документации, представленного в приложении 1.

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 ЭК, не входящий в экспертную группу, присутствие других лиц запрещено.

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

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

4. Требования к дипломному проекту (работе) и порядок его выполнения

4.1. 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.

4.2. Требования к содержанию дипломного проекта (работы)

Дипломный проект (работа) должен отвечать следующим основным требованиям:

- соответствие названия работы ее содержанию, четкая целевая направленность, актуальность;
- логическая последовательность изложения материала, базирующаяся на прочных теоретических знаниях по избранной теме и убедительных аргументах;
- корректное изложение материала с учетом принятой научной терминологии;
- достоверность полученных результатов и обоснованность выводов;
- научный стиль написания;
- оформление работы в соответствии с требованиями приказа АНО ВО «Университет «Сириус» от 25.01.2023 № 13/3-ОД-У «Об утверждении Стандарта АНО ВО «Университет «Сириус» «Студенческие работы: общие положения и правила оформления» (далее – Стандарт).

4.3. Тематика дипломного проекта (работы)

Обучающимся предлагается подготовить дипломный проект (работу) по следующим примерным темам:

1. Организация безопасного удаленного доступа к инфраструктуре предприятия.
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии.
3. Автоматизация процесса проверок наличия конфиденциальных документов на общедоступных ресурсах сети предприятия.
4. Разработка проекта программно-аппаратной защиты информации предприятия.
5. Разработка систем видеонаблюдения и сигнализации для обеспечения защиты информации на предприятии.

6. Внедрение многофакторной аутентификации в корпоративной среде крупных предприятий (фонд "Талант и успех").

7. Тестирование операционной системы Astra Linux методом черного ящика.

8. Автоматизированное тестирование web-приложений используемых на ресурсах предприятия.

9. Отдельные аспекты внедрения Kaspersky Unified Monitoring and Analysis Platform на крупном объекте информатизации: опыт внедрения, проблемы, результаты.

10. Совершенствование системы защиты информации в помещениях (название предприятия).

11. Защита речевой информации в каналах связи коммерческого предприятия.

12. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации.

13. Анализ методов оценки качества функционирования комплексной системы защиты предприятия.

14. Организация процесса мониторинга конфиденциального документооборота предприятия.

15. Построение системы антивирусной защиты в гетерогенной инфраструктуре.

16. Построение и автоматизация процесса управления уязвимостями в корпоративной инфраструктуре.

17. Построение процесса повышения осведомленности по информационной безопасности в организации.

Рекомендуемый объем дипломного проекта (работы) должен составлять от 60 до 80 страниц.

Работа должна включать следующие структурные элементы в указанной ниже последовательности:

- титульный лист;
- задание для дипломного проекта (работы);
- сокращения, обозначения, термины и определения;
- оглавление;
- введение
- основной текст работы (пояснительная записка);
- заключение;
- список использованных источников;
- приложения.

В пояснительную записку вкладываются, но не подшиваются:

- отзыв руководителя;
- рецензия.

К дипломному проекту (работе) прилагается разработанный программный продукт на внешнем носителе.

4.5. Содержание дипломного проекта (работы)

К структурным элементам дипломного проекта (работы) предъявляются следующие требования:

- титульный лист является первой страницей дипломного проекта (работы) и служит источником информации для обработки документа;

Формулировка темы дипломного проекта (работы) на титульном листе и в задании должна точно соответствовать ее формулировке в приказе об утверждении тем и закреплении руководителей дипломных проектов (работ);

- пояснительная записка:

а) содержание дает представление о структуре работы и включает в себя введение, наименование всех разделов, подразделов, пунктов, заключение, список использованных источников и приложений с указанием страниц, с которых начинаются перечисленные элементы дипломного проекта (работы). Названия заголовков, разделов, подразделов и пунктов в содержании перечисляются в той же последовательности, в тех же формулировках, что и в тексте работы. В содержание не включают титульный лист, задание;

б) структурный элемент «Перечень используемых условных обозначений, сокращений, терминов» содержит перечень условных обозначений, сокращений, терминов, применяемых в дипломном проекте (работе). Перечень составляется в порядке приведения их в тексте дипломного проекта (работы) с необходимой расшифровкой и пояснениями. В том случае, когда в дипломном проекте (работе) обозначения, символы, сокращения и т.д. повторяются менее трех раз, перечень не составляют, а приводят расшифровку в тексте при первом их упоминании;

в) введение краткая характеристика документа с точки зрения его назначения, содержания, вида, формы и других особенностей. Введение включает характеристику основной темы, проблемы объекта, цели работы и ее результаты. Во введении указывают, что нового несет в себе данный документ в сравнении с другими, родственными по тематике и целевому назначению, должно содержать оценку современного состояния решаемой проблемы, основание и исходные данные для выполнения дипломного проекта (работы).

Введении включает следующие аспекты содержания исходного документа:

- предмет, тему, объект и цель работы
- метод или методологию проведения работы
- результаты работы
- область применения результатов
- выводы
- дополнительную информацию;

г) основная часть дипломного проекта (работы) должна содержать разделы, отражающие сущность, методику, решение основных задач в соответствии с заданием, и основные результаты работы. Рекомендуемые разделы:

- Анализ предметной области и выбор средств разработки. Описание объектов и процессов, их взаимосвязей, а также представление моделей «AS-IS» и «TO BE» рассматриваемой сферы. Обзор аналогов с указанием их достоинств и недостатков для организации, в которой планируется внедрение. Сравнение методов и средств проектирования и создания с указанием их ограничений и особенностей использования. Итогом раздела является вывод о необходимости разработки уникального решения для конкретной организации с выбором конкретных средств проектирования разработки и внедрения.
- Описание процесса проектирования, создания и внедрения разработанного решения. Последовательное изложение всех этапов работы над проектом – от проектирования до внедрения. Раздел должен содержать все нюансы и технические детали разрабатываемого решения. Должны быть предоставлены сценарии использования решения и

схемы взаимодействия с пользователями и другими информационными системами. В разделе представляются результаты тестирования решения и возможные ограничения при его внедрении.

- Экономическая эффективность. Приводится оценка проекта с точки зрения затрат разного рода ресурсов (временных, человеческих, материальных и т.д.), а также прогноз окупаемости. Сравниваются затраты организации до и после внедрения разработанного решения по разным критериям, которые характерны для предметной области.

д) в заключении подводятся итоги исследования, обобщаются и формулируются выводы. Заключение должно содержать краткие выводы по результатам дипломного проекта (работы), оценку полноты выполнения задания и рекомендации по практическому и научному применению результатов работы;

е) список использованных источников должен быть составлен в соответствии с требованиями Стандарта и содержать сведения о литературных источниках, электронных изданиях и электронных информационных ресурсах, использованных при выполнении дипломного проекта (работы). На 80 % литературных источников обязательно должны быть ссылки по тексту. Общее количество источников информации, использованных при выполнении дипломного проекта (работы), должно быть не менее 10 наименований. Все источники нумеруются последовательно (не по разделам), научная литература должна быть не более 5-ти летней давности;

ж) материал, дополняющий основную часть дипломного проекта (работы), оформляют в виде приложений. Объем приложений в дипломном проекте (работе) не регламентируется. В тексте работы на все приложения должны быть даны ссылки. Рекомендуется включать в приложения материалы, связанные с выполненной работой, которые по каким-либо причинам не могут быть включены в основную часть. В приложениях целесообразно приводить графический материал большого объёма и/или формата, таблицы большого формата.

4.6. Оформление дипломного проекта (работы)

Дипломный проект (работа) оформляется в соответствии со Стандартом 01-2023 «Студенческие работы: общие требования и правила оформления», утвержденным приказом АНО ВО «Университет «Сириус» №13/3-ОД-У от 25 января 2023 г.

4.7. Порядок защиты дипломного проекта (работы)

Защита дипломного проекта (работы) проводится на открытом заседании экзаменационной комиссии. На доклад по теме дипломного проекта (работы) отводится 10 минут и 5 минут на ответы на вопросы членов экзаменационной комиссии.

После окончания публичной защиты проводится закрытое заседание ЭК. Оценка («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») определяется открытым голосованием простым большинством голосов. При равном числе голосов голос председателя является решающим. Результаты защиты объявляются обучающимся в день защиты дипломного проекта (работы).

5. Критерии оценки результатов итоговой аттестации

Результаты любой из форм ИА определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Результаты ИА объявляются в день их проведения после оформление в установленном порядке протоколов заседаний ЭК.

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

5.1. Критерии оценки результатов итогового (демонстрационного) экзамена

Оценка	Критерии оценки итогового (демонстрационного) экзамена
2 «неудовлетворительно»	от 0 до 49 баллов
3 «удовлетворительно»	от 50 до 69 баллов
4 «хорошо»	от 70 до 89 баллов
5 «отлично»	от 90 до 100 баллов

5.2. Критерии оценки результатов защиты дипломного проекта (работы)

Оценка	Критерии оценки результатов защиты дипломного проекта (работы)
2 «неудовлетворительно»	Дипломный проект (работа) не отвечает предъявляемым требованиям задания и/или оформлен с серьёзными отклонениями от требований; Выступление студента на защите не структурировано, допускаются грубые ошибки при раскрытии актуальности темы, цели, задачи и основных результатов работы; Присутствует плагиат.
3 «удовлетворительно»	Дипломный проект (работа) не в полной мере отвечает предъявляемым требованиям задания, в работе используются только ссылки на устаревшие источники информации/литературу (нет источников по теме дипломного проекта (работы) за последние 5 лет); Выступление студента на защите не всегда структурировано, допускаются ошибки при раскрытии актуальности темы, цели, задачи и основных результатов работы; Отсутствует плагиат.
4 «хорошо»	Дипломный проект (работа) отвечает предъявляемым требованиям задания и оформлен с незначительными отклонениями от требований; в работе используются ссылки на современные источники информации/литературу за последние 5 лет по теме дипломного проекта (работы); Выступление студента на защите структурировано, раскрыты актуальность темы, цель, задачи и основные результаты работы, выводы не вполне соответствуют полученным результатам; Отсутствует плагиат.
5 «отлично»	Дипломный проект (работа) отвечает предъявляемым требованиям задания и оформлен в соответствии с требованиями; в работе используются ссылки на современные источники информации/литературу за последние 5 лет по теме дипломного проекта (работы);

	Выступление студента на защите структурировано, раскрыты актуальность темы, цель, задачи и основные результаты работы; приведено доказательство значимости представленных результатов, выводы соответствуют полученным результатам; Отсутствует плагиат.

После окончания публичной защиты проводится закрытое заседание экзаменационной комиссии. Оценка («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») определяется открытым голосованием простым большинством голосов. При равном числе голосов голос председателя является решающим. Результаты защиты объявляются обучающимся в день защиты дипломного проекта (работы).

6. Учебно-методическое и информационное обеспечение итоговой аттестации

6.1. Основная литература:

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва: Издательство Юрайт, 2026. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8.

2. Компьютерные сети и системы связи. Вводный курс: учебное пособие для среднего профессионального образования / А. Н. Рабчевский. — Москва: Издательство Юрайт, 2024. — 226 с. — (Профессиональное образование). — ISBN 978-5-534-19073-1.

3. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3.

6.2. Дополнительная литература:

1. Администрирование системы защиты информацииViPNet версии 4. Учебно-методическое пособие / Под редакцией д.п.н., профессора А.О. Чефрановой / В.Е.Чаплыгин, А.О. Чефранова, Ю.Ф. Алабина – Москва: ОАО «ИнфоТеКС» - 2020 – 188с. – ISBN 978-5-9912-0676-1

2. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание / В. Олифер, Н. Олифер — СПб.: Питер, 2020. — 1008 с.: ил. — (Серия «Учебник для вузов»).ISBN 978-5-4461-1426-9

3. Основы локальных компьютерных сетей: Учебное пособие / А. Н Сергеев. — СПб.: Издательство «Лань», 2016. — 184 с.: ил. —(Учебники для вузов. Специальная литература). ISBN 9785811421855

4. Программно-аппаратные комплексы ViPNet HW 4. / Под редакцией д.п.н. А.О. Чефрановой = Москва : ОАО «ИнфоТеКС», 2023 – 144с. – ББК 32.973.26-018.2 – Г96

Технология построения VPN ViPNet: курс лекций. Изд. 3-е. / А.О. Чефранова – Москва – 2024 – 292с. – ББК 32.973.26-018.2 – Ч55

6.3. Современные профессиональные базы данных и ресурсов информационно-телекоммуникационной сети «Интернет»:

Электронно-библиотечная система издательства "Юрайт" - Режим доступа: https://urait.ru/

7. Материально-техническое и программное обеспечение итоговой аттестации

7.1. Материально-техническое обеспечение:

Для проведения защиты дипломных проектов:

Вид аудитории	Технические средства и оборудование
Учебная аудитория для проведения итоговой аттестации	Компьютер с проектором. Маркерная доска, маркер. Учебная мебель. Рабочие места по числу членов комиссии

Для проведения ДЭ:

На каждого студента:

1.	Стол	Технические характеристики на усмотрение образовательной организации (далее ОО)	1	шт
2.	Стул	Технические характеристики на усмотрение ОО	1	шт
3.	Персональный компьютер в сборе	Персональный компьютер в сборе: CPU: x86-64, не менее 8 ядер, Частота процессора максимальная не ниже 3,5ГГц, с поддержкой аппаратной виртуализации или аналог; • RAM: не менее 16 ГБ; • HDD: не менее 500 ГБ или аналог, возможна замена на твердотельный накопитель SATA или NVMe с объёмом не менее 240ГБ; • сеть: технология Ethernet стандарта 100BASE-T или аналог; • видеокарта: дискретная или интегрированная с возможностью подключения двух мониторов или аналог; • монитор: не менее 23,8” и разрешением не менее 1920x1080 или аналог; • клавиатура: интегрированная, стандартная проводная или аналог; • манипулятор «мышь»: стандартный проводной или аналог Возможен аналогичный по параметрам ноутбук	3	шт
		Наличие пользовательского графического окружения (GUI)	3	шт

4.	Операционная система (далее ОС)	Совместимость с позицией №3 Возможно присутствие в комплекте поставки: Веб-браузер Программное обеспечение (далее ПО) для просмотра документов в формате PDF ПО для архивации Пакет офисных программ		
5.	Веб-браузер	Поддержка работы по схеме HTTPS Поддержка разметки HTML5 Может входить в состав других позиций.	1	шт
6.	Программное обеспечение (далее ПО) для просмотра документов в формате PDF	Может входить в состав других позиций.	1	шт
7.	ПО для архивации	Может входить в состав других позиций.	1	шт
8.	ПО для виртуализации		1	шт
9.	Пакет офисных программ	Компоненты офисного пакета: графический редактор, редактор электронных таблиц, средство просмотра документов, текстовый редактор. Может входить в состав других позиций.	1	шт
10.	ВМ «базовая ОС»	ОС РедОС 8/аналог vRAM: не менее 1 Гб или аналог vCPU: не менее 1 ядро или аналог vHDD: не менее 10 Гб или аналог	1	шт
11.	ВМ «сетевое устройство»	ОС Coordinator HW-VA или аналог с функциями маршрутизации vRAM: не менее 1 Гб или аналог vCPU: не менее 1 ядро или аналог vHDD: не менее 1 Гб или аналог	3	шт
12.	ВМ «рабочая станция»	ОС РедОС 8 Рабочая станция/аналог vRAM: не менее 2 Гб или аналог vCPU: не менее 1 ядро или аналог vHDD: не менее 100 Гб или аналог	5	шт
13.	Бумага формата А4		1	шт
14.	Ручка шариковая		1	шт
15.	Карандаш		1	ш

				т

На экспертную группу:

1.	Стол	Технические характеристики на усмотрение образовательной организации (далее ОО)	По количеству членов комиссии	шт
2.	Стул	Технические характеристики на усмотрение ОО	По количеству членов комиссии	шт
3.	Персональный компьютер в сборе	Персональный компьютер в сборе: CPU: x86-64, не менее 4 ядер, Частота процессора максимальная не ниже 3,5ГГц, с поддержкой аппаратной виртуализации или аналог; • RAM: не менее 8 ГБ; • HDD: не менее 500 ГБ или аналог, возможна замена на твердотельный накопитель SATA или NVMe с объёмом не менее 240ГБ; • сеть: технология Ethernet стандарта 100BASE-T или аналог; • видео карта: дискретная или интегрированная с возможностью подключения двух мониторов или аналог; • монитор: не менее 23,8” и разрешением не менее 1920x1080 или аналог; • клавиатура: интегрированная, стандартная проводная или аналог; • манипулятор «мышь»: стандартный проводной или аналог Возможен аналогичный по параметрам ноутбук	1	шт
		Наличие пользовательского графического окружения (GUI)	1	шт

4.	Операционная система (далее ОС)	Совместимость с позицией №3 Возможно присутствие в комплекте поставки: Веб-браузер Программное обеспечение (далее ПО) для просмотра документов в формате PDF ПО для архивации Пакет офисных программ		
5.	Веб-браузер	Поддержка работы по схеме HTTPS Поддержка разметки HTML5 Может входить в состав других позиций.	1	шт
6.	Программное обеспечение (далее ПО) для просмотра документов в формате PDF	Может входить в состав других позиций.	1	шт
7.	ПО для архивации	Может входить в состав других позиций.	1	шт
9.	Пакет офисных программ	Компоненты офисного пакета: графический редактор, редактор электронных таблиц, средство просмотра документов, текстовый редактор. Может входить в состав других позиций.	1	шт
10.	Бумага формата А4		По количеству членов комиссии	шт
11.	Ручка шариковая		По количеству членов комиссии	шт
12.	Карандаш		По количеству членов комиссии	шт

Приложение 1
к рабочей программе итоговой аттестации
по специальности 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ

к итоговому (демонстрационному) экзамену

Модуль № 1: Эксплуатация информационно – телекоммуникационных систем и сетей

1. *Задача 1.1. Моделирование сети.*

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 (см. рисунок 2).

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»:192.12.10.0/27
- Офис филиал «Сеть 1 Филиал»:192.13.10.64/28
- 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.

Всего 10 баллов	Баллы
1. Моделирование сети	2
1. Настроены все сетевые интерфейсы 2. Сетевые настройки соответствуют заданию	
1. Развертывание рабочих станций	6
1. Все рабочие станции развернуты 2. Проведена предварительная настройка рабочих станций (пароли, сетевые интерфейсы, наименование узлов)	
1. Подготовка отчета	2
1. Представлены скриншоты всех ключевых настроек	

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

2. *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).

3. *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.

Всего 20 баллов	Баллы
1. Развертывание ПК Administrator	12
1. ЦУС (серверное и клиентское приложение) установлен и настроен 2. Удостоверяющий и ключевой центр (УКЦ) установлен и настроен	
1. Установка ПО VPN Client	8
1. ПО Client рабочее место администратора установлено и настроено 2. ПО Client рабочее место пользователя установлено и настроено	

Модуль № 1: Эксплуатация информационно – телекоммуникационных систем и сетей

4. *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.

Всего 15 баллов	Баллы
1. Инициализация Coordinator HW-VA	15
1. Инициализация двух экземпляров Coordinator HW-VA произведена	

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

5. *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.

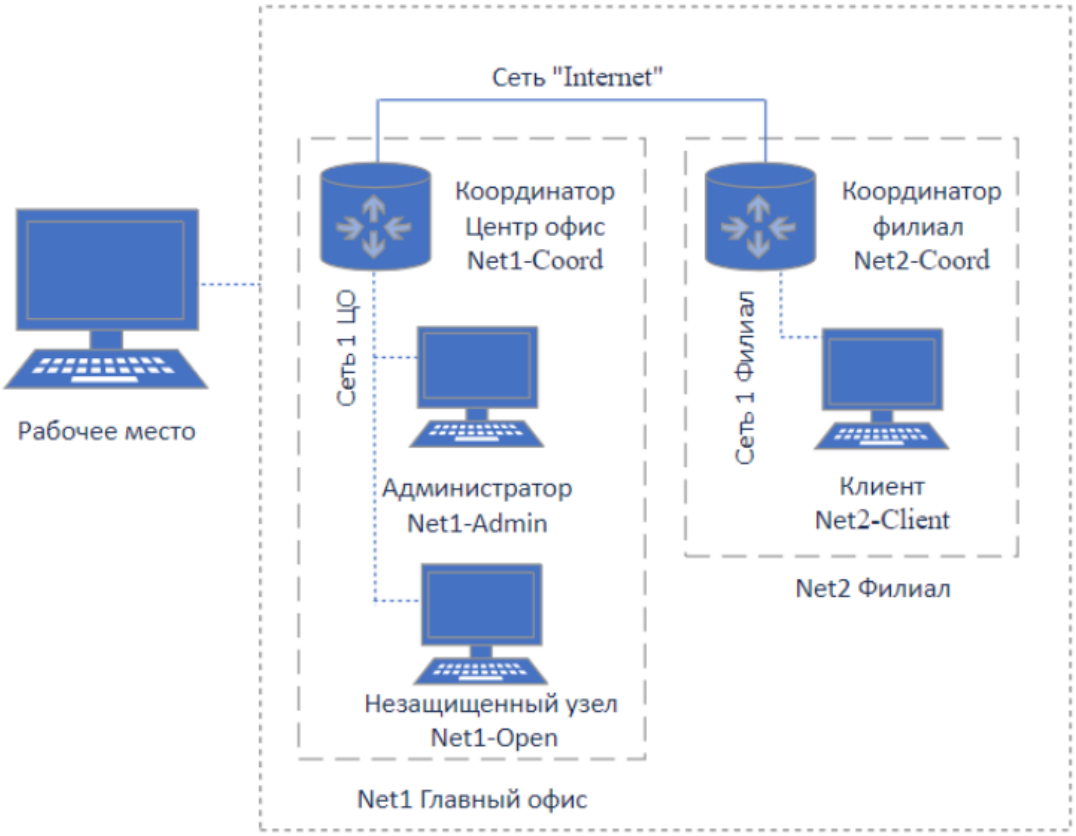

Рисунок 1 Схема защищенной сети

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, УКЦ), Client	Пользовательская или серверная ОС	AdmN
Net1-Coord (ЦО)	Координатор офиса	Coordinator	HW-VA	CoordO
Net2-Coord (филиал)	Координатор филиала	Coordinator	HW-VA	CoordB
Net2-Client (филиал)	Пользователь филиала	Client	Пользовательская или серверная ОС	UserB

6. *Задача 2.4. Создание структуры защищенной сети*

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

Таблица 2 - Схема связей пользователей

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

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

7. *Задача 2.5. Работа Деловой почты*

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.

8. *Задача 2.6. Межсетевое взаимодействие защищённых сетей*

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

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.

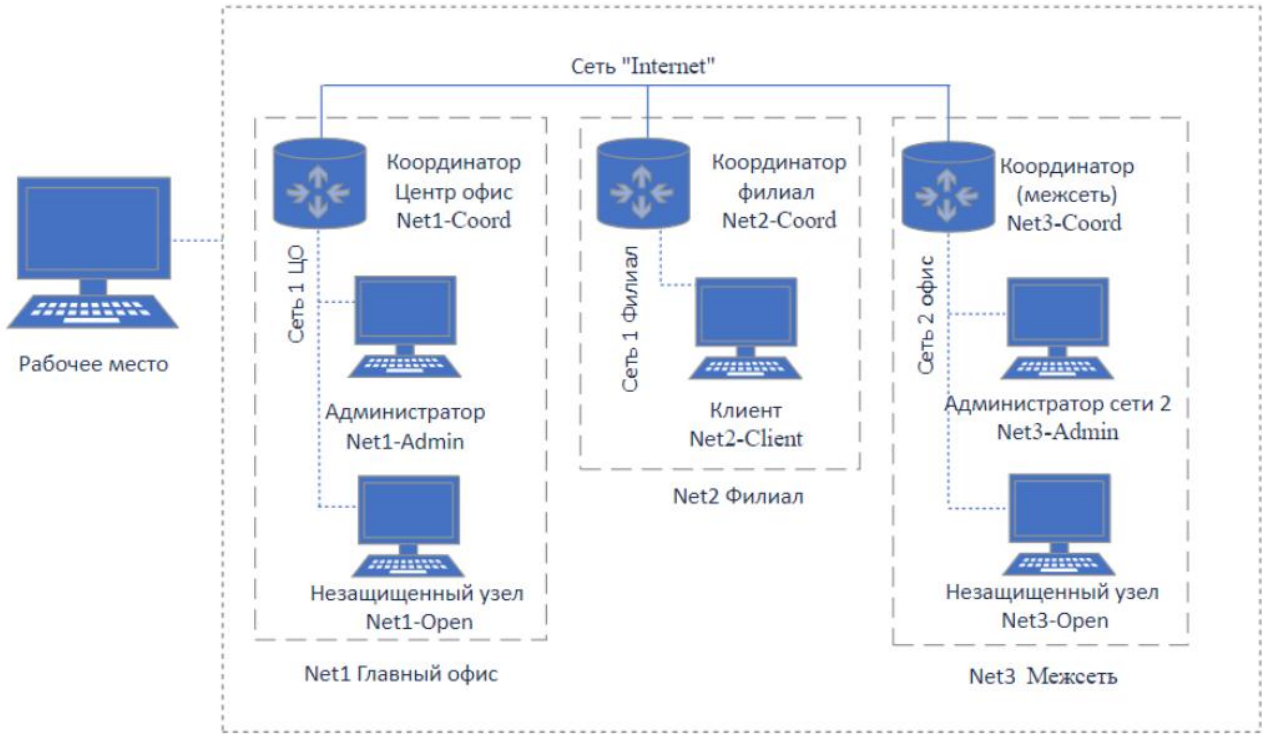

Рисунок 2 - Схема межсетевого взаимодействия

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

9. *Задача 2.7. Восстановление сетевого взаимодействия в случае компрометации ключей*

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.

10. *Задача 2.8. Настройка правил в сети.*

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

Всего 40 баллов	Баллы
1. Развертывание защищенной сети	8
1. Настроены все сетевые интерфейсы 2. Сетевые настройки соответствуют заданию 3. Наименование виртуальных машин, сетевых узлов, пользователей соответствуют заданию	
1. Создание структуры защищенной сети	12
1. Произведены необходимые настройки ЦУС 2. Проведена предварительная настройка рабочих станций (пароли, сетевые интерфейсы, наименование узлов)	

3. Сформированы и разнесены дистрибутивы ключей 4. Произведена первичная инициализация узлов сети 5. Проведена проверка доступности узлов сети
1. Деловая почта
1. Деловая почта работоспособна, что подтверждено отправкой тестового письма
1. Межсетевое взаимодействие защищённых сетей 5
1. Инициализация Coordinator HW-VA произведена 2. Межсетевое взаимодействие с использованием ассиметричного шифрования настроено 3. Произведена проверка работы межсетевого взаимодействия успешной отправкой Деловой почты
1. Восстановление сетевого взаимодействия 5
1. Произведена компрометация ключа 2. Произведена процедура замена ключа 3. Проверена работоспособность после восстановления
1. Настройка правил в сети 5
1. Сетевые фильтры настроены согласно задания 2. Произведено тестовое подключение по RDP
1. Подготовка отчета 5
1. Представлены скриншоты всех ключевых моментов задания

Модуль № 1: Эксплуатация информационно – телекоммуникационных систем и сетей

11. *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 шифрованному 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.

Всего 15 баллов	Баллы
1. Туннелирование в рамках межсетевого взаимодействия	10
1. Net3-Open подключена 2. Туннелирование настроено 3. Доступность незащищенных машин проверена	
1. Подготовка отчета	5
1. Представлены скриншоты всех ключевых моментов задания	