ЗАДАНИЕ
ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА
(2026 год)

Код и наименование профессии (специальности) среднего профессионального образования	10.02.05 Обеспечение информационной безопасности автоматизированных систем
Наименование квалификации (направленности)	Техник по защите информации
Вид аттестации	Государственная итоговая аттестация
Уровень демонстрационного экзамена	Профильный уровень
Шифр варианта задания	В3_КОД 10.02.05-1-2026-ПУ
Продолжительность ДЭ[1]	4 часа 0 минут

Вариант № 3

Модуль № 1 Настройка сетевого окружения, установка SQL-сервера

Продолжительность выполнения модуля задания: 0 ч. 20 мин.

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.

Для правильной работы сети надо создать или убедиться в наличии 4 сетей:

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

IP адреса защищенных сетей:

- Центральный офис «Сеть 1 ЦО»: 192.168.110.0/28

[1] Продолжительность ДЭ указана в соответствии с таблицей № 2 Том 1

- Офис филиал «Сеть 1 Филиал»: 10.10.10.0/26
- Офис сеть 2 «Сеть 2 Офис»: 172.21.10.0/27
- «Интернет» для всех координаторов: 198.18.10.0/20

Задача 1.1 Установить SQL-сервер, входящий в комплект дистрибутивов программного комплекса, на виртуальную машину Net1-Open (незащищенный узел).

Необходимые приложения:

Модуль № 2 Установка компонентов защищенной сети

Продолжительность выполнения модуля задания: 0 ч. 40 мин.

В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети, задать пароли пользователей и администраторов сети. Все пароли пользователей в сети: xxXX3344, все пароли администраторов в сети: 4433XXxx. В случае изменения каких-либо логинов или паролей необходимо отобразить это в отчете.

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

Задача 2.2. Инициализация VPN Coordinator и установка ПО VPN Client. На виртуальной машине Net1-AdminCA (ЦО) установить ПО VPN Client, рабочее место администратора, на виртуальной машине Net1-Coord (ЦО) инициализировать координатор.

Задача 2.3. Инициализация VPN Coordinator и установка ПО VPN Client для организации сети филиала. На виртуальной машине Net2-Coord (филиал)

инициализировать координатор, на виртуальной машине Net2-Client (филиал) установить ПО VPN Client, рабочее место пользователя.

В отчете необходимо зафиксировать процесс установки скриншотами форм, сделать скриншот директории, в которую установлено ПО, и скриншот первого запуска приложения.

Необходимые приложения:

Модуль № 3 Создание структуры защищенной сети

Продолжительность выполнения модуля задания: 0 ч. 30 мин.

Задача 3.1 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.

Необходимо создать в центре управления сетью структуру защищенной сети в соответствии с заданной схемой, представленной на рисунке 1. Создать пользователей узлов, настроить полномочия пользователей (таблица 1) и их связи в соответствии со схемой связей (таблица 2).

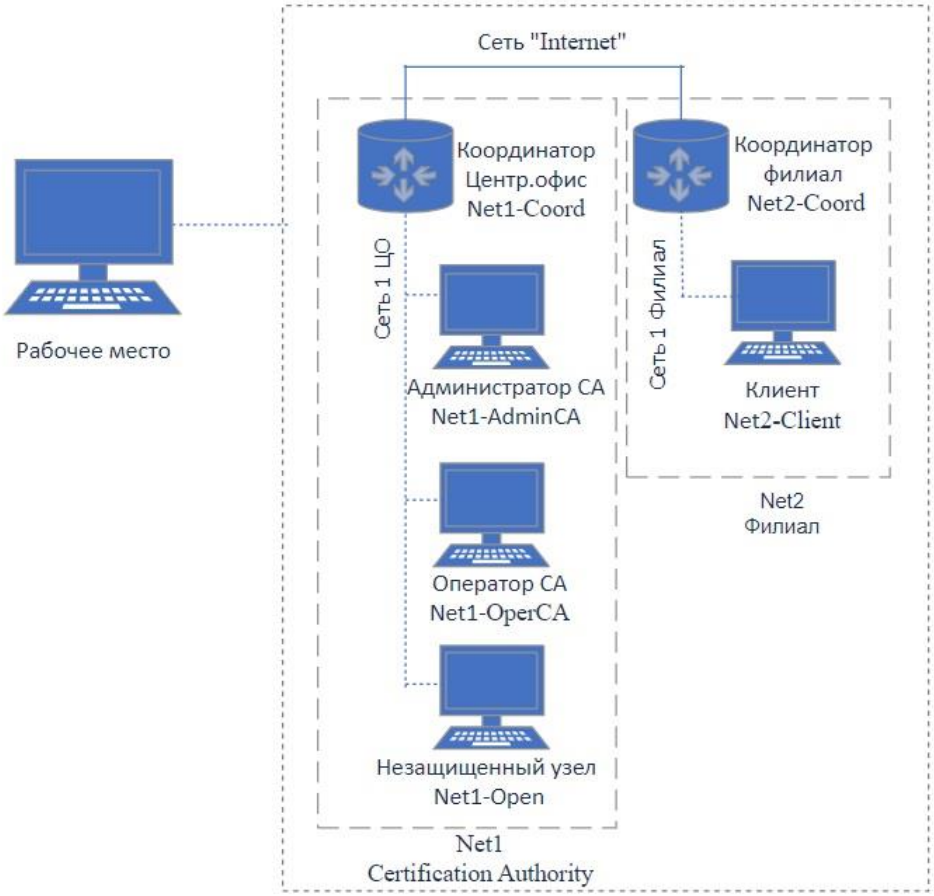

Рисунок 1 Схема защищенной сети

Таблица 1

Вирт. машина	Название сетевого узла	ПО	ОС сетевого узла	Имя пользователя сетевого узла
Net1-AdminCA (ЦО)	Администратор сети	Administrator (ЦУС сервер, УКЦ), Client, CA Informing	Пользовательская или серверная ОС	AdminCA
Net1-CoordCA (ЦО)	Координатор офиса	Coordinator	HW-VA	Coord_CO
Net1-OperatorCA (ЦО)	Оператор УЦ	Client, Publication Service, Registration Point	Пользовательская или серверная ОС	OperCA

Net2-Coord (филиал)	Координатор филиала	Coordinator	HW-VA	Coord_S
Net2-Client (филиал)	Пользователь филиала	Client	Пользовательская или серверная ОС	User_Br

Таблица 2

Пользователь	Coord_CO	AdminCA	OperCA	BranchCoord	User_Br
Coord_CO	×	*	*	*	
AdminCA	*	×	*		*
OperCA	*	*	×	*	
BranchCoord	*		*	×	*
User_Br		*		*	×

Задача 3.2. Провести инициализацию УКЦ, поменять тип паролей для пользователей («собственный»). Сформировать дистрибутивы ключей для всех сетевых узлов. Разнести дистрибутивы ключей по рабочим местам пользователей, провести первичную инициализацию узлов защищенной сети, проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задача 3.3. Отправить письмо по Деловой почте пользователю User_Br с узла пользователя AdminCA, отправить текстовое сообщение пользователю AdminCA от пользователя User_Br.

В отчете необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

- скриншоты деловой почты на отправителе и получателе (при отправке письма);
- скриншоты текстового сообщения на отправителе и получателе.

Необходимые приложения:

Модуль № 4 Установка компонентов удостоверяющего центра

Продолжительность выполнения модуля задания: 0 ч. 10 мин.

Задача 4.1 Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

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

В отчет внести скриншоты результата процесса установки программного обеспечения.

Необходимые приложения:

Модуль № 5 Настройка компонентов удостоверяющего центра. Компрометация пользователя

Продолжительность выполнения модуля задания: 1 ч. 20 мин.

Задача 5.1. Настройка работы удостоверяющего центра в аккредитованном режиме

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

- сведения о средствах УЦ,
- средство электронной подписи издателя: CSP,
- средства удостоверяющего центра: ПК УЦ 4
- сертификат на средство электронной подписи издателя: Сертификат DC.lab.crt
- сертификат на средство удостоверяющего центра: Сертификат DC.lab.p7b
- класс защищенности, которому соответствуют программные средства УЦ.

После перевода УКЦ в аккредитованный режим необходимо выпустить:

- корневой квалифицированный сертификат, назначить текущим,
- квалифицированные электронные подписи для пользователей AdminCA, User_Br; выдать с новым дистрибутивом ключей.

При формировании сертификатов необходимо заполнить следующие поля:

- Имя: <Имя пользователя или узла>
- Электронная почта: <Имя пользователя>@sec.lab
- Город: Калининград
- Область: Калининградская область
- Организация: ООО Легенда
- Подразделение: ИБ
- Почтовый индекс: 236001

Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации. Выполнить публикацию сертификатов пользователей сети в ручном режиме. Проверить результат публикации в Сервисе Публикации.

Посредством Центра Регистрации: зарегистрировать пользователя User_Br, отправить запрос в УКЦ на выпуск сертификата, удовлетворить

запрос. Отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос. Результаты отразить в отчёте.

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

В отчет поместить скриншоты процесса настройки Центра регистрации, Сервиса Публикации и Сервиса Информирования.

Задача 5.2. Компрометация пользователя

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

- скомпрометировать ключи пользователя User_Br 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_Br администратору с использованием чата.

В отчете необходимо зафиксировать процесс настройки скриншотами:

- компрометация пользователя,
- смена ключей пользователя и сетевых узлов,
- процедура смены ключа на клиенте,
- результат проверки доступности узлов.

Необходимые приложения:

Модуль № 6 Агрегирование каналов связи. Реализация межсетевого взаимодействия защищённых сетей

Продолжительность выполнения модуля задания: 1 ч. 00 мин.

Задача 6.1. Настроить агрегированный канал связи (интерфейс) на Net2-Coord в сторону внешней сети Inet. Применить режим, который используется для балансировки нагрузки на подчиненных физических интерфейсах и защищает от сбоев (преимущественно применим в сетях с простой топологией).

Задача 6.2. 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.

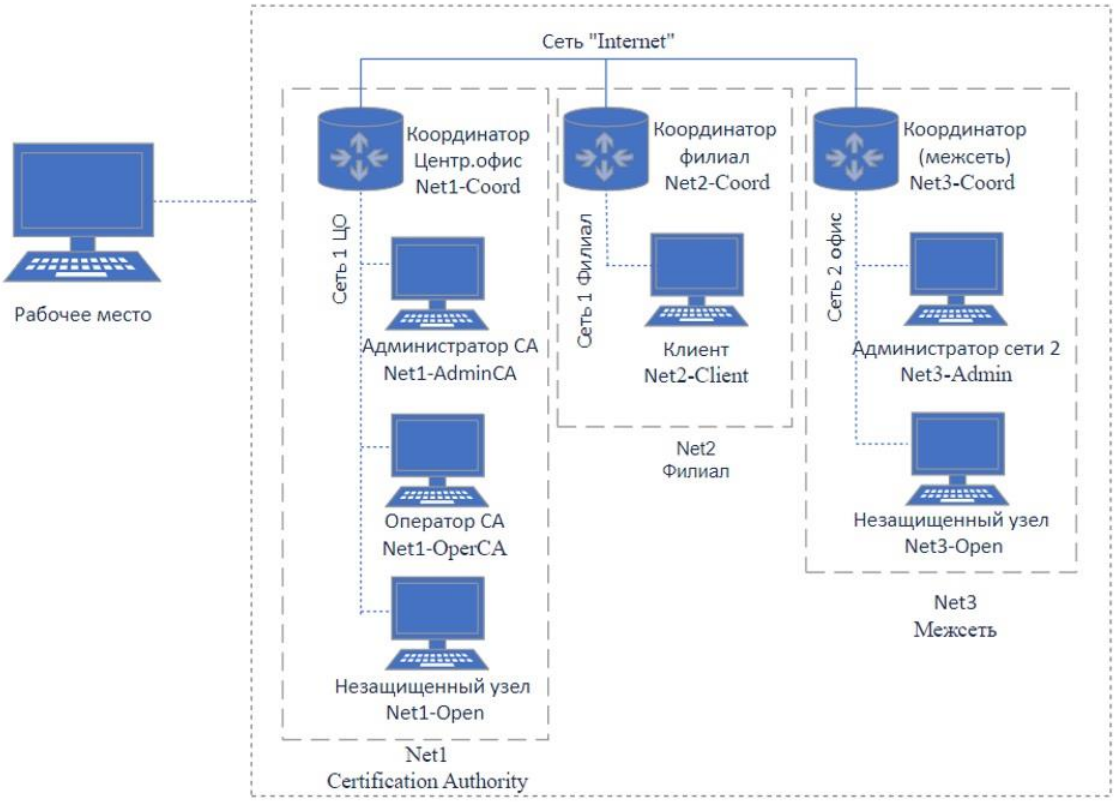

Рисунок 2

Создать структуру второй сети: рабочее место администратора на виртуальной машине Net3-Admin (БД, ЦУС, УКЦ, Client), координатор. Установить и настроить необходимое ПО. Настроить межсетевое взаимодействие, с использованием ассиметричных межсетевых ключей, между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

Задача 6.3. Проверить взаимодействие узлов, отправив сообщение чата и деловой почты с узла Администратор сети (Net1-AdminCA) на Admin (Net3-Admin). Скриншоты с результатами пересылки сообщений и писем поместить в отчет.

Необходимые приложения: