Образец Заданий для демонстрационного экзамена
Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Содержание задания ДЭ зависит от вида аттестации и уровня ДЭ. Продолжительность выполнения каждого задания представлена в таблице 11.

Таблица 11

Задания	Вид деятельности	Продолжительность выполнения Задания / Максимальная продолжительность ДЭ	
		ДЭ в рамках ПА	ГИА ДЭ БУ
Задание 1	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении	0 ч. 20 мин	0 ч. 20 мин.
Задание 2	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	0 ч. 40 мин.	0 ч. 40 мин.
Задание 3	Защита информации в автоматизированных системах программными и программно-аппаратными средствами	0 ч. 30 мин	0 ч. 30 мин
Задание 4	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении		0 ч. 10 мин.
Задание 5	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. Защита информации в автоматизированных системах программными и программно-аппаратными средствами		1 ч. 00 мин.
Задание 6	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении. Защита информации в автоматизированных системах программными и программно-аппаратными средствами		0 ч. 50 мин
Максимальная продолжительность ДЭ:		1 ч. 30 мин.	3 ч. 30 мин

Образец задания для ДЭ в рамках ПА

Задание 1. Настройка сетевого окружения, установка SQL-сервера

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 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. Внутренняя сеть адаптер для виртуального «Интернета».

IP адреса защищенных сетей:

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

Задание 2. Установка компонентов защищенной сети

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

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

Задача 2.2. Установка ПО VPN Client на рабочие места пользователей и для организации сети филиала

На виртуальные машины Net1-Admin, Net1-OperCA установить ПО Client (пользовательская или серверная ОС), на виртуальной машине Net2-Client (филиал) установить ПО Client, рабочее место пользователя. В отчете необходимо зафиксировать процесс установки скриншотами форм.

Необходимые приложения: отсутствуют.

Задание 3. Создание структуры защищенной сети

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 (таблица 1) и их связи в соответствии со схемой связей (таблица 2).

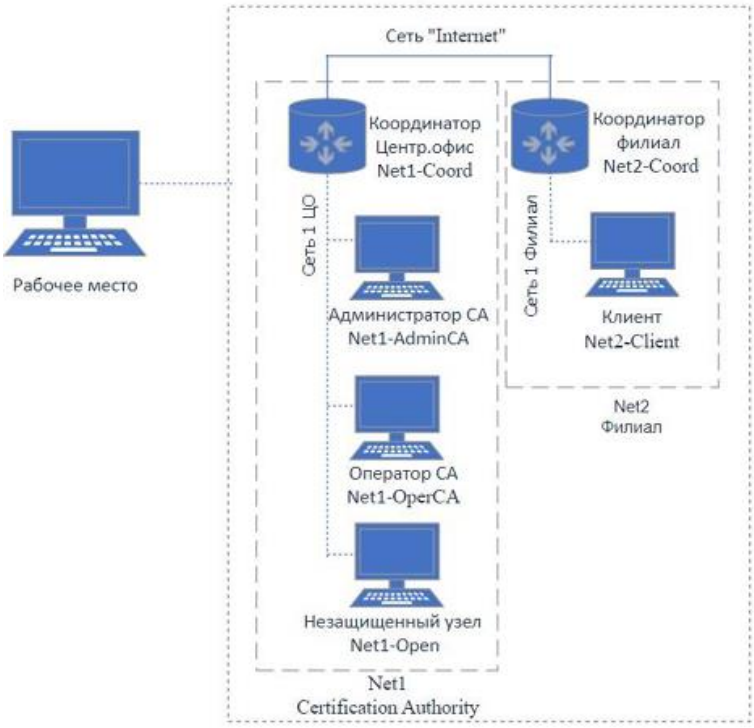


Рис. 1. Схема защищенной сети

Таблица 1

Узлы защищенной сети

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

Таблица 2

Схема связей пользователей

Пользователь	Root_ Coordinator	AdminS	Node_CR	Sub_Coordinator	Rem_Client
Root_ Coordinator	x	*	*	*	
AdminS	*	x	*		*
Node_CR	*	*	x	*	

Sub_Coordinator	*		*	x	*
Rem_Client		*		*	x

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.

Задача 3.3. Инициализация VPN Coordinator

На виртуальной машине Net1-Coord инициализировать Coordinator HWVA, на виртуальной машине Net2-Coord инициализировать Coordinator HW-VA.

Поверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задача 3.4. Отправить письмо по Деловой почте пользователю Rem_Client с узла AdminS, отправить текстовое сообщение пользователю AdminS от пользователя Rem_Client. В отчете необходимо представить скриншоты текстового сообщения и деловой почты на отправителе и получателе (при отправке письма).

Необходимые приложения: отсутствуют.

Задание 4. Установка компонентов удостоверяющего центра

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

1. На виртуальной машине Net1-OperCA установить ПО Client, Сервис публикации.
2. На виртуальной машине Net1-OperCA установить ПО Центр регистрации.
3. На виртуальной машине Net1-AdminCA установить ПО Сервис информирования.

Необходимые приложения: отсутствуют.

Задание 5. Настройка компонентов удостоверяющего центра. Компрометация пользователя

Задача 5.1. Настройка работы удостоверяющего центра в аккредитованном режиме.

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

После перевода УКЦ в аккредитованный режим необходимо выпустить:

– корневой квалифицированный сертификат, назначить текущим;

– квалифицированную электронную подпись для пользователя AdminS, выдать с новым дистрибутивом ключей;

– квалифицированную электронную подпись для пользователя Rem_Client, сохранить электронные ключи в файл.

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

Посредством Центра Регистрации: отправить запрос в УКЦ на выпуск сертификата пользователя Rem_Client, удовлетворить запрос. Отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

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

Задача 5.2. Компрометация пользователя

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС: скомпрометировать ключи пользователя Rem_Client на узле Удаленный клиент, произвести смену ключей пользователя и сетевых узлов, отправить обновления и произвести процедуру смены ключа пользователя на узле Удаленный клиент, проверить работу защищенной сети после обновления отправив сообщение от пользователя

Rem_Client администратору с использованием чата и Деловой почты. В отчете необходимо зафиксировать процесс настройки скриншотами.

Необходимые приложения: отсутствуют.

Задание 6. Реализация межсетевого взаимодействия 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.

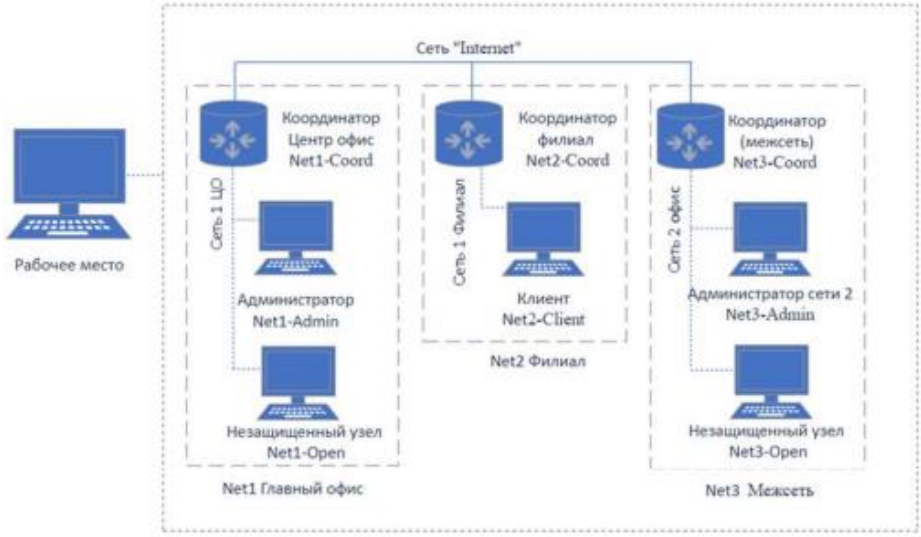


Рис. 2. Схема межсетевого взаимодействия

Создать структуру второй сети:

– рабочее место администратора на виртуальной машине Net3-Admin (БД, ЦУС, УКЦ, Client) - узел Admin и пользователь Admin;

– координатор (Net3-Coord).

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

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

Необходимые приложения: отсутствуют.