КОНКУРСНОЕ ЗАДАНИЕ

Региональные чемпионаты 2021-22

Сокращенное типовое задание - 85 баллов

Корпоративная защита от внутренних угроз информационной безопасности

Модуль 4
День 3

Менеджер компетенции: А.В. Сергеев

FUTURE SKILLS

Задание 1: настройка сетевого окружения и компонентов систем

С помощью технологии виртуальных машин *Vmware* для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах.

Необходимо самостоятельно настроить соединения между виртуальными машинами используя сетевые интерфейсы.

При выполнении заданий необходимо ключевые настройки (установка паролей, настройки соединения с БД, компрометация, скриншоты работоспособной сети ViPNet и аналогичные) или указанные моменты в задании подтверждать скриншотами. Скриншоты необходимо сохранить на рабочем столе в папке «Модуль InfoTeCS». Формат названия скриншотов: ITCS-1-2-1.jpg (задание 1.2, скриншот 1). Можно добавить комментарий (ITCS-1-2-1-Coordinator).

В ходе выполнения данного задания нужно установить основное ПО VipNet на рабочие станции будущей защищенной сети.

Доступ на все Windows 10: без пароля

Доступ на все Windows Server: логин: admin пароль: xxXX1234

Все пароли пользователей в сети ViPNet сделать 12344321

Все пароли администраторов в сети ViPNet сделать xxXX1234.

В случае изменения паролей обязательно отразить это в отчете!

Перед установкой ПО ViPNet необходимо настроить сеть в соответствии со схемой. Если машины для координаторов не маршрутизирует пакеты между интерфейсами, необходимо настроить это самостоятельно.

Необходимо записать все IP адреса, логины и пароли в текстовый файл vipnet.txt на рабочем столе хост-компьютера, где развернута сеть 1.

В связи с особенностями работы системы на различных версиях Windows может потребоваться устанавливать компоненты системы вручную (например БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов.

Все дистрибутивы и лицензии находятся на хост машине в папке Дистрибутивы ПО_УМК_2021 на жестком диске

При выполнении задания можно пользоваться документацией к ПО, презентациями из папки и справочными ресурсами в интернете.

Задание 1. Создание виртуальной машины Оператора УЦ

Необходимо склонировать (скопировать) любую ВМ сети 1 (например Net1-AdminCA) для последующего использования в качестве оператора.

Название новой ВМ: Net1-OperCA

В случае установки Админа и Оператора на 1 машину — это будет считаться некорректным выполнением, но допустимо для продолжения дальнейшей работы.

Задание 1.1. Установка ПО ViPNet Administrator для создания защищённой сети:

- Установить и настроить рабочее место администратора VipNet (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное и клиентское приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ).

Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.

Задание 1.2. Установка ПО ViPNet Coordinator и ПО VipNet Client на соответствующие виртуальные машины:

- На компьютере на Net1-AdminCA (ЦО) установить ПО ViPNet Client (Windows), рабочее место администратора;
- На компьютере на Net1-Coord (ЦО) установить ПО ViPNet Coordinator (Windows);
- На компьютере на Net2-Coord (Филиал) установить ПО ViPNet Coordinator (Windows);
- На ВМ на Net2-Client (филиал) установить ПО ViPNet Client, рабочее место пользователя;

  Необходим скриншот первого запуска приложения.

Задание 1.3. Установка центра регистрации, сервиса публикации и сервиса информирования VipNet Certification Authority на соответствующие виртуальные машины:

- На компьютере на Net1-OperCA(ЦО) установить ПО ViPNet Client (Windows);
- На компьютере на Net1-OperCA(ЦО) установить ПО ViPNet Publication Service;
- На компьютере на Net1-OperCA(ЦО) установить ПО ViPNet Registration Point;
- На компьютере на Net1-Admin (ЦО) установить ПО ViPNet CA Informing;

Задание 2. Защита локально-вычислительной сети предприятия с применением ПО ViPNet

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

Схема сети, которую требуется создать, приведена далее.

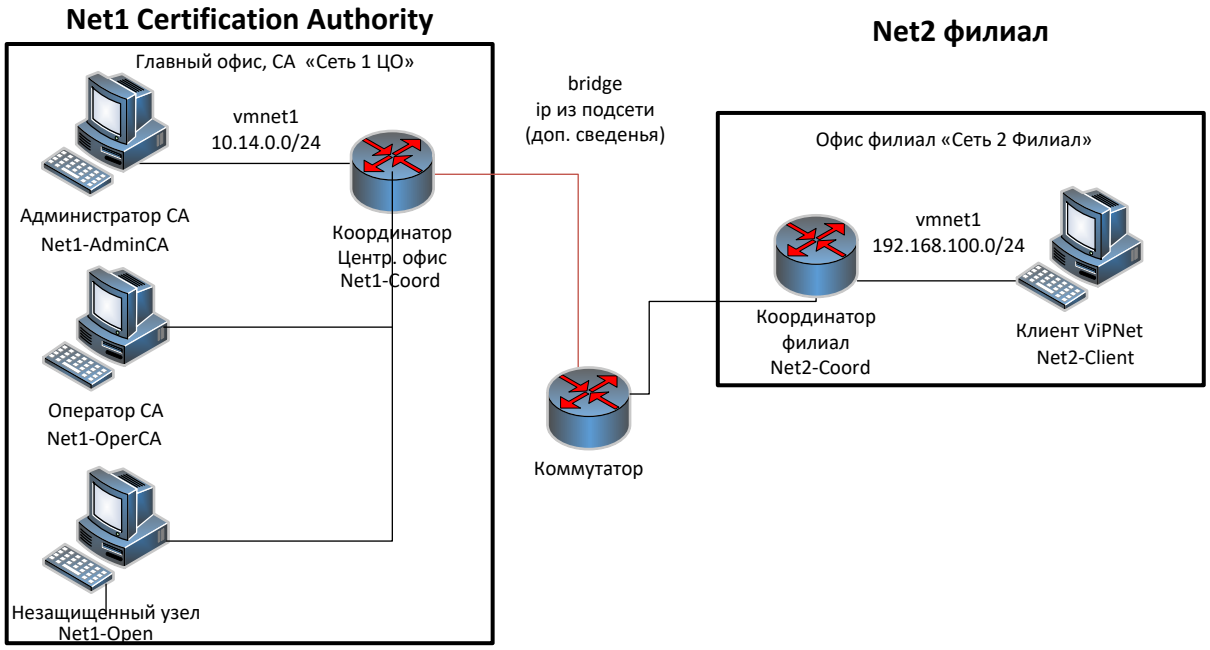

Рисунок 1 Схема защищенной сети

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

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	**Название сетевого узла**	**ПО VipNet**	**ОС сетевого узла**	**Имя пользователя сетевого узла, уровень полномочий**
Net1-AdminCA (ЦО)	Главный администратор (VM)	ViPNet Administrator (ЦУС клиент и сервер + УКЦ) ViPNet Client	ОС Windows 10	AdminCA

Net1-Coord (ЦО)	Координатор Центр Офис (VM)	ViPNet Coordinator	ОС Windows Server 2016	CoordinatorOffice
Net1-OperCA(ЦО)	Оператор УЦ	ViPNet Client ViPNet Publication Service ViPNet Registration	ОС Windows 10	OperCA
Net2-Coord (Филиал)	Координатор Филиал (VM)	ViPNet Coordinator	ОС Windows Server 2016	CoordinatorSub
Net2-Client (Филиал)	Пользователь_2 Филиал (VM)	ViPNet Client	ОС Windows 10	User2

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coordinator Office	AdminCA	OperCA	Coordinator Sub	User2
CoordinatorOffice	×	*	*	*	
AdminCA	*	×	*		*
OperCA	*	*	×	*	
CoordinatorSub	*		*	×	*
User2		*		*	×

Задание 2.1. Создание структуры защищенной сети

- ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой (**выгрузить отчет в HTML**). Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой.
- УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора на внешнем устройстве – токене (напр. Rutoken S) ИЛИ (что оценивается меньше), в общей подпапке Задание 2.1). Ппоменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп (проверить, что пароль работает).

- На всех узлах сети корректно настроить или проверить корректность настройки сетевых интерфейсов в соответствии со схемой (на координаторах 2 интерфейса – внешний и внутренний), проверить доступность соседних узлов.
- Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задание 2.2. 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: ViPNet CSP
- Средство удостоверяющего центра: ПК ViPNet УЦ 4
- Сертификат на средство электронной подписи издателя: Сертификат Demo.lab.crt
- Сертификат на средство удостоверяющего центра: Сертификат Demo.lab.p7b
- В настройках средства электронной подписи владельца сертификата ничего менять не требуется.
- Класс защищенности, которому соответствуют программные средства УЦ,

После перевода УКЦ в аккредитованный режим необходимо выпустить:

1. Корневой квалифицированный сертификат. Назначить текущим.
2. Квалифицированную электронную подпись для пользователя Admin. Выдать с новым дистрибутивом ключей.
3. Квалифицированную электронную подпись для пользователя Client. Сохранить электронные ключи в файл.

При выдаче сертификатов необходимо заполнить следующие поля:

Имя: <Имя пользователя или узла>

Электронная почта: <Имя пользователя>@demo.lab

Город: ___

Область: ___

Страна: RU

Организация: WorldSkills

Подразделение: Защита информационной безопасности

Почтовый индекс: 450000

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети.

Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (ViPNet Publication Service).

Настроить переход в автоматический режим (при бездействии администратора): передачу на публикацию и обновление CRL с периодичностью 1 день.

Реализовать автоматическую публикацию сертификатов издателей на FTP-сервере.

Посредством Центра Регистрации (ViPNet Registration Point):

- зарегистрировать пользователя: User2.
- Отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос. Результат выпуска сертификата зафиксировать скриншотом.
- Отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос. Результат зафиксировать скриншотом.

Посредством Сервиса Информирования (ViPNet CA Informing):

- Настроить способ выдачи уведомлений (файлы *.eml локально для последующей отправки должны сохраняться в папке на рабочем столе);
- Сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов (на рабочем столе).

Задание 2.3. Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя, т. к. в случае неудачной компрометации структура сети может нарушиться.

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

- скомпрометировать ключи пользователя User2 на узле Пользователь_2 Филиал
- произвести смену ключей пользователя и сетевых узлов,
- отправить обновления и произвести процедуру смены ключа пользователя на узле Пользователь_2 Филиал (фиксировать все шаги),
- проверить работу защищенной сети после обновления отправив сообщение от пользователя User2 администратору.

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами или иным указанным способом:

- **Компрометация пользователя.**
- **Смена ключей пользователя и сетевых узлов.**

- **Процедура смены ключа на клиенте с использованием резервного набора ключей.**
- **Скриншот экрана «защищенная сеть» в VipNet Monitor на узле Пользователь_2 Филиал + результат проверки доступности узлов.**

Кроме того, нужно сохранить архив директории, в которой расположен резервный набор ключей на рабочем столе компьютера (после смены ключей).

Необходимо делать скриншоты до, после и в процессе компрометации, иначе другие задания могут быть не зачтены в случае неудачной компрометации.

Задание 2.4. Модификация защищенной сети

Модификация структуры сети:

- Добавить новый сетевой узел Ivanov и пользователя Ivanov за координатором ЦентрОфис (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем User2. На указанных узлах проверить появление нового узла.
- Добавить пользователя Petrov на узле Пользователь_2 Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи.
- Отправить **письмо по Деловой почте** пользователю Petrov с узла admin.
- Отправить **текстовое сообщение пользователю** AdminCA от пользователя Petrov

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**
- **Скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.**

Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС.

Задание 3. Межсетевое взаимодействие защищённых сетей (со связями «все со всеми»)

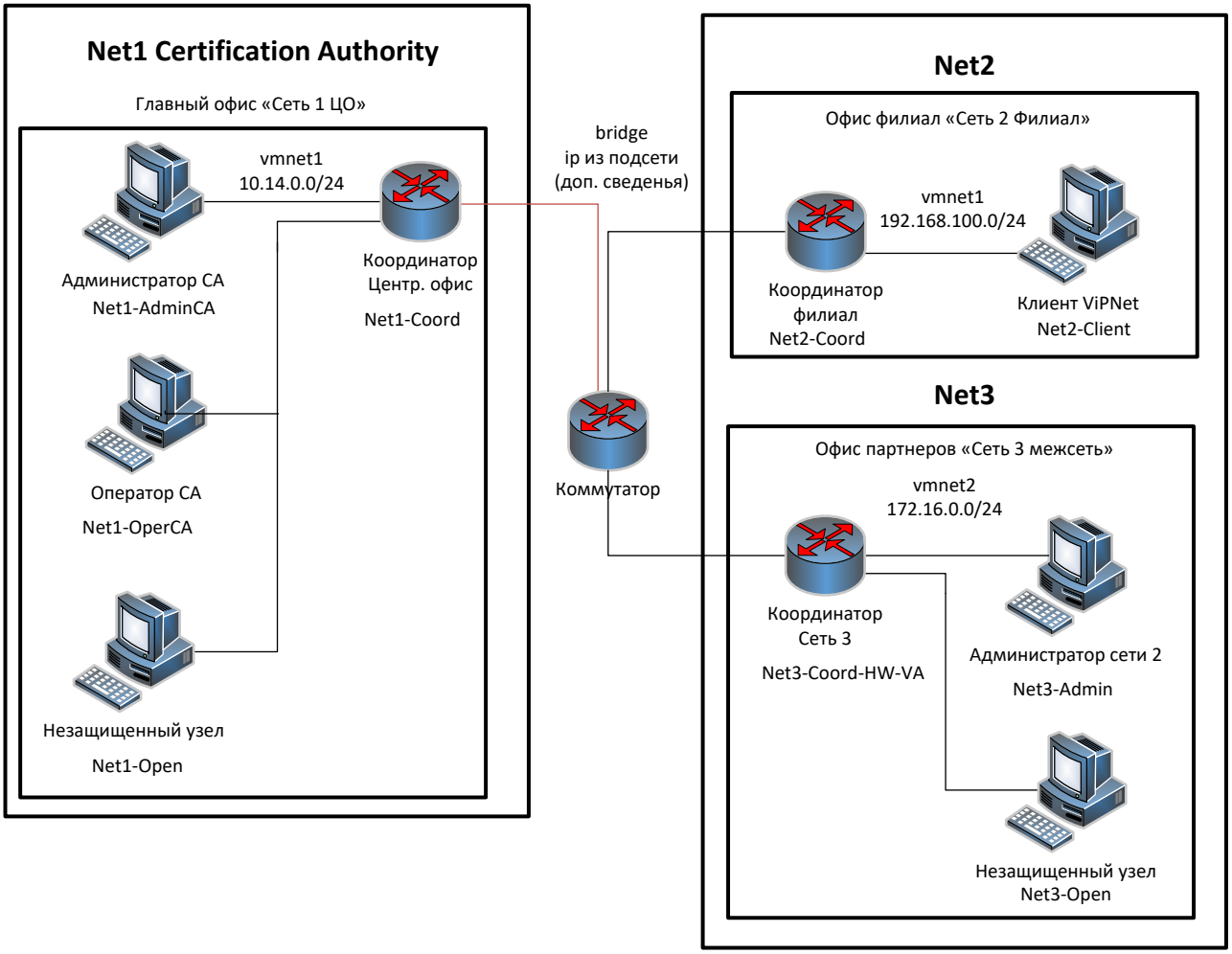

Рисунок 2 Схема межсетевого взаимодействия

Развернуть на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

- Рабочее место администратора (БД, ЦУС, УКЦ, ViPNet Client)
- 1 координатор (Net3-Coord-HW-VA)
- 1 узел Admin и пользователь Admin

Установите виртуальный координатор, развернув OVA-образ виртуальной машины HW-VA (из папки **Дистрибутивы ПО_УМК_2021** на жестком диске)

Все пароли пользователей в сети ViPNet сделать 12344321

Пароли администраторов сети ViPNet сделать xxXX1234

Установить и настроить необходимое ПО

- Настроить межсетевое взаимодействие между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.
- Проверить взаимодействие узлов, отправив **сообщение деловой почты** в программе ViPNet Client Monitor с узла Admin (сеть 1) на Admin (сеть 2).

Необходимо предоставить:

Файлы HTML структуры защищенной сети для обеих сетей после выполнения задания.

Скриншоты:

- **Скриншоты ключевых этапов установки межсетевого взаимодействия и обработки межсетевой информации (в ЦУС и УКЦ обеих сетей).**
- **Структура защищенной сети в ЦУС после установления межсетевого взаимодействия (для обеих защищенных сетей) с экраном проверки доступности узлов.**
- **Скриншоты деловой почты на отправителе и получателе (при отправке письма).**
- **Скриншоты текстового сообщения на отправителе и получателе (при отправке письма).**

Задание 3.1. Настройка координатора ПАК HW-VA

Для настройки HW-VA необходимо:

- Включить SSH доступ к HW-VA для удаленного управления внутри локальной сети
  Предоставить скриншоты создания/настройки правил и скриншот работоспособной SSH-сессии к HW-VA
  При необходимости на виртуальные машины можно самостоятельно установить любой SSH-клиент
- Включить удаленный доступ через web-интерфейс внутри локальной сети, настроив соответствующие правила firewall и проверить работоспособность
  Предоставить скриншоты создания/настройки правил и скриншот работоспособной веб-консоли HW-VA

Задание 4. 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.

Скриншоты:

- **Настройка максимального количества туннелей на координаторах**
- **Скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла**
- **Скриншоты журнала IP-пакетов координатора с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования**