

Региональный этап чемпионата по
профессиональному мастерству «Профессионалы» и
чемпионата высоких технологий Республики
Башкортостан

по компетенции:

F7 «Корпоративная защита от внутренних угроз
информационной безопасности»

Конкурсное задание

День 3

Уфа 2023

Модуль Г: Технологии защиты и анализа сетевого трафика

Задание 1: настройка сетевого окружения и компонентов систем

С помощью технологии виртуальных машин VMWare и аппаратных ViPNet Coordinator HW для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах и 1 офисе партнеров.

Необходимо самостоятельно настроить соединения между виртуальными машинами и аппаратными ViPNet Coordinator HW 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 **правого хост-компьютера** 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).

Делать лишние скриншоты установки ПО нет необходимости, только скриншоты работоспособности!

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

Доступ на все Windows 10: xxXX1234 или без пароля.

Все пароли пользователей в сети ViPNet сделать 12344321

Все пароли администраторов в сети ViPNet сделать XxXX1243

В случае изменения паролей обязательно отразить это в отчете!

Перед установкой ПО ViPNet необходимо настроить сеть в соответствии со схемой.

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.

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

Схема сети, которую требуется создать, приведена далее.

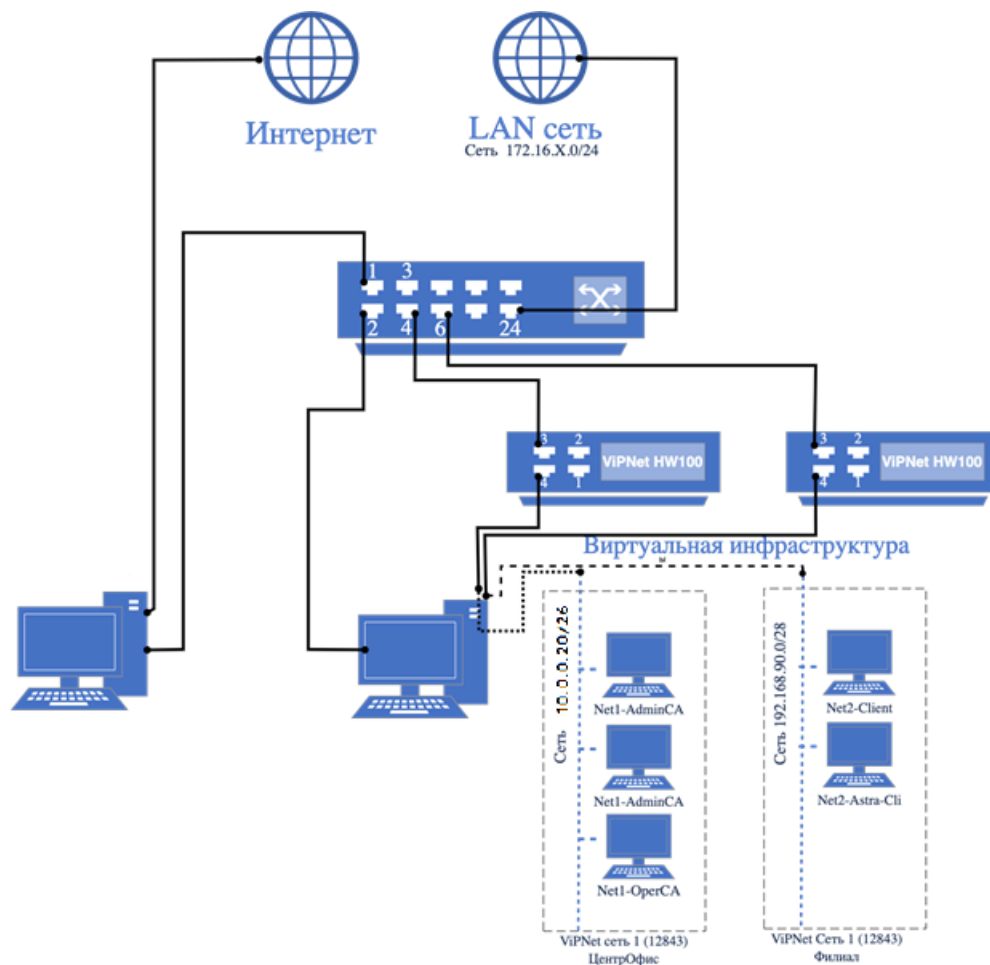


Рисунок 1 Схема защищенной сети

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

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

- Установить базу данных MSSQL на Net1-Open (незащищенный узел)
- Установить и настроить рабочее место администратора VipNet Certification Authority (на базе виртуальной машины Net1-AdminCA (ЦО)): Центр управления сетью (серверное и клиентское приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД.
- Установить клиент ЦУС на VM Net1-Open (незащищенный узел)

Установка «Все-в-одном» будет считаться некорректным выполнением развертывания, но

допустимо для продолжения дальнейшей работы.

- На компьютере на Net1-AdminCA (ЦО) установить ПО ViPNet Client (Windows), рабочее место администратора;
- Установить **Policy Manager** на Net1-AdminCA

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

Задание 1.2. 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-AdminCA (ЦО) установить ПО ViPNet CA Informing;

Задание 1.3. Установка ПО VipNet для организации сети филиала:

- На VM Net2-Client (филиал) установить ПО ViPNet Client Windows, рабочее место пользователя;
- На VM Net2-Astra-Cli (филиал) установить ПО ViPNet Client Linux, рабочее место пользователя;

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

Необходимо использовать рабочее место администратора для создания структуры защищенной сети предприятия и настроить необходимые АРМ в соответствии с заданными ролями. 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 узла
Net1-AdminCA (ЦО)	Главный администратор (VM)	ViPNet Administrator (ЦУС сервер + УКЦ) ViPNet Client ViPNet CA Informing	ОС Windows 10	Admin (защита с помощью токена, способ аутентификации: устройство)

Net1-OperCA (ЦО)	Оператор УЦ	ViPNet Client ViPNet Publication Service, ViPNet Registration Point	OC Windows 10	OperCA
Net1-Open (ЦО)	Клиент ЦУС, База данных ЦУС	Клиент ЦУС, БД MSSQL	OC Windows 10	—
Net1-Coord HW (ЦО)	Координатор Центр Офис (VM)	ViPNet Coordinator HW	HW-VA	CoordinatorOffice
Net2-Coord HW (Филиал)	Координатор Филиал (VM)	ViPNet Coordinator HW	HW-VA	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	ViPNet Client	OC Windows 10	User2
Net2-Astra-Cli (филиал)	Пользователь_3 Филиал (VM)	ViPNet Client	OC Astra Linux SE	User3

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coord Office	Admin	OperCA	Coord Sub	User2	User3
Coord Office	×	*	*	*		
Admin	*	×	*		*	*
OperCA	*	*		×		
Coord Sub	*			×	*	*
User2		*		*	×	*
User3		*		*	*	

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.

Настроить ViPNet клиент администратора на вход с помощью токена (способ аутентификации: устройство). Зафиксировать процесс записи информации на токен с помощью скриншота.

- УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке (создать подпапку Задание 2.1), поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл на рабочем столе. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса (удостоверяющего центра) 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, 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.
- Произвести первичную инициализацию аппаратного HW 1 и аппаратного HW 2
 - Настроить удаленный доступ через веб интерфейс к HW 1 с открытого узла своей сети
 - Настроить удаленный доступ по SSH к HW 1 с открытых узлов своей сети

Если у Вас возникают трудности с настройкой аппаратных HW, для продолжения работы Вы можете воспользоваться машинами HW VA. Однако, использование данных машин приводит к снижению баллов.

Необходимо проверить работоспособность сети с помощью отправки текстовых сообщений между Администратором и пользователем филиала.

Необходимо проверить работоспособность сети с помощью отправки деловой почты между Администратором и пользователем филиала.

Отправку и получение сообщений зафиксировать скриншотами.

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 DSDemo.lab.crt
- Сертификат на средство удостоверяющего центра: Сертификат DSDemo.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 User2. Сохранить электронные ключи в файл.
- 4) При выдаче сертификатов необходимо заполнить следующие поля:

Имя: <Имя пользователя или узла>

Электронная почта: <Имя пользователя>@demo.lab

Город: Уфа

Страна: RU

Организация: Профессионалы

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):

- Сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов (на рабочем столе).

Задание 2.3. Сервер установки штампа времени и подписание OCSP.

Компании необходим сервер, отвечающий за выдачу штампов времени пользователям. Поэтому в сети филиала на узле с клиентом ViPNet должен быть установлен сервер TSP-OCSP (ПК ViPNet УЦ 4).

Для функционирования сервера необходимо издать сертификат для TSP сервиса. Поместить контейнер ключей и сертификат необходимо в программу VipNet CSP. И после указать изданный сертификат для TSP в программе TSP-OCSP Service.

Также для корректной работы TSP сервера необходимо на работающем сервере УКЦ создать политику применения, которая будет использоваться для выдачи дальнейших сертификатов:

- Наименование: test TSP Policy
- Идентификатор: 1.2.643.100.1.2.3
- Краткое описание: Проверка штампа времени

Для TSP сервера необходимо задать эту политику применения по умолчанию.

Перед запуском TSP-OCSP сервера, требуется провести небольшую настройку:

- Номер порта сервера: 8777
- Серийный номер: 01 00 00 00 00 00 00 00
- Параметры OSCP-сервера: отключить все функции.

Задание 2.4. 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 user 2 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 user 2 администратору.

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Необходимо зафиксировать процесс настройки скриншотами:

- 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.

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

Задание 3. Межсетевое взаимодействие защищённых сетей

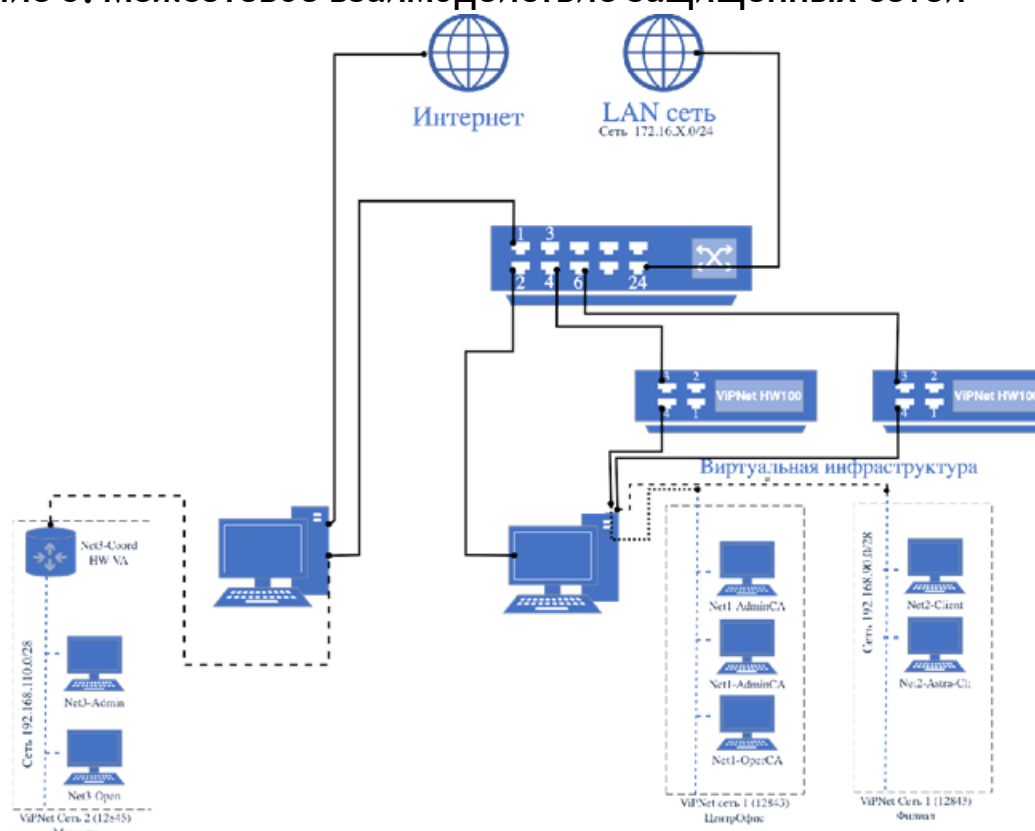


Рисунок 2 Схема межсетевого взаимодействия

Развернуть на Net3-Admin (Сеть 2 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

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

Настроить связи узлов/пользователей администраторов и необходимых для работоспособности узлов и проверки задания.

Инициализируйте HW-VA: при настройке необходимо включить DHCP сервер

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 правил в сети

- Необходимо настроить удаленное подключение по протоколу RDP между узлом Net3-Open и Net2-Client
- Необходимо настроить доступ к SSH по порту 2522 с узла Net3-Open до узла Net2-Astra-Cli

Предоставить скриншоты создания/настройки правил и скриншоты работоспособности: RDP сессии, Подключения к SSH.

Задание 3.2. Policy manager

3.2.1 Создать шаблон политики безопасности, т. е. определить сетевой фильтр в соответствии с которым Net2-Astra-Cli должен быть доступен по SSH только с узлов Admin СА и внешней сети (фильтр защищенной сети) для работоспособности соединения с Net3-Open. При этом, необходимо порт SSH на машине Net2-Astra-Cli изменить на 4567.

Назначить сформированный шаблон сетевым узлам, отправить политику безопасности на сетевой узел.

Зафиксировать результат (скриншотами) через журнал отправки и применения политик безопасности, на узлах в Мониторе просмотреть списки сетевых фильтров.

3.2.2 Создать шаблон политики безопасности для запрета на использование популярных соцсетей instagram.com, facebook.com, tiktok.com с узлов пользователей сети (клиенты).

Применить политику к клиентам. Зафиксировать результат (скриншотами)

настройки и проверки.

3.2.3 Создать шаблон политики безопасности для возможности подключения защищенных и незащищенных узлов своей сети по протоколу RDP к AdminCA. Также необходимо включить RDP доступ на данном узле.

Применить политику к устройствам. Зафиксировать результат (скриншотами) настройки и проверки.

3.2.3 Создать шаблон политики безопасности для возможности подключения защищенных и незащищенных узлов своей сети по протоколу RDP к Net3-Admin. Также необходимо включить RDP доступ на данном узле.

Применить политику к устройствам. Зафиксировать результат (скриншотами) настройки и проверки.

Задание 4. Туннелирование в рамках межсетевого взаимодействия

- Подключить незащищенную машину в сети 3
- Для второй открытой машины использовать узел в сети 1
- Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по зашифрованному каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping); 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 прохождения IP-пакетов на веб-интерфейсе с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования

Задание 5. Кластер горячего резервирования

В связи с участвовавшими случаями «падения» координатора межсети было принято решение добавить дополнительный координатор HW-VA в «Сеть 2 Межсеть» в дополнение к Net3-Coord HW-VA.

Для настройки необходимо самостоятельно развернуть соответствующий OVA-образ из дистрибутивов в сегмент межсети, настроить горячее резервирование и проверить работоспособность отключением одного из координаторов (система не должна прекращать работать при отключении одного из устройств от сети или питания).

Выбор IP координаторов и виртуальных адресов выбирается самостоятельно и записывается в отчет на рабочем столе.

Скриншоты:

- Развертывание нового координатора и инициализация (достаточно установку ключевой информации)
- Скриншот изменения конфигурации для кластера горячего резервирования

Оба координатора необходимо оставить включенными!