ЗАДАНИЕ 1: НАСТРОЙКА СЕТЕВОГО ОКРУЖЕНИЯ И КОМПОНЕНТОВ СИСТЕМ

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

Необходимо самостоятельно настроить соединения между виртуальными машинами используя предустановленные сетевые интерфейсы (Net[X]_lan и INTERNET).

Все виртуальные машины (кроме отрытого узла) имеют интерфейс Wan_shared (DHCP, имеет связь с RDP машиной и всеми ВМ), которым можно пользоваться при первоначальной настройке для распространения ключей/дистрибутивов.
После настройки данный сетевой адаптер необходимо отключить в ОС!

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 7: без пароля

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 включить эту опцию самостоятельно.

Необходимо записать все IP адреса, логины и пароли в текстовый файл vipnet.txt на рабочем столе компьютера.

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

Все дистрибутивы находятся на диске “C” каждой виртуальной машины или в общей сетевой папке \\192.168.111.250 , логин/пароль: share : xxXX1234

Лицензии (на 2 сети ViPNet с межсетевым взаимодействием) находятся в общей сетевой папке.
При выполнении задания можно пользоваться документацией к ПО, презентациями из общей папки и справочными ресурсами в интернете.

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-Admin (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 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 ESXi* сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена далее.

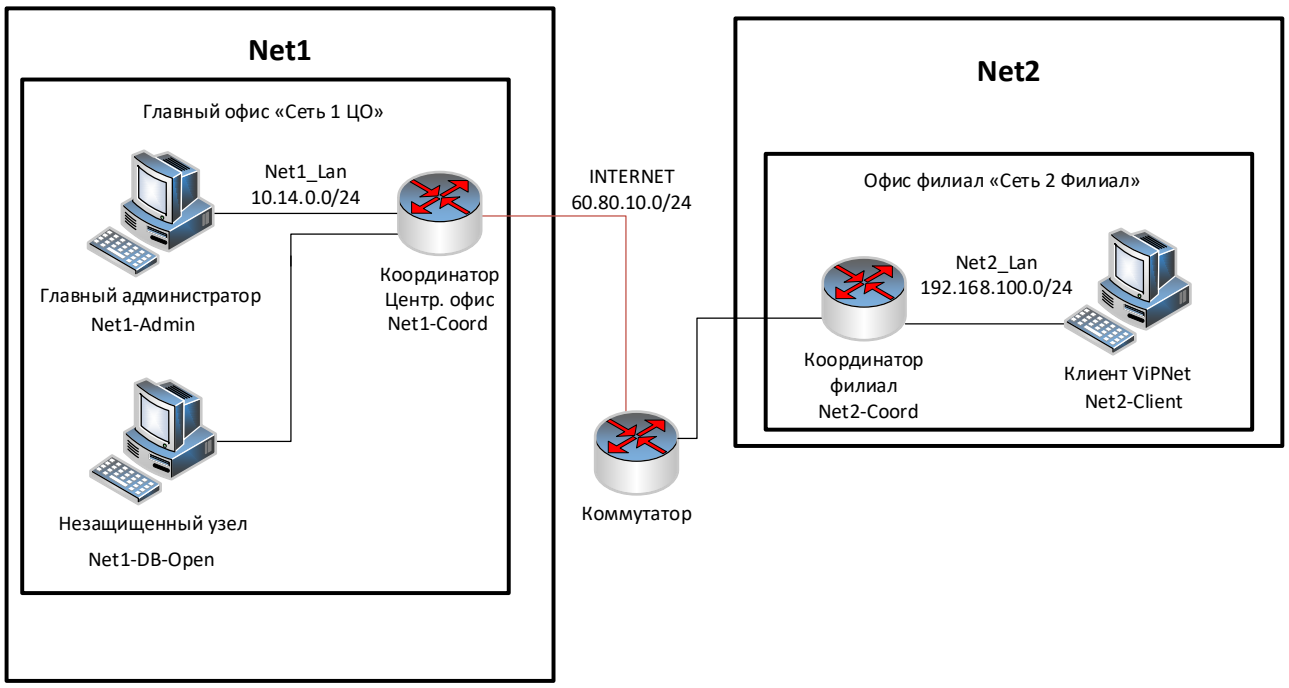

Рисунок 1 Схема защищенной сети

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-Admin (ЦО)	Главный администратор (VM)	ViPNet Administrator (ЦУС клиент и сервер + УКЦ) ViPNet Client	ОС Windows 7	Admin
Net1-Coord (ЦО)	Координатор Центр Офис (VM)	ViPNet Coordinator	ОС Windows 7	CoordinatorOffice
Net2-Coord (Филиал)	Координатор Филиал (VM)	ViPNet Coordinator	ОС Windows 7	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал (VM)	ViPNet Client	ОС Windows 7	User2

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coordinator Office	Admin	Coordinator Subsidiary	User2
CoordinatorOffice	×	*	*	
Admin	*	×		*
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 в общей папку (создать подпапку Задание 2.1), поменять 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. 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 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).

ЗАДАНИЕ 2.3. МОДИФИКАЦИЯ ЗАЩИЩЕННОЙ СЕТИ

Перед началом выполнения сделать Snapshot всех модифицируемых машин.

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.

Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

- **Скриншоты деловой почты на отправителе и получателе (при отправке письма)**
- **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»)

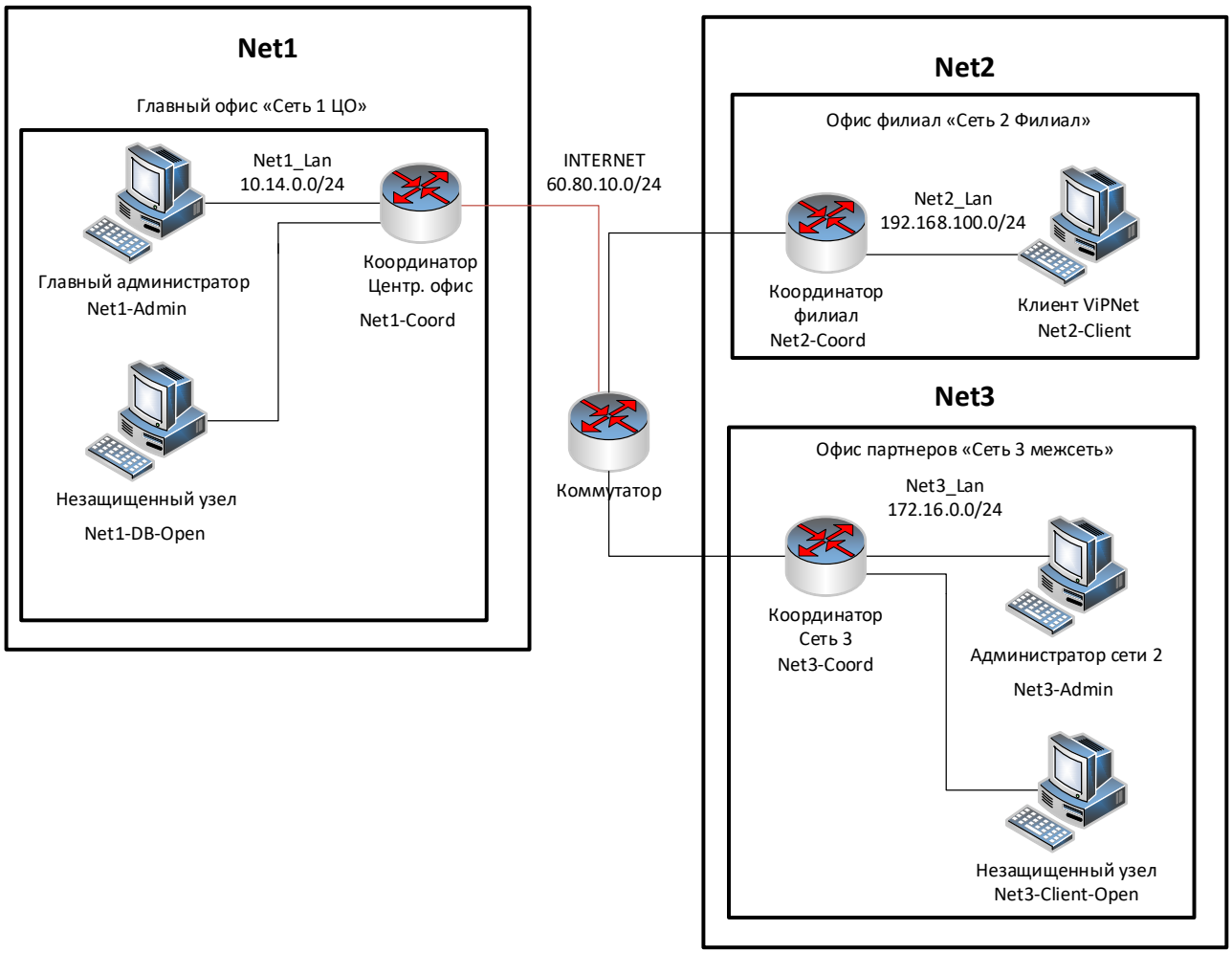

Рисунок 2 Схема межсетевого взаимодействия

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)
- 1 узел Admin и пользователь Admin

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).**

После настройки вспомогательный сетевой адаптер Wan_Shared необходимо отключить!

ЗАДАНИЕ 2. ТУННЕЛИРОВАНИЕ В РАМКАХ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

- Подключить незащищенную машину в сети 3 (Net3-Client-Open).
- Для второй открытой машины использовать Net1-DB-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); проанализировать журналы IP-пакетов на координаторах.

Скриншоты:

- **Настройка максимального количества туннелей на координаторе**
- **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**