Администрирование системы защиты информации ViPNet.

ПРАКТИКУМ

Принцип функционирования защищенной сети ViPNet

Сеть ViPNet представляет собой наложенную сеть, которая может быть развернута поверх локальных или глобальных сетей любой структуры. Для защиты информации в сети ViPNet используются такие технологии как:

- фильтрации трафика – технология, обеспечивающая комплексную фильтрацию всех входящих и исходящих открытых и защищенных IP-пакетов.
- VPN – технология, обеспечивающая защиту соединений между локальными сетями или отдельными компьютерами с использованием средств криптографии.
- PKI – технология, основным элементом которой является использование пары асимметричных ключей для формирования электронной подписи, аутентификации и других целей.

Сеть ViPNet состоит из сетевых узлов – компьютеров, на которых установлено программное обеспечение ViPNet. Сетевые узлы делятся на две категории:

- Координаторы – серверы сети ViPNet. Одна из функций координатора – маршрутизация прикладных и управляющих транспортных конвертов, передаваемых между клиентами.
- Клиенты – защищенные рабочие места пользователей сети ViPNet.

Для каждого сетевого узла администратор сети ViPNet задает набор ролей, от которого зависят возможности узла и программное обеспечение, которое может быть установлено на этом узле. Список ролей, которые могут быть использованы в сети, ограничения на количество узлов с различными ролями, максимальное количество сетевых узлов и другие ограничения содержатся в файле лицензии на сеть ViPNet.

В защищенной сети ViPNet, построенной с использованием технологии VPN и фильтрации трафика, Координаторы могут быть программной реализации ViPNet Coordinator for Windows, либо ViPNet Coordinator for Linux, а также программно-аппаратные комплексы ViPNet Coordinator HW и Клиенты – ПО ViPNet Client. Для создания отказоустойчивого решения на базе ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW предназначена система защиты от сбоев ViPNet Failover.

Клиенты и координаторы, на которых установлено ПО ViPNet, называются защищенными узлами. Сетевые узлы, на которых не установлено это программное обеспечение, называются открытыми. В сети ViPNet также могут присутствовать туннелируемые узлы.

В зависимости от потребностей и применяемой политики безопасности ПО ViPNet Coordinator может выполнять следующие задачи:

- Сервер IP-адресов – функция, которая в автоматическом режиме обеспечивает взаимодействие защищенных узлов (клиентов и координаторов) как внутри данной виртуальной сети, так и при взаимодействии с другими виртуальными сетями ViPNet. Это возможно благодаря использованию специального протокола динамической маршрутизации VPN-трафика, реализующего обмен информацией о параметрах доступа узлов друг к другу. Данный протокол обеспечивает маршрутизацию VPN-трафика между узлами в сети ViPNet тем методом, который наиболее оптимален для используемого способа подключения узла к сети.
- Маршрутизатор VPN-пакетов – функция, обеспечивающая маршрутизацию транзитного защищенного трафика, проходящего через координатор, на другие защищенные узлы. Маршрутизация осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется трансляция адресов (NAT). В случае фильтрации и трансляции трафика сторонними устройствами координатор может выступать в роли координатора соединений.
- VPN-шлюз – стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты.
- Сервер-маршрутизатор – функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами между узлами.
- Межсетевой экран – функция, благодаря которой координатор выполняет фильтрацию открытых и защищенных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.

Координаторы, работающие под ОС Windows, ОС Linux и ПАК ViPNet Coordinator HW, могут также выполнять функцию TCP-туннеля, то есть обеспечивать получение IP-пакетов по протоколу TCP и их дальнейшую передачу по протоколу UDP.

В сегментированных сетях можно использовать каскадную схему установки координаторов.

ПО ViPNet Coordinator или ViPNet Client, установленное на прикладном сервере, можно использовать для защиты трафика определенных прикладных сервисов (например, контроллер домена, SMTP/FTP/веб-службы, сервер базы данных).

В сети ViPNet существует возможность централизованного управления политиками безопасности на сетевых узлах. С помощью программы ViPNet Policy Manager, установленной на одном из клиентов, для отдельных узлов или групп формируются шаблоны политики безопасности, содержащие сетевые фильтры и правила трансляции.

Для наблюдения за состоянием сетевых узлов в сети ViPNet можно развернуть комплекс мониторинга защищенной сети ViPNet StateWatcher. Сервер мониторинга собирает информацию о состоянии сетевых узлов и установленных на них компонентах ПО ViPNet. При обнаружении сбоев система оповещает об этом администратора сети.

Кроме того, сеть ViPNet может включать терминальные клиенты для организации защищенных удаленных рабочих мест пользователя, мобильные клиенты на платформе iOS или Android и другие специализированные решения.

Программный комплекс ViPNet Client предназначен для защиты рабочих мест корпоративных пользователей. ViPNet Client надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика. Кроме того, ПК ViPNet Client обеспечивает защищенную работу с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей.

Программный комплекс ViPNet Client выполняет следующие функции:

- VPN-клиент (шифрование и имитозащита IP-пакетов).
- Персональный сетевой экран (в версии ViPNet Client for Windows, ViPNet Client for Linux).
- Контроль сетевой активности приложений и компонентов операционной системы (в версии ViPNet Client for Windows).
- ViPNet Client работает в составе сети ViPNet и совместим со всеми продуктами линейки ViPNet Network Security.

ViPNet Client поддерживает работу на компьютерных устройствах под управлением ОС Microsoft Windows, Linux и OS X.

ПК ViPNet Client входит в реестр Российского ПО (https://reestr.minsvyaz.ru/reestr/75098/).

Варианты поставки

Программный комплекс ViPNet Client 4 поставляется в трех вариантах исполнения, соответствующих классам защищенности от КС1 до КС3.

- Поставка ПК ViPNet Client 4 в варианте исполнения 1 в соответствии с формуляром ФРКЕ.00116-03 30 01 ФО обеспечивает класс защищенности КС1.
- Поставка ПК ViPNet Client 4 в варианте исполнения 2 в соответствии с формуляром ФРКЕ.00116-03 30 01 ФО обеспечивает класс защищенности КС2 при совместном использовании с сертифицированным аппаратно-программным модулем доверенной загрузки (АПМДЗ).
- Поставка ПК ViPNet Client 4 в варианте исполнения 3 в соответствии с формуляром ФРКЕ.00116-03 30 01 ФО обеспечивает класс защищенности КС3 при совместном использовании с сертифицированным АПМДЗ и специализированным ПО ViPNet SysLocker (входящим в комплект поставки) для создания и контроля замкнутой программной среды.

Архитектура ViPNet Administrator 4

Возможность соединений между защищенными узлами определяется связями, которые задает администратор сети ViPNet.

Для управления сетью ViPNet используется программное обеспечение ViPNet Administrator.

ViPNet Administrator 4 — программный комплекс, предназначенный для настройки и управления защищенной сетью, включающий в себя:

- ViPNet NCC (Центр управления сетью, ЦУС) — приложение для конфигурирования и управления виртуальной защищенной сетью ViPNet.
- ViPNet KCA (Удостоверяющий и ключевой центр, УКЦ) — приложение, которое выполняет функции центра формирования ключей шифрования и персональных ключей пользователей.
- Функции Удостоверяющего центра — издание сертификатов для аутентификации, электронной подписи, шифрования и других криптографических операций.

Программа ViPNet Центр управления сетью предназначена для формирования структуры сети ViPNet, задания основных параметров сетевых узлов и пользователей, централизованной отправки обновлений ключей, справочников и программного обеспечения на сетевые узлы ViPNet.

В отличие от программы ЦУС версии 3.2.x, программа ЦУС версии 4 состоит из двух взаимосвязанных программных компонентов:

- Серверное приложение, с помощью которого осуществляется работа с базой данных, содержащей полную информацию о структуре и объектах сети ViPNet. Серверное приложение и база данных могут быть установлены как на одном компьютере (на рабочем месте администратора или на специально выделенном сервере), так и на разных.
- Клиентское приложение, которое представляет собой удобный графический интерфейс для управления структурой сети ViPNet и свойствами сетевых объектов. Оно может быть установлено на одном компьютере с серверным приложением, на удаленном компьютере или на нескольких компьютерах, если управление сетью ViPNet осуществляется с нескольких рабочих мест.

Возможно удаленное подключение клиентского приложения к серверному приложению, а также одновременное подключение нескольких клиентских приложений к серверному.

Программа ViPNet Удостоверяющий и ключевой центр предназначена для управления ключевой структурой сети ViPNet, а также для издания и обслуживания сертификатов ключей проверки электронной подписи. В

соответствии с основными функциями УКЦ условно можно разделить на два компонента: ключевой центр и удостоверяющий центр.

В версии ViPNet Administrator 4 взаимодействие ЦУС и УКЦ осуществляется посредством базы данных SQL. Программы независимо друг от друга обращаются к SQL-базе, в которой хранится вся необходимая информация. Изменения, выполненные в одной программе, незамедлительно отображаются в другой. Механизм взаимодействия всех компонентов ViPNet Administrator с базой данных SQL повышает надежность работы программы и ее устойчивость к различным сбоям.

Рисунок 1 – Схема взаимодействия компонентов ViPNet Administrator 4

ViPNet Administrator 4 входит в реестр Российского ПО (https://reestr.minsvyaz.ru/reestr/77544/**).**

Преимущества ViPNet Administrator 4:

- клиент-серверная архитектура, позволяющая нескольким администраторам удалённо управлять защищённой сетью через удобный графический интерфейс;
- поддержка распределённой установки компонентов программного комплекса позволяет гибко масштабировать систему и обеспечить требуемую производительность;
- эффективное управление защищённой сетью с использованием групп узлов и шаблонов политик;
- настраиваемый автоматический режим работы Ключевого центра позволяет автоматизировать работу с приложением;
- надёжный аудит событий системы и действий администраторов.

Рекомендации по планированию защищенной сети

При планировании сети ViPNet следует исходить из задач, которые требуется решить с помощью программного комплекса ViPNet, учитывая существующую физическую структуру сети организации и применяемую политику информационной безопасности.

Если компания, в которой планируется внедрить программный комплекс ViPNet, имеет несколько филиалов регионального уровня, в этих филиалах можно развернуть собственные сети ViPNet и установить между ними межсетевое взаимодействие. В этом случае целесообразно создать иерархическую структуру сетей ViPNet, чтобы централизованно управлять распределением лицензий в подчиненных сетях из главного Центра управления сетью (ЦУС).

Логическая структура создаваемой сети ViPNet (в первую очередь, это привязка клиентов к координаторам) в большинстве случаев определяется существующей физической структурой сети. Программный комплекс ViPNet позволяет создавать структуры, объединяющие в единую защищенную виртуальную сеть произвольное количество локальных подсетей, удаленных и мобильных пользователей.

Важным вопросом является выработка правил именования защищенных узлов. Это позволит увеличить эффективность управления большой сетью.

	**Примечание.** В целях обеспечения большей продуктивности во время выполнения практических заданий необходимо учитывать мощность персонального компьютера, на котором будет развернут виртуальный стенд. Поэтому рекомендуется ориентироваться на системные требования ПО ViPNet **(**см. стр. 180**)** и выбирать наименее требовательную к ресурсам операционную систему. Лучше начинать с одной виртуальной машины и постепенно, по мере необходимости, запускать дополнительные.

Планирование схемы защищенной сети

Представим, что нам поставлена задача внедрить в небольшой, но активно развивающейся организации ViPNet сеть. Поэтому, начиная с первого задания, постепенно, по мере необходимости, будут подключаться новые сетевые узлы.

Но для начала необходимо спланировать схему защищенной сети (*то есть выбрать из локальных сетей те сетевые узлы, на которые по политике безопасности организации необходимо установить средства криптографической защиты информации и межсетевые экраны*), в состав которой будут входить следующие сетевые узлы:

Таблица 1 – Перечень координаторов защищенной сети

№	Название СУ	Расположение СУ	Комментарии
1	*Координатор Центр офис*	Центральный офис компании	На узле будет развернуто ПО ViPNet Coordinator. Узел предназначен для организации защищенных каналов с Филиалом компании и другими сетями ViPNet.
2	*Координатор Филиал*	Филиал компании	На узле будет развернуто ПО ViPNet Coordinator. Узел предназначен для организации защищенного канала с Центральным офисом компании.

Таблица 2 – Перечень клиентов защищенной сети

№	Название СУ	Расположение СУ	Комментарии
1	*Главный администратор*	Центральный офис компании	На узле будут развернуты SQL-сервер, ПО ViPNet Administrator (серверное и клиентское приложения ЦУС, УКЦ), ViPNet Policy Manager. Узел будет выступать в качестве основного рабочего места главного администратора сети ViPNet.
2	*Помощник глав админа*		На узле будет развернуто клиентское приложение ЦУС. Узел будет выступать в качестве рабочего места помощника главного администратора сети ViPNet.
3	*Сотрудник_1 Центр офис*		На узле будет развернуто ПО ViPNet Client. Узел выступает в качестве рабочего места специалиста центрального офиса.
4	*Сотрудник_2 Филиал*	Филиал компании	На узле будет развернуто ПО ViPNet Client специалиста филиала.

Как видно из таблиц 1 и 2, в сети центрального офиса компании потребуется создать три сетевых узла *Координатор Центр офис, Главный администратор, Помощник глав админа и Сотрудник_1 Центр офис,* а в сети филиала сетевые узлы *Координатор Филиал и Сотрудник_2 Филиал.*

Схема организации сети в этом случае примет следующий вид (*Рисунок 2*).

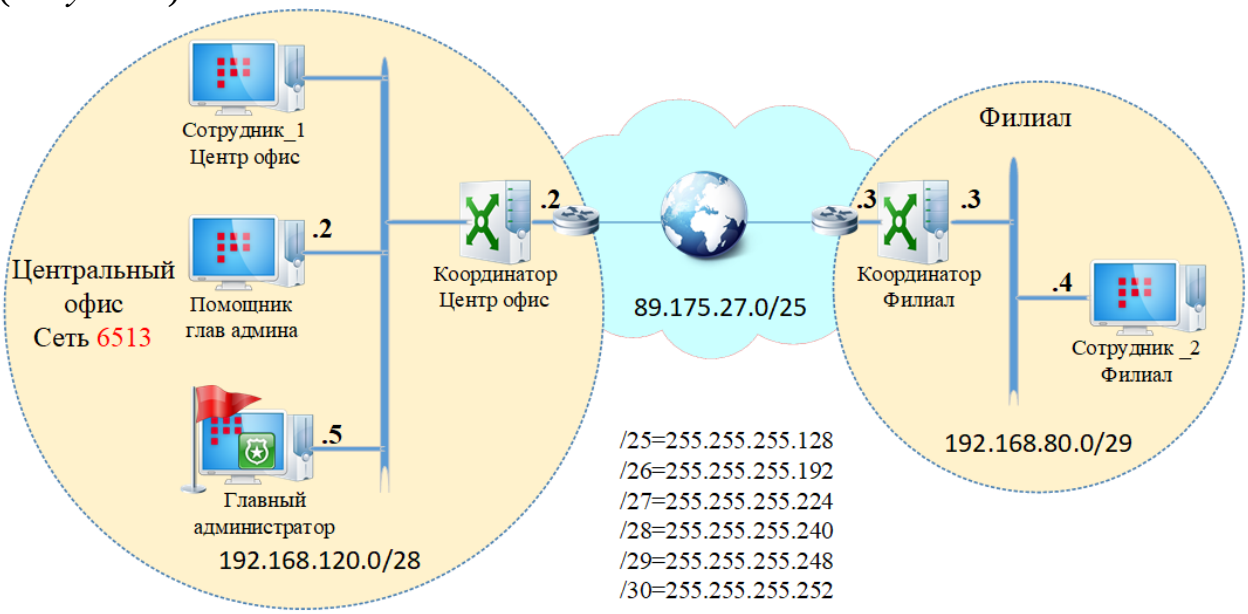

Рисунок 2 – Схема развертывания ViPNet в локальной сети компании

	Примечание. Количество узлов в схеме, как защищенных, так и не защищенных может быть любое, в зависимости от реальной структуры сети организации. Для выполнения практических заданий выбрана оптимальная схема, с целью лучшего восприятия. Однако для выработки навыков по формированию сети ViPNet можно создавать дополнительные сетевые узлы и вносить изменения в структуру (по желанию). Но стоит не забывать, что на имеющемся стенде все узлы будет невозможно развернуть и рекомендуется запускать только то количество узлов (виртуальных машин), которое требуется для выполнения конкретного практического задания!

Подготовка виртуального стенда

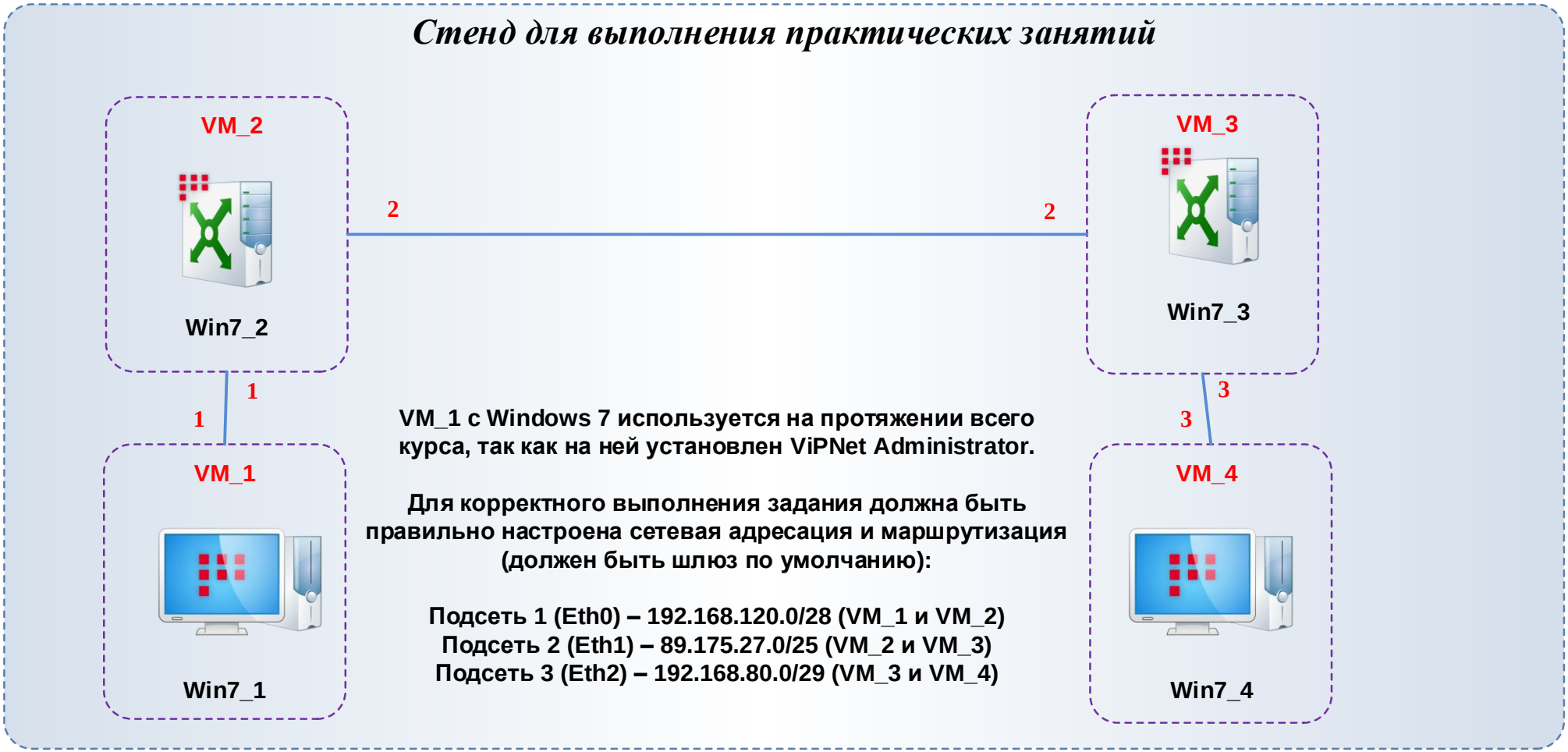

Рисунок 3 – Схема стенда для выполнения практических занятий

В данном разделе приведенная на рисунке 3 схема универсальна и используется на протяжении практически всех занятий. Поэтому от того насколько корректно будет настроена сетевая связность между виртуальными машинами будет зависеть скорость и качество выполнения заданий, а соответственно и освоение функционала ПО ViPNet.

Однако стоит учитывать, что сразу запускать все виртуальные машины нет необходимости и в каждом из занятий будет отдельно указано сколько виртуальных машин нужно на текущий момент.

Поэтому в процессе подготовки к каждому из занятий необходимо проверить корректность настроек виртуальных машин в соответствии с приводимыми в каждом из занятий схем. И в случае несоответствия произвести их настройку.

	**Примечание.** Номера сетевых интерфейсов на схеме, предназначены для упрощения настройки и указывают на то, что интерфейсы на разных VM, но с одинаковым номер входят в одну подсеть. Также на данные номера сетевых адаптеров рекомендуется обращать внимание и брать за основу, в процессе настройки самой виртуальной среды. Например, в VirtualBox для разнесения VM в разные подсети можно использовать тип подключения *Виртуальный адаптер хоста,* в случае выбора данного типа подключения необходимо предварительно создать нужное количество виртуальных адаптеров, после чего в настройках самой VM включить нужное количество *Адаптеров* и произвести их настройку. Проверить наличие *Виртуальных адаптеров хоста* можно в разделе меню Virtual Box *Файл→Настройки…→Сеть→Виртуальные сети хоста*

Практическое занятие № 1. Развертывание защищенной сети ViPNet

Содержание практического занятия

1.1. Установка программного комплекса ViPNet Administrator 4
1.2. Создание структуры защищенной сети.
1.3. Настройка резервного копирования данных и восстановление данных в ПО ViPNet Administrator.
1.4. Развертывание рабочего места помощника главного администратора.
1.5. Дополнительное задание.

Для выполнения первого практического задания нам понадобятся две виртуальные машины VM_1 и VM_2 (Рисунок 4). На каждой из виртуальных машин должно быть поднято по 1-ому сетевому адаптеру, оба адаптера должны находиться в одной подсети.

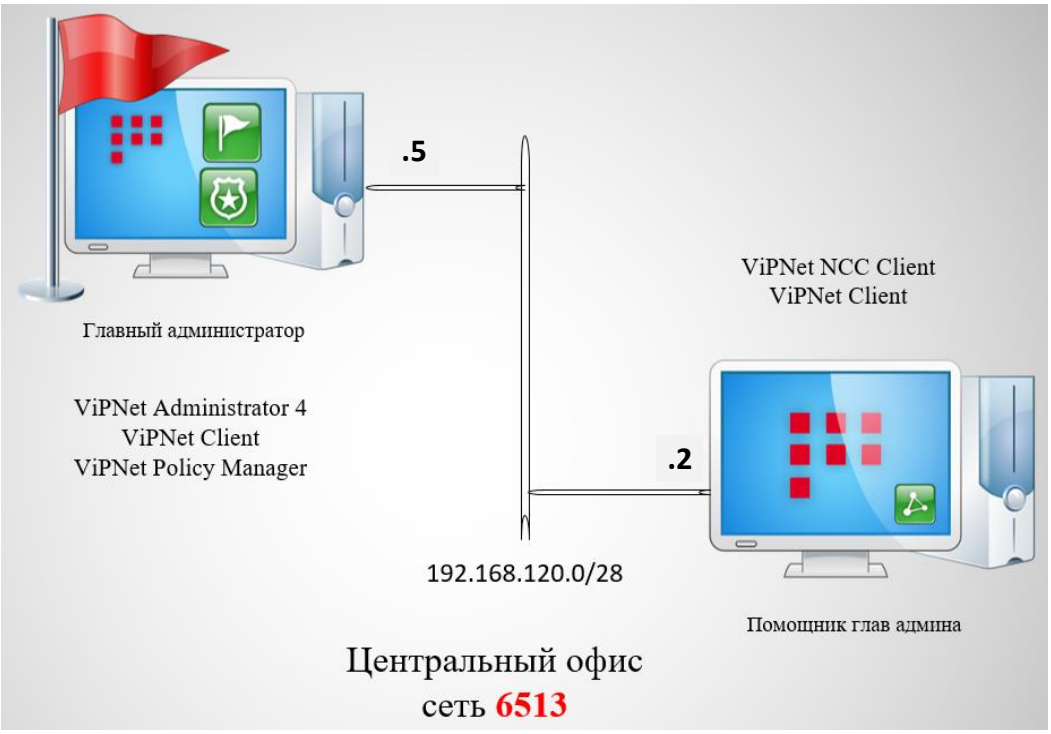

Рисунок 4 – Схема стенда для Практического занятия №1

Задание № 1.1. Установка ПК ViPNet Administrator 4

Формулировка задания

Установить все компоненты ViPNet Administrator 4 на одно рабочее место VM_1.

	Примечание. Перед установкой компонентов ViPNet необходимо убедиться в соответствии узла (персонального компьютера/сервера/виртуальной машины) системным требованиям. В случае, если узел, на котором запланирована установка компонентов ViPNet, не соответствует системным требованиям, его необходимо переконфигурировать. В противном случае корректная работа и правильность выполнения практических заданий не гарантирована. С системными требованиями для каждого из компонентов можно ознакомиться в разделе Справочная информации **(**см. стр. 180**)** или в технической документации (портал документации ViPNet – ***http://docs.infotecs.ru***)

1.1.1. Установка серверного приложения ViPNet Центр управления сетью

Для установки серверного приложения *ViPNet Центр управления сетью* откройте файл *Setup.exe* из каталога серверного приложения *ViPNet Administrator*.

В окне *Установка ViPNet Administrator Центр управления сетью* будет предложено установить дополнительное программное обеспечение. Список необходимого дополнительного программного обеспечения зависит от ранее установленных на компьютер программ. Чтобы начать установку, нажмите кнопку *Продолжить (Рисунок 5)*.

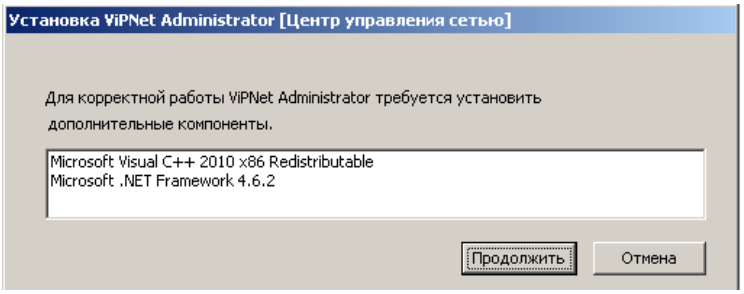

Рисунок 5 - Установка дополнительного программного обеспечения

В появившемся окне выберите язык для программы *ViPNet Центр управления сетью* и нажмите *Продолжить (Рисунок 6)*.

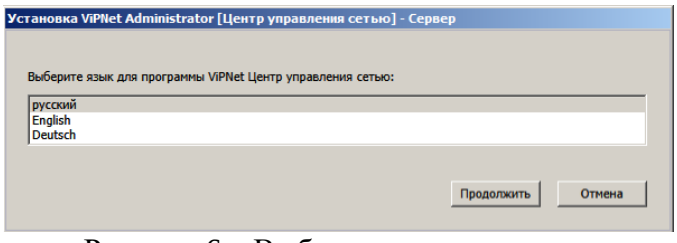

Рисунок 6 – Выбор языка программы

На странице *Лицензионное соглашение* ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку *Продолжить*.

На странице *Установка продукта* задайте параметры подключения к базе данных. Если вы не укажете имя существующего SQL-сервера, то на компьютере будет установлен SQL-сервер из комплекта поставки и создан именованный экземпляр с именем *WINNCCSQL*. При необходимости вы можете задать другое имя экземпляра. В рамках выполнения практического задания изменять параметры подключения не требуется. Нажмите кнопку *Продолжить (Рисунок 7)* и, в следующем окне, *Установить сейчас*.

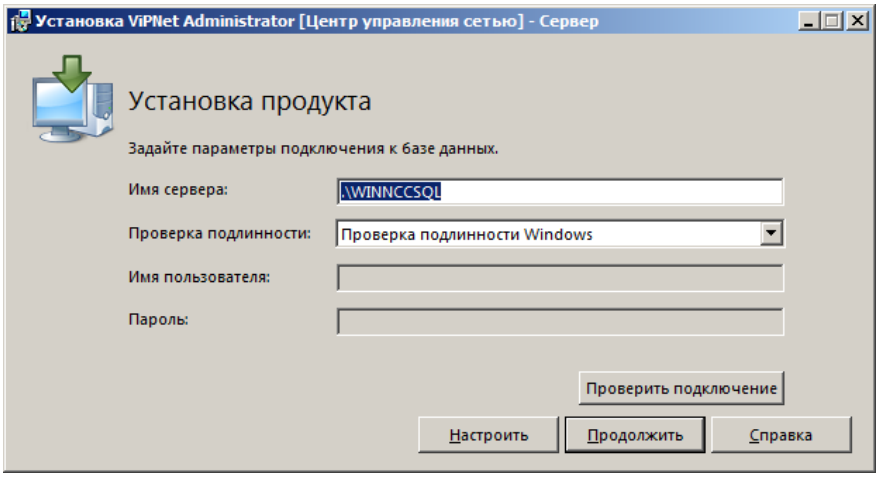

Рисунок 7 – Параметры подключения к базе данных

В появившемся окне о создании сервера базы данных нажмите кнопку *Да (Рисунок 8)*.

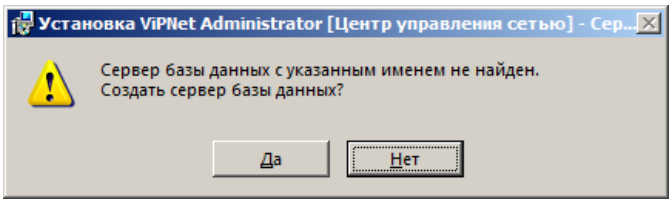

Рисунок 8 – Создание сервера базы данных

При этом на SQL-сервере будут созданы:

- База данных с именем *ViPNetAdministrator*.
- База данных с именем *ViPNetJournals*, в которой хранятся журналы аудита программы *ViPNet Центр управления сетью*.
- Учетная запись пользователя с правами администратора базы данных для пользователя, от имени которого был запущен файл установки серверного приложения ЦУСа.
- Две учетные записи пользователей *KcaUser* и *NccUser*, под которыми осуществляется подключение УКЦ и серверного приложения ЦУСа к базе данных соответственно.

После создания сервера базы данных требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку. Если после перезагрузки установка серверного приложения не продолжилась автоматически, необходимо самостоятельно запустить *Setup.exe* из каталога серверного приложения *ViPNet Administrator (это необходимо для завершения установки серверного приложения, так как до перезагрузки были установлены только дополнительные компоненты и SQL-сервер).*

В появившемся окне выберите язык для программы *ViPNet Центр управления сетью* и нажмите *Продолжить*.

На странице *Установка продукта* нажмите кнопку *Продолжить*.

В появившемся окне проверьте выбранные параметры установки. Чтобы начать установку, нажмите кнопку *Установить сейчас*.

По завершении установки нажмите кнопку *Закрыть*.

В результате серверное приложение ЦУСа будет установлено на компьютер. Далее можно приступить к установке клиентского приложения ЦУСа.

1.1.2. Установка клиентского приложения ViPNet Центр управления сетью

В рамках настоящего практического задания клиентское приложение ViPNet Центр управления сетью устанавливается на то же рабочее место, что и серверное приложение.

1. Для установки клиентского приложения *ViPNet Центр управления сетью* откройте файл *Setup.exe* из каталога клиентского приложения ViPNet Administrator.
2. В появившемся окне выберите язык для клиентского приложения ViPNet Центр управления сетью и нажмите *Продолжить (Рисунок 9)*.

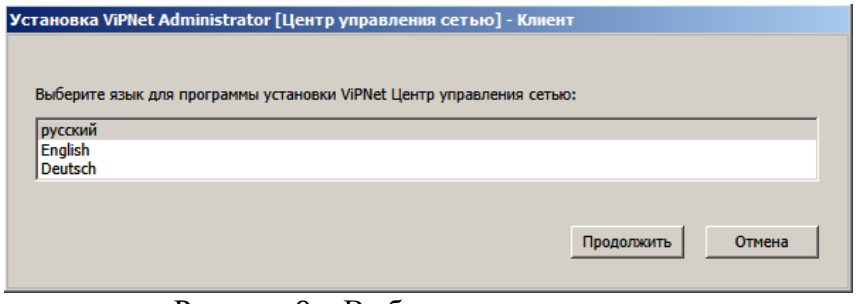

Рисунок 9 – Выбор языка программы

3. На странице *Лицензионное соглашение* ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку *Продолжить*.
4. На странице *Способ установки* нажмите кнопку *Установить сейчас* (Рисунок 10).

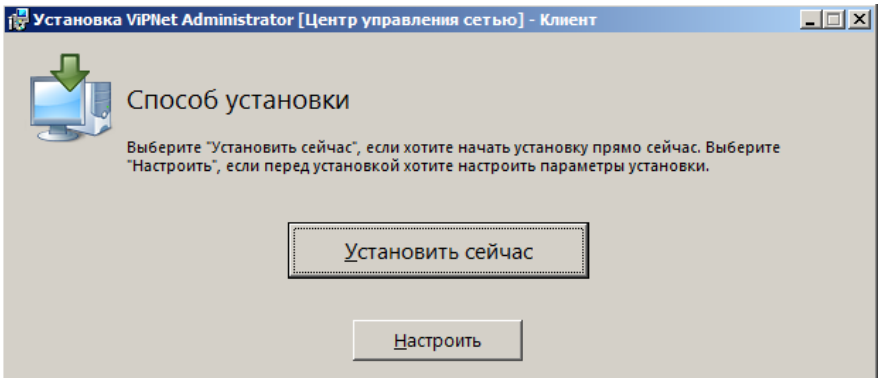

Рисунок 10 – Способ установки

Если требуется настроить параметры установки, то нажмите кнопку *Настроить* на странице *Способ установки* и укажите:

- путь к папке установки программы на компьютере;
- имя пользователя и название организации;
- название папки программы и ее расположение в меню *Пуск*.

5. По завершении установки нажмите кнопку *Закрыть*.

В результате клиентское приложение ЦУСа будет установлено на компьютер. Далее можно приступить к установке *ViPNet Удостоверяющий и ключевой центр*.

1.1.3. Установка ViPNet Удостоверяющий и ключевой центр

В рамках настоящего практического задания *ViPNet Удостоверяющий и ключевой центр* устанавливается на то же рабочее место, что и серверное приложение.

1. Для установки компонента *ViPNet Удостоверяющий и ключевой центр* откройте файл *Setup.exe* из каталога удостоверяющего и ключевого центра ViPNet Administrator.
2. Подождите, пока на компьютер будет автоматически установлено необходимое программное обеспечение, в том числе программа ViPNet CSP.
3. В окне *Установка ViPNet Administrator [Удостоверяющий и ключевой центр]* на странице *Лицензионное соглашение* ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку *Продолжить*.

4. На странице Способ установки нажмите кнопку Установить сейчас.
5. Если потребуется настроить параметры установки, то нажмите кнопку *Настроить* (Рисунок 11) на странице *Способ установки* и укажите:
   - путь к папке установки программы на компьютере;
   - имя пользователя и название организации;
   - название папки программы и ее расположение в меню *Пуск*.

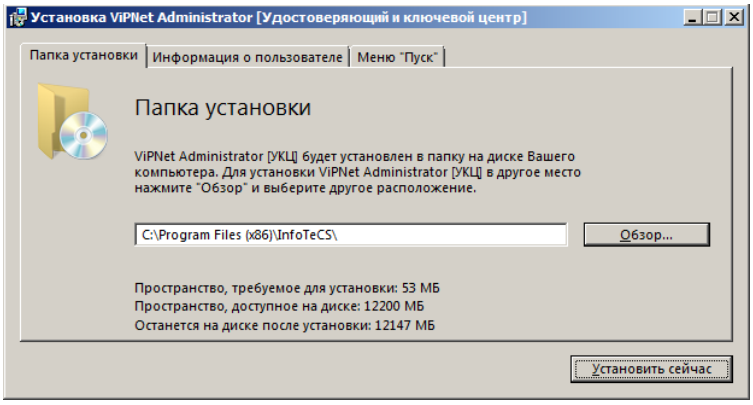

Рисунок 11 – Настройка установки

6. По окончании установки нажмите кнопку *Закрыть*.

После установки УКЦ потребуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку.

Теперь можно начинать работу с ПО ViPNet Administrator 4.