МИНОБРНАУКИ РОССИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ “ТВЕРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ”**

**(ФГБОУ ВО «ТГУ»)**

Математический факультет

Кафедра Компьютерной безопасности и математических методов управления

**ОТЧЕТ**

# по \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ практике

студента \_\_ курса \_\_ группы

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Специальность 10.05.01 Компьютерная безопасность

Специализация «Математические методы защиты информации»

Зав. кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_. \_\_.20\_\_

Обучающийся \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_. \_\_.20\_\_

Руководитель ООП

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.\_\_.20\_\_

Руководитель практики от предприятия

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_.\_\_.20\_\_

Тверь 20\_\_

# Содержание

1. Введение --- 3
2. Постановка задачи и ее выполнение: --- 4
   1. Настройка серверного оборудования --- 4
   2. Установка сети ViPNet: --- 4
      * 1. Установка и настройка ViPNet Administrator 4.3 --- 4

Установка компонентов ViPNet Administrator на одном компьютере. --- 5

Размещение клиентского приложения ViPNet Центр управления сетью. --- 5

Порядок установки компонентов ПО ViPNet Administrator --- 6

Установка программы ViPNet Удостоверяющий и ключевой центр. --- 8

* + - 1. Установка и настройка ViPNet Registration point --- 9

Состав ViPNet Registration point --- 10

Основные возможности ViPNet Registration point 12

Порядок действии при типовом варианте развертывания ViPNet Registration point. ---16

* + - 1. Установка и настройка ViPNet Client --- 18

Состав ПО ViPNet Client. --- 18

ViPNet драйвер --- 18

ViPNet Монитор --- 19

ViPNet MFTP --- 20

ViPNet Контроль приложений --- 20

ViPNet Деловая почта --- 20

Криптопровайдер ViPNet CSP --- 21

Система обновлений ViPNet --- 21

* + - 1. Развертывание TSP-OCSP сервера --- 22

Порядок развертывания --- 23

Получение сертификатов для работы ViPNet TSP/OCSP сервера. --- 24

1. Заключение --- 25
2. Приложение --- 26

# Введение

Прохождение производственной практики проходило в Центре Информационных Технологий "Цитадель" основанном в феврале 2008 года. Основными видами деятельности организации являются консультирование по аппаратным средствам вычислительной техники и разработка программного обеспечения.

Являясь лицензиатом [ФСБ](http://www.fsb.ru/) и [ФСТЭК](http://www.fstec.ru/), в тесном сотрудничестве с [ФГУП "ЦентрИнформ"](http://www.center-inform.ru/) организация осуществляет выпуск сертификатов квалифицированной электронной подписи для [ЕГАИС](http://egais.ru/) и сдачи отчетности в [Росалкогольрегулирование](http://www.fsrar.ru/), а так же для участия в электронных торгах.

Практика проходила с \_\_ июня по \_\_ июля 2017 год

# Поставленная задача в начале практики состояла, в том, чтобы с нуля установить сеть ViPNet, осуществляющую создание и выпуск электронных ключей и сертификатов и выпустить электронный сертификат, заверенный Удостоверяющим Центром, на мое имя.

Для этого в первую очередь нужно было установить оборудование в серверную.

# Оборудованием был сервер компании HP(Hewlett-Packard) модели ProLiant ML110 G7 седьмой формаций.

Далее нужно было установить программное обеспечение(ПО) на данный сервер, а именно Windows Server 2008 R2.

После установки программного обеспечения, нужно было

зарезервировать IP-адрес под сервер ViPNet.

Далее приступим к установке самой сети ViPNet. И начнем с ViPNet Administrator 4.3, включающего в себя ViPNet Центр управления сетью (ЦУС)

и ViPNet Удостоверяющий и ключевой центр (УКЦ).

**Установка ViPNet Administrator**

Перед установкой ПО ViPNet Administrator нужно выбрать компьютеры, на которых будут размещены следующие компоненты:

- База данных ViPNet Administrator.

- Серверное приложение ViPNet Центр управления сетью.

- Программа ViPNet Удостоверяющий и ключевой центр.

- Одно или несколько клиентских приложений ViPNet Центр управления сетью.

Указанные компоненты можно установить на один или несколько компьютеров сети в любой комбинации. Принципиальное различие между вариантами размещения заключается во взаимном расположении компонентов и базы данных ViPNet Administrator. Поэтому можно выделить две базовые схемы размещения компонентов ПО ViPNet Administrator:

**1** Установка компонентов ViPNet Administrator на одном компьютере.

**2** Установка компонентов ViPNet Administrator на разных компьютерах.

Мы будем использовать схему установки компонентов ViPNet Administrator на один компьютер.

**Установка компонентов ViPNet Administrator на одном компьютере**

Эта схема является наиболее простой и подходит для небольших сетей с одним администратором, работающим и с ЦУСом, и с УКЦ. Она предполагает размещение ЦУСа, УКЦ и SQL-сервера с базой данных ViPNet Administrator на одном компьютере, поэтому исключаются дополнительные трудности c развертыванием SQL-сервера.



Рисунок 1. Установка серверного приложения ЦУСа и УКЦ на одном компьютере.

**Размещение клиентского приложения ViPNet Центр управления сетью**

Клиентское приложение ЦУСа может быть установлено на любом компьютере сети ViPNet. Существуют следующие возможности установки приложений:

- Серверное и клиентское приложения ЦУСа могут быть установлены как на один, так и на разные компьютеры.

- Клиентское приложение ЦУСа может быть установлено как на один, так и на несколько компьютеров.

Установка серверного и клиентского приложений ЦУСа на разные компьютеры дает возможность использовать отдельный мощный компьютер для размещения серверного приложения. Установка клиентских приложений на несколько компьютеров дает возможность администрирования в многопользовательском режиме. Вы можете выбрать расположение клиентского приложения ЦУСа, учитывая потребности вашей организации и необходимое количество администраторов.



Рисунок 2. Варианты установки приложений ЦУСа.

**Порядок установки компонентов ПО ViPNet Administrator**

Для успешного развертывания ПО ViPNet Administrator требуется выполнить все действия из приведенного ниже списка.

**Таблица 1. Порядок установки компонентов ПО ViPNet Administrator**

|  |  |
| --- | --- |
| **Действие** |  |
| Продумайте схему размещения компонентов ПО ViPNet Administrator. | Схемы размещения компонентов ПО ViPNet Administrator |
| Определите количество компьютеров, на которых будет установлено клиентское приложение ЦУСа. | Размещение клиентского приложения ViPNet Центр управления сетью |
| Подготовьте нужное количество  компьютеров и организуйте их  подключение к физической сети. | |
| Убедитесь, что располагаете файлом лицензии на сеть ViPNet \*.itcslic или infotecs.reg. | Лицензия на сеть ViPNet |
| Разверните SQL-сервер на выделенном компьютере, если требуется, чтобы база данных размещалась отдельно от компонентов ViPNet Administrator. |  |
| Выполните установку серверного приложения ЦУСа с учетом выбранного варианта установки приложений ЦУСа.  Если база данных ViPNet Administrator размещена на отдельном компьютере, в процессе установки серверного приложения подключитесь к ней. | Установка серверного приложения ViPNet Центр управления сетью |
| Выполните установку клиентского приложения ЦУСа с учетом выбранного варианта установки приложений ЦУСа. | Установка клиентского приложения ViPNet Центр управления сетью |
| Установите обновления безопасности для используемого ПО сторонних производителей | Установка обновлений для стороннего ПО |
| Выполните установку УКЦ с учетом выбранной схемы размещения компонентов ПО ViPNet Administrator. | Установка программы ViPNet Удостоверяющий и ключевой центр |
| Установите ПО ViPNet Client версии 4.2 и выше на компьютеры с серверным и клиентским приложениями ЦУСа, а также на компьютер с УКЦ. |  |
| Выполните первый запуск клиентского приложения ЦУСа и создайте структуру сети ViPNet. | Первый запуск программы ViPNet Центр управления сетью |
| Выполните первый запуск и первичную инициализацию УКЦ. | Первый запуск программы ViPNet Удостоверяющий и ключевой центр  Первичная инициализация программы ViPNet Удостоверяющий и ключевой центр |

**Установка программы ViPNet Удостоверяющий и ключевой центр**

После установки серверного и клиентского приложений ЦУСа можно приступать к установке УКЦ.

Прежде чем начать установку программы:

- Убедиться, что на компьютере выполнены стандартные региональные настройки, а также правильно заданы часовой пояс, дата и время (см. «Региональные настройки» на стр. 72). Иначе возможны проблемы с отображением символов.

- Убедиться, что располагаете установочным файлом программы ViPNet Удостоверяющий и ключевой центр.

Далее, после установки и настройки Центра управлению сетью и Удостоверяющего и ключевого центра на сам сервер нужно установить VipNet Registration point на локальный компьютер администратора для регистрации и обслуживания внешних пользователей и пользователей сети ViPNet и хранения их регистрационных данных.

**Установка и настройка ViPNet Registration point**

VipNet Registration point - Программное обеспечение, предназначенное для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов подписи и дистрибутивов ключей, создаваемых в программе ViPNet Удостоверяющий и ключевой центр по соответствующим запросам.

Внешний пользователь - Лицо, которое не является пользователем сетевого узла ViPNet и для которого в программе ViPNet Удостоверяющий и ключевой центр издан сертификат ключа проверки электронной подписи.

Пользователь ViPNet - Лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

В части инфраструктуры PKI программа ViPNet Registration Point является связующим звеном между внешними пользователями и удостоверяющим центром (далее — программой ViPNet Удостоверяющий и ключевой центр, УКЦ) и обеспечивает взаимодействие между ними — формирует и обрабатывает запросы на выпуск сертификатов пользователей, аннулирование, приостановление и возобновление их действия.



Рисунок 3. Взаимодействие ViPNet Registration Point в части инфраструктуры PKI

С точки зрения VPN-технологии, ViPNet Registration Point выполняет функции обслуживания пользователей как клиентов защищенной сети ViPNet — формирует запросы на создание дистрибутивов ключей, производит выдачу готовых дистрибутивов ключей.



Рисунок 4. Взаимодействие ViPNet Registration Point при обслуживании клиентов сети ViPNet.

**Состав ViPNet Registration Point**

Программное обеспечение ViPNet Registration Point включает в себя:

- Исполняемый модуль программы ViPNet Registration Point.

- Транспортный модуль ViPNet MFTP.

- Криптопровайдер ViPNet CSP.

- Систему обновления ViPNet

-ViPNet MFTP

Транспортный модуль (MFTP) обеспечивает информационное взаимодействие между узлом с программой ViPNet Registration Point и узлом администратора сети с развернутым ПО ViPNet Administrator. Посредством ViPNet MFTP осуществляется обмен управляющими конвертами с запросами на сертификаты и дистрибутивы ключей, изданными сертификатами, созданными дистрибутивами ключей и другими данными между указанными узлами.

Подробную информацию о транспортном модуле, его настройке и использовании см. в документе «ViPNet MFTP. Руководство администратора».

Информацию о том, как можно запустить транспортный модуль и настроить параметры его работы, см. в разделе Работа транспортного модуля ViPNet MFTP .

-ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций через интерфейс Microsoft CryptoAPI 2.0. Она позволяет использовать криптографические функции, реализованные в соответствии с российскими стандартами, в различных приложениях, например Microsoft Office.

С помощью криптопровайдера ViPNet CSP вы можете выполнять следующие операции:

- Формирование и проверка электронной подписи.

- Шифрование данных, в том числе сообщений электронной почты.

- Аутентификация и защита соединений по протоколу TLS/SSL.

-Система обновления ViPNet

Система обновления ViPNet обеспечивает получение и установку в ViPNet Registration Point обновлений ПО, справочников и ключей, отправляемых администратором сети из программы ViPNet Registration Point 4.6.

**Основные возможности программы ViPNet Registration Point**

Основные возможности программы ViPNet Registration Point представлены в таблице ниже. Для удобства они распределены на три категории: общая функциональность, функциональность в части технологии PKI и функциональность с точки зрения технологии VPN.

Таблица 2. Основные возможности программы ViPNet Registration Point.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Категория** | **Функциональная возможность** | | | | **Ссылка** | |
| Общие | **Регистрация пользователей ViPNet**. Программа позволяет регистрировать пользователей ViPNet | | | | Регистрация пользователей | |
| **Возможность импорта данных из LDAP Active Directory**. Регистрацию пользователей можно производить на основе данных из домена Active Directory | | | Регистрация через Active Directory | | | |
| **Удаление учетных записей пользователей**. Программа позволяет удалять учетные записи зарегистрированных пользователей: внешних пользователей — из базы данных ViPNet Registration Point, пользователей сети ViPNet — из программы ViPNet Центр управления сетью по соответствующему запросу | | | Удаление учетных записей пользователей | | | |
| **Ведение журнала событий**. Регистрация событий и учет действий администратора программы ViPNet Registration Point | | | Работа с журналом событий программы ViPNet Registration Point | | | |
| **Использование резервных копий конфигураций программы ViPNet Registration Point**. Возможность создания резервных копий конфигураций программы и восстановления конфигураций из резервных копий | | | Работа с резервными копиями конфигураций программы | | | |
| В части технологии PKI | **Создание запросов на выдачу сертификатов ключа проверки электронной подписи**. Для зарегистрированных пользователей ViPNet можно формировать запросы на получение сертификата ключа проверки электронной подписи | | | | Создание запроса на новый сертификат | |
| **Добавление сертификата пользователя в контейнер ключей**. При получении сертификата возможно его добавление в контейнер ключей | | | Добавление сертификата в контейнер ключей | | | |
| **Создание запросов на аннулирование сертификатов пользователей, приостановление и возобновление их действия. От имени администратора ViPNet Registration Point можно формировать запросы на аннулирование, приостановление и возобновление действия изданных сертификатов пользователей** | | | -Аннулирование сертификата  -Приостановление действия сертификата  -Возобновление действия сертификата | | | |
| **Обработка запросов на сертификаты от внешних пользователей. Прием запросов на получение или обновление сертификатов от внешних пользователей в формате PKCS#10 или CMC и выдача готовых сертификатов по данным запросам** | | | Обработка запросов на сертификаты от внешних пользователей | | | |
| **Экспорт сертификатов пользователей. Возможен экспорт полученных сертификатов пользователей в различные форматы** | | | Экспорт сертификата | | | |
| **Просмотр контейнеров ключей. Возможен просмотр параметров контейнеров ключей, созданных в программе или пользователями** | | | Просмотр свойств контейнера ключей | | | |
| В части технологии VPN | | **Создание запросов на дистрибутивы ключей или их обновления.** Для зарегистрированных пользователей ViPNet можно формировать запросы на получение или обновление дистрибутивов ключей ViPNet | | | | Создание запроса на дистрибутив ключей (на стр. 139)  Создание запроса на обновление дистрибутива ключей |
| **Обработка дистрибутивов ключей**. Перенос или распаковка созданных дистрибутивов ключей для передачи пользователям | | | | -Перенос дистрибутива в папку  -Распаковка дистрибутива ключей | | |

**Порядок действий при типовом варианте развертывания программы ViPNet Registration Point**

При развертывании на сетевом узле программы ViPNet Registration Point вместе с программой ViPNet Client выполните все задачи из приведенного ниже списка.

Таблица 3. Последовательность действий при типовом варианте установки ViPNet Registration Point

|  |  |
| --- | --- |
| **Задача** | **Ссылка на раздел или документ для использования** |
| Установите программу ViPNet Registration Point. | Установка программы. |
| Установите программу ViPNet Client. | Документ «ViPNet Client Монитор. Руководство пользователя», раздел «Установка ПО ViPNet Client». |
| Установите справочники и ключи с помощью дистрибутива ключей.  При использовании нескольких программ ViPNet на одном сетевом узле справочники и ключи помещаются в папку установки одной из них. В связи с этим в процессе установки справочников и ключей укажите одну из программ: ViPNet Registration Point или ViPNet Client. В результате справочники и ключи будут помещены только в папку установки выбранной программы. | Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet. |
| При запуске второй программы, для которой не были установлены справочники и ключи, укажите папку ключей узла. В качестве папки ключей узла выберите папку установки программы, в которую были помещены справочники и ключи на предыдущем шаге. | Использование справочников и ключей, установленных ранее. |

Установив и настроив ViPNet Registration Point, переходим к установке ViPNet Client.

**Установка ViPNet Client.**

Программное обеспечение ViPNet Client предназначено для использования в сетях ViPNet, управляемых с помощью ПО ViPNet Administrator и ПО ViPNet Network Manager. ViPNet Client выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях.

Программное обеспечение ViPNet Client может быть установлено для защиты трафика на любом компьютере с ОС Windows, будь то стационарный, удаленный, мобильный компьютер или сервер.

**Состав ПО ViPNet Client**

Программное обеспечение ViPNet Client состоит из следующих компонентов:

- Низкоуровневый драйвер сетевой защиты ViPNet-драйвер.

- Программа ViPNet Монитор.

- Транспортный модуль ViPNet MFTP.

- Программа ViPNet Контроль приложений.

- Программа ViPNet Деловая почта.

- Криптопровайдер ViPNet CSP.

- Система обновления ViPNet.

ViPNet-драйвер

ViPNet-драйвер — это низкоуровневый драйвер сетевой защиты, осуществляющий шифрование и фильтрацию IP-трафика. ViPNet-драйвер взаимодействует непосредственно с драйверами сетевых интерфейсов компьютера (реальных или их эмулируемых), что обеспечивает независимость программы от операционной системы и ее недокументированных возможностей. ViPNet-драйвер перехватывает и контролирует весь входящий и исходящий IP-трафик компьютера.

Одна из важнейших функций драйвера — эффективный контроль IP-трафика во время загрузки операционной системы. В ОС Windows для инициализации загрузки компьютера используется только одна служба. Инициализация ViPNet-драйвера и ключей шифрования ViPNet выполняется перед входом пользователя в Windows, то есть до инициализации остальных служб и драйверов операционной системы. ViPNet Client for Windows 4.3.

В результате ViPNet-драйвер первым получает контроль над стеком протоколов TCP/IP. К моменту инициализации драйверов сетевых интерфейсов ViPNet-драйвер подготовлен к шифрованию и фильтрации трафика, тем самым обеспечивается защищенное соединение с контроллером домена, контроль сетевой активности запущенных на компьютере приложений и блокирование нежелательных пакетов извне. В момент загрузки операционной системы ПО ViPNet проверяет собственные контрольные суммы, гарантирующие целостность программного обеспечения, наборов ключей и списка приложений, которым разрешена сетевая активность.

ViPNet Монитор

Основной функцией программы ViPNet Монитор является настройка различных параметров ViPNet-драйвера и запись событий, возникающих в процессе обработки трафика драйвером, в журнал регистрации IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 196). Если выгрузить программу ViPNet Монитор из памяти компьютера, ViPNet-драйвер продолжит работу и будет обеспечивать безопасность компьютера, но в журнале регистрации IP-пакетов может отсутствовать информация о трафике, обработанном драйвером при закрытой программе ViPNet Монитор (ViPNet-драйвер может хранить в памяти не более 10000 записей журнала).

На компьютере программа ViPNet Монитор:

- Позволяет настраивать параметры встроенного сетевого.

- Позволяет управлять параметрами обработки прикладных протоколов.

- Предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена и так далее.

ViPNet MFTP

На клиентском узле транспортный модуль ViPNet MFTP обеспечивает обмен управляющими конвертами, конвертами программы ViPNet Деловая почта и файлами с другими сетевыми узлами ViPNet. Подробнее о программе см. документ «ViPNet MFTP. Руководство администратора».

ViPNet Контроль приложений

Программа «Контроль приложений» является необязательным модулем программного обеспечения ViPNet Client. Чтобы иметь возможность контролировать сетевую активность приложений на каждом компьютере, необходима специальная лицензионная запись в регистрационном файле на ПО ViPNet. ViPNet Client for Windows 4.3.

Программа «Контроль приложений» позволяет:

- Получать информацию обо всех приложениях, которые запрашивали доступ в сеть.

- Ограничивать (разрешить или запретить) доступ приложений к сети.

- Просматривать журнал событий по сетевой активности приложений.

ViPNet Деловая почта

ViPNet Деловая почта — это программа в составе ПО ViPNet Client, предназначенная для обмена электронной почтой между пользователями сети ViPNet. C помощью программы ViPNet Деловая почта можно отправлять и получать сообщения с вложенными файлами, шифровать сообщения и вложения, подписывать сообщения и вложения электронной подписью. В программе предусмотрена система автоматической обработки входящих сообщений и файлов в соответствии с заданными правилами (автопроцессинг).

ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций через интерфейс Microsoft CryptoAPI 2.0. Она позволяет использовать криптографические функции, реализованные в соответствии с российскими стандартами, в различных приложениях, например Microsoft Office.

С помощью криптопровайдера ViPNet CSP вы можете выполнять следующие операции:

- Формирование и проверка электронной подписи.

- Шифрование данных, в том числе сообщений электронной почты.

- Аутентификация и защита соединений по протоколу TLS/SSL.

После установки и настройки ViPNet Client переходим к развертыванию сервера TSP-OCSP Service

Система обновления ViPNet

Система обновления ViPNet обеспечивает получение и установку в ViPNet Client обновлений ПО,

справочников и ключей, отправляемых администратором сети из программы ViPNet Administrator

или ViPNet Network Manager, а также обновлений политик безопасности, отправленных из

программы ViPNet Policy Manager.

# **Развертывание ViPNet TSP/OCSP-сервера**

Для развертывания ViPNet TSP/OCSP-сервера и его корректной работы кроме программы ViPNet TSP-OCSP Service требуется криптопровайдер ViPNet CSP. Криптопровайдер необходим для выполнения различных криптографических операций при обработке сервером TSP/OCSP-запросов (в частности, для подписи формируемых ответов на запросы).

Криптопровайдер ViPNet CSP может быть установлен на сервер отдельно либо в составе программного обеспечения ViPNet Client или ViPNet CryptoService.

Типовым вариантом считается установка криптопровайдера совместно с программным обеспечением ViPNet Client. Такой вариант является рекомендуемым, поскольку кроме того, что на сервере будет установлен криптопровайдер, он с помощью программы ViPNet Client сможет автоматически получать из удостоверяющего центра (программы ViPNet Удостоверяющий и ключевой центр) актуальные сертификаты издателей и списки аннулированных сертификатов, необходимые при его работе как сервиса проверки статуса сертификатов (см. «ViPNet TSP/OCSP-сервер в роли сервиса проверки статуса сертификатов» на стр. 12), и устанавливать их в системное хранилище сертификатов Windows.

Также ViPNet TSP/OCSP-сервер в данном случае будет являться защищенным узлом сети ViPNet, а установленная на нем программа ViPNet Client выступать в качестве межсетевого экрана.



Рисунок 5. Типовая схема развертывания ViPNet TSP/OCSP-сервера

**Порядок развертывания**

Для развертывания ViPNet TSP/OCSP-сервера потребуются:

- Файл установки программного обеспечения ViPNet Client версии не ниже 4.2 — с учетом типового варианта установки криптопровайдера (см. раздел Варианты установки криптопровайдера на ViPNet TSP/OCSP-сервер, файл установки программного обеспечения ViPNet CryptoService версии не ниже 4.2 либо ViPNet CSP сертифицированной версии — при установке криптопровайдера не в составе ViPNet Client.

- Файл установки программы ViPNet TSP-OCSP Service.

- Дистрибутив ключей (файл \*.dst) и пароль пользователя к данному дистрибутиву, если в качестве дополнительного программного обеспечения на сервере будет установлен ViPNet Client либо ViPNet CryptoService.

Файл \*.dst и пароль пользователя нужно получить у администратора сети ViPNet.

Развертывание ViPNet TSP/OCSP-сервера должен выполнять пользователь, обладающий правами администратора в операционной системе Windows. Перед началом развертывания на компьютере рекомендуется произвести стандартные сетевые настройки и убедиться, что правильно заданы часовой пояс, дата и время.

Для успешного развертывания, настройки и корректной работы ViPNet TSP/OCSP-сервера следует выполнить все действия из приведенного ниже списка.

|  |
| --- |
| В зависимости от выбранной схемы установки на сервер криптопровайдера ViPNet CSP:  - Установите программу ViPNet Client либо ViPNet CryptoService, выполните процедуру ее первичной инициализации и сделайте все необходимые дополнительные настройки.  - Установите программу ViPNet CSP. |
| -Установите программу ViPNet TSP-OCSP Service. |
| -Зарегистрируйте программу ViPNet TSP-OCSP Service. |
| -Получите и установите сертификаты, необходимые для работы сервера. |
| -Выполните настройку общих параметров работы ViPNet TSP/OCSP-сервера. |

**Получение сертификатов для работы ViPNet TSP/OCSP-сервера**

Для обработки TSP/OCSP-запросов и подписи формируемых ответов на запросы ViPNet TSP/OCSP-серверу необходимо иметь два сертификата ключа проверки электронной подписи, один из которых будет содержать расширение «Установка штампа времени» (OID 1.3.6.1.5.5.7.3.8), второй — «Подписание OCSP» (OID 1.3.6.1.5.5.7.3.9), и соответственно два ключа электронной подписи. Сертификат с расширением «Установка штампа времени» позволит серверу функционировать в роли службы штампов времени, сертификат с расширением «Подписание OCSP» — функционировать в роли сервиса проверки статуса сертификатов. При отсутствии одного из указанных сертификатов работа сервера будет ограничена, при отсутствии всех сертификатов — невозможна.

# **Заключение**

# В итоге проделанной мной работы по установке и настройке сети ViPNet с помощью мануала разработчика Infotex и дополнительной информации, взятой из сети интернет, я получил 2 электронных сертификата Удостоверяющего Центра Центра Информационных Технологии Цитадель. А именнно:

1. Сертификат выданный и заверенный УЦ ЦИТ Цитадель на имя Султан т. е. на меня. (Действителен с 30.06.2017 13.38 по 30.09.2018 13.38. Версия сертификата: Version 3).
2. Сертификат выданный и заверенный УЦ ЦИТ Цитадель на ЦИТ Цитадель (Действителен с 23.06.2017 11.57 по 23.06.2020 11.57. Версия сертификата: Version 3).