# Установка и настройка SQL Server

**Обязательно** выключаем на всех виртуальных машинах брандмауэр!

1. На Net1-Open устанавливаем БД (SQL SERVER). Называем БД «DB».

2. В установщике ставим тип запуска SQL Server Browser – «Automatic».

3. Выбираем режим аутентификации Mixed, пишем новый пароль и записываем его в блокнотик.

4. Во вкладке FILESTREAM включаем всё.

5. После установки запускаем SQL Server Configuration Manager.

6. Заходим в SQL Server Network Configuration -> Protocols for DB и включаем все протоколы.

7. Перезапускаем сервер.

# Установка ЦУС

1. Устанавливаем ЦУС сервер на Net1-Admin.

2. В параметрах подключения к базе данных меняем «Имя сервера» на айпишник\_машины\_с\_сервером\DB и выбираем «проверка подлинности SQL Server».

3. Ставим логин «sa». Пароль же из установщика SQL Server.

4. Запускаем ЦУС. Сервер оставляем localhost. Логин и пароль: «Administrator».

5. Меняем пароль, записываем его, устанавливаем лицензию.

6. Структуру настраиваем самостоятельно!

# Настройка ЦУС

Галочки с создания одноимённых пользователей убираем!

1. Создаём координаторы.

2. В их свойствах выставляем им роль «Coordinator HW-VA».

3. Создаём межсерверный канал меж ними.

4. Добавляем координаторам адреса во внешних сетях. Жмём «использовать для MFTP».

5. Выключаем межсетевой экран и межсетевой экран клиентов.

6. Создаём клиентов, первый админ!

7. Присваиваем OperCA роль Registration Point

8. Настраиваем адрес во внешней сети. Жмём «использовать для MFTP».

9. Создаём пользователей, настраиваем им связи по таблице.

10. Создаём группы узлов: Центральный офис Net-1 и филиал Net-2

11. В группы узлов добавляем подходящие сетевые узлы.

12. Проверяем конфигурацию сети, создаём справочники для всего списка.

13. Выгружаем структуру сети в html!

14. Сворачиваем ЦУС.

# Настройка УКЦ

1. Выбираем настройку новой базы данных.

2. Подключаемся к айпишнику\_Net1-Open\DB

3. ТИП ПРОВЕРКИ НЕ МЕНЯЕМ, имя пользователей и пароль тоже.

4. Выбираем собственный пароль.

5. В настройках/Сертификаты ставим недостающую галочку.

6. Контейнер ключей администратора копируем в общую папку. Сам контейнер хранится в «%appdata%/InfoTeCS/ViPNet Administrator».

7. Создаём пароли пользователям, записываем к себе в блокнот.

8. Задаём пароли сетевым узлам.

9. Выделяем все сетевые узлы и выдаём дистрибутив ключей.

10. Копируем папку с дистрибутивом ключей в удобное место.

11. Создаём пароли группам узлов.

12. Пингуем машины друг с другом.

13. Выделяем все сетевые узлы и передаём ключи в ЦУС.

14. Ключи записываем на диск/флешку. В случае отсутствия флешки, записываем папку ключей в ISO образ любым удобным методом.

# ПО Клиент

1. Устанавливаем Client на машины, указываем соответствующий машине ключ. Вводим пароли.

2. На Net1-Admin в ЦУСе отправляем справочники и ключи на все узлы.

# Настройки координаторов

1. В настройках виртуальной машины Net1-Coord/Net2-Coord настраиваем сетевые адаптеры так, чтобы первый интерфейс смотрел в Custom Network NAT (NAT, естественно, предварительно настроен по заданию), а второй в свой LAN-сегмент.

2. Устанавливаем в графическом интерфейсе (Full-screen interface)!

3. Настройки времени, часового пояса и даты должны быть полностью корректными, иначе не будет связи.

4. Монтируем ISO-образ, либо флешку с ключами. Выбираем соответствующий координатору ключ и вводим его пароль.

5. Настраиваем адрес во внешней сети.

Шлюз интернета для координаторов можно посмотреть в Virtual Network Editor -> NAT Settings -> Gateway IP.

IP адреса для координаторов должны быть старше IP шлюза!

К примеру:

IP интернет для координаторов: 8.9.10.0

IP шлюза интернета для координаторов: 8.9.10.2

Внешний IP координатора: 8.9.10.3

6. Остальные службы и интерфейсы оставляем выключенными. Даём имя координатору.

7. Отключаем настройку Firewall.

8. Проверяем соединение на машине с установленным ПО Client. Если понадобится, вводим IP-адрес.

9. Включаем ВПН-сервис перед выходом из меню установки.

# Проверка работоспособности сети

В ПО Client все узлы должны быть доступны.

1. Отправляем, по заданию, письмо и проверяем пришло ли оно на вторую машину.

2. Заходим в координатор, пишем:

enable

//Вводим пароль

#iplir view

3. Проверяем порты 5000-5003

4. Сохраняем в ЦУСе структуру сети в html.

# Настройка аккредитованного режима УКЦ

1. Заходим в настройки -> программные средства -> средства удостоверяющего центра.

2. Заполняем наименования и номера в соответствии с заданием.

3. Ключ ЭП и ключ УКЦ мы копировали в общую папку ранее, на шаге 6 настройки УКЦ.

4. Выставить в настройках - > сертификаты все галочки.

5. Создаём администратору корневой сертификат, вводим данные админа. Остальное по умолчанию.

6. Создаём ключи электронных подписей пользователей.

# Настройка PUBLICATION SERVICE

1. Устанавливаем на OperCA: Registration Point, Publication Service

2. Включаем на Net1-Admin в «Программы и компоненты» службу FTP

3. Открываем диспетчер служб IIS -> сайты добавляем тут FTP-сайт. Выбираем общую папку.

4. Разрешаем всем подключаться к ней.

5. С админа для папки ProgramData/Infotecs/ViPNet Administrator/KC/Publication делаем общий доступ.

6. Монтируем папку как сетевой диск на OperCA. ПКМ на мой компьютер, подключить сетевой диск. Путь должен быть в формате [\\1.2.3.2\Publication](file:///\\1.2.3.2\Publication)

7. На OperCA, в сервисе публикации, указываем в настройках папки приёма из примонтированного диска. Приём = Out, Отправка = In.

8. Настраиваем публикации сертификатов. Сертификаты, FTP, пишем адрес FTP-сервера. Создаём в общей папке папку для сертификатов и вписываем её сюда.

9. Делаем проверку.

10. Создадим парочку публикаций. CRL, издателей, пользователей.

11. В ЦУС, в УЦ выбираем пользователей сети и нажимаем опубликовать. Опубликованные сертификаты должны появиться в ранее созданной папке для сертификатов в общей папке.

# Настройка REGISTRATION POINT

1. Создаём папку для ключей, указываем её в первом поле.

2. В настройке REGPOINT выбираем папка ключей пользователя и выбираем недавно созданную папку.

3. Должен будет появиться пользователь.

4. В настройках запускаем транспортный модуль, регистрируем пользователя самостоятельно.

5. Создаём запрос на сертификат, указываем куда сохранить ключи.

6. Ждём уведомление от УКЦ. Удовлетворяем запрос. После удовлетворения пользователь появится во внешних пользователях.

7. Заходим в REGPOINT, создаём запрос на аннулирование.

8. Ждём уведомление от УКЦ. Удовлетворяем запрос. После удовлетворения пользователь меняет статус на «Аннулирован».

# Настройка CA INFORMING

1. Устанавливаем на Net1-Admin CA INFORMING.

Тип базы данных: SQL Server (УКЦ 4.Х)  
Строка подключения к базе данных: Data Source=айпишник\_Net1-Open\DB;Initial Catalog=ViPNetAdministrator;User Id=KcaUser;Password=Number1;

Строку лучше выучить!

2. Настраиваем способ выдачи уведомлений, формируем отчёт. Нажимаем выполнить.

# МОДИФИКАЦИЯ СУЩЕСТВУЮЩЕЙ СЕТИ

1. Добавляем в ЦУС новый узел (Клиент), создаём пользователя. Связываем с пользователями из его сегмента сети и с координатором.

2. В ЦУСе создаём справочники и ключи. В УКЦ выдаём новому пользователю дистрибутив ключей.

4. На Net2-Client выходим из ПО Client и закидываем на машину новый дистрибутив ключей.

5. Запускаем его, завершаем работу необходимых приложений.

6. Выходим из Client (ПКМ по иконке с панели задач).

7. Указываем новый дистрибутив ключей.

//Теперь при входе в ПО Client можно выбирать разных пользователей.

8. Выделяем в УКЦ узлы, которым нужно создать ключи, а также нового клиента. Создаём и передаём в ЦУС ключи.

9. В ЦУСе отправляем ключи на весь список. Ждём статуса «Приняты». Теперь остальные клиенты должны видеть нового клиента, а старого нет.

10. Отправим новому клиенту письмо, смотри на пакеты в координаторе (порт 5000-5003).

10.5 Делаем скриншот списка изданных сертификатов в УКЦ. Как корневых, так и пользовательские.

11. Выгружаем структуру сети в html.

# Компрометация пользователя

Задача 1.4. Компрометация пользователя

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

скомпрометировать ключи пользователя Rem\_Client на узле Удаленный клиент,   
произвести смену ключей пользователя и сетевых узлов,   
отправить обновления и произвести процедуру смены ключа пользователя на узле Удаленный клиент,   
проверить работу защищенной сети после обновления отправив сообщение от пользователя Rem\_Client администратору.

В отчете необходимо зафиксировать процесс настройки скриншотами.

# Настройка агрегированного (соединённого) канала связи

Задача 1.5 Настроить агрегированный канал связи (интерфейс) на Net2-Coord в сторону внешней сети Inet (задействовать eth0 и eth1).

Применить режим, который используется для балансировки нагрузки на подчиненных физических интерфейсах и защищает от сбоев (преимущественно применим в сетях с простой топологией).