Описание модуля А: «Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз»

Необходимо произвести установку и настройку основных компонентов VPN-сети.

При выполнении модуля А ставятся следующие цели:

1. Произвести настройку сетевых интерфейсов

2. Произвести установку ПО на соответствующие узлы

3. Произвести первичную инициализацию узлов

4. Настроить роли и права узлов

5. Произвести выпуск сертификатов безопасности

6. Настроить взаимодействие между узлами

7. Произвести проверку работоспособности

При выполнении данного модуля А ставятся следующие задачи:

Задача 1.1. Развертывание ПК Administrator в качестве центра сертификации

Установить базу данных на ВМ Net1-DB (незащищенный узел)

Установить и настроить рабочее место администратора Certification Authority (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД.

Установить клиент ЦУС на ВМ Net1-DB (незащищенный узел)

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

Предисловие

Перед выполнением модуля **ОБЯЗАТЕЛЬНО** синхронизируйте время на всех виртуальных машинах, иначе ваша сеть не будет работать корректно.

Отключите или настройте Firewall для взаимодействия между виртуальными машинами.

При создании нужных сетевых адаптеров убедитесь, что вы не допустили ошибки при их указании на виртуальные машины в соответствии со схемой.

Задача 1.1: Решение

Устанавливаем БД SQL на ВМ Net1-Open.

Для инсталляции БД используется пакет, лежащий в каталоге с ЦУСом.

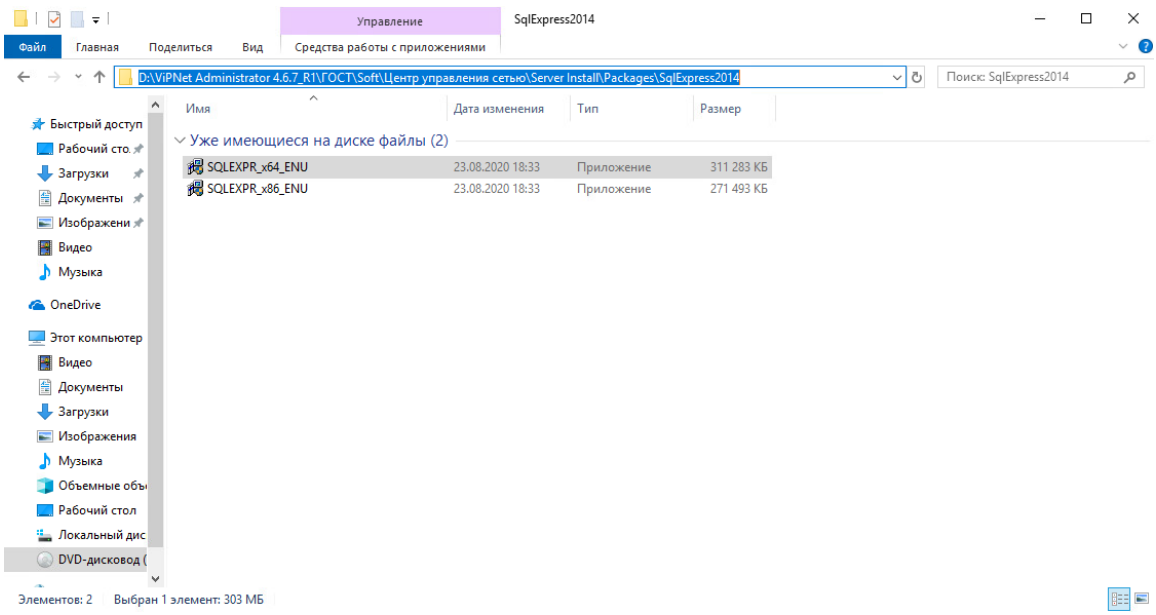

Рисунок 1 – Пакет с БД

Выбираем каталог для извлечения пакета, нажимаем ЛКМ «Ok». После чего должно открыться окно установщика.

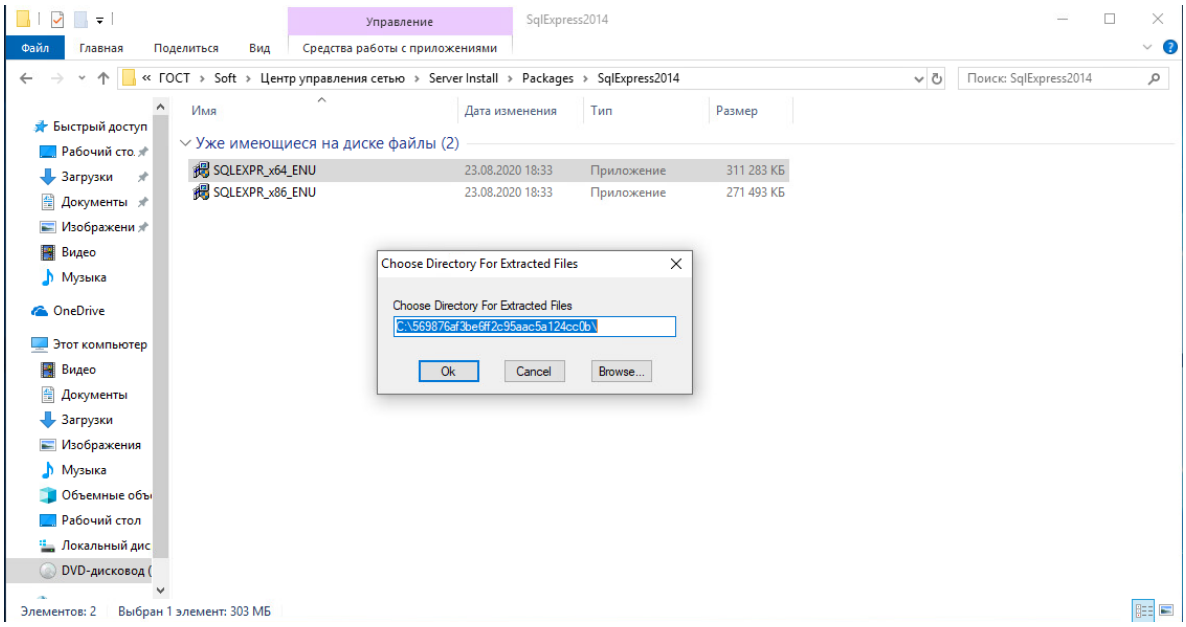

Рисунок 2 – Извлечение пакета с БД

Выбираем ЛКМ «New SQL Server stand-alone installation or add features to an existing installation».

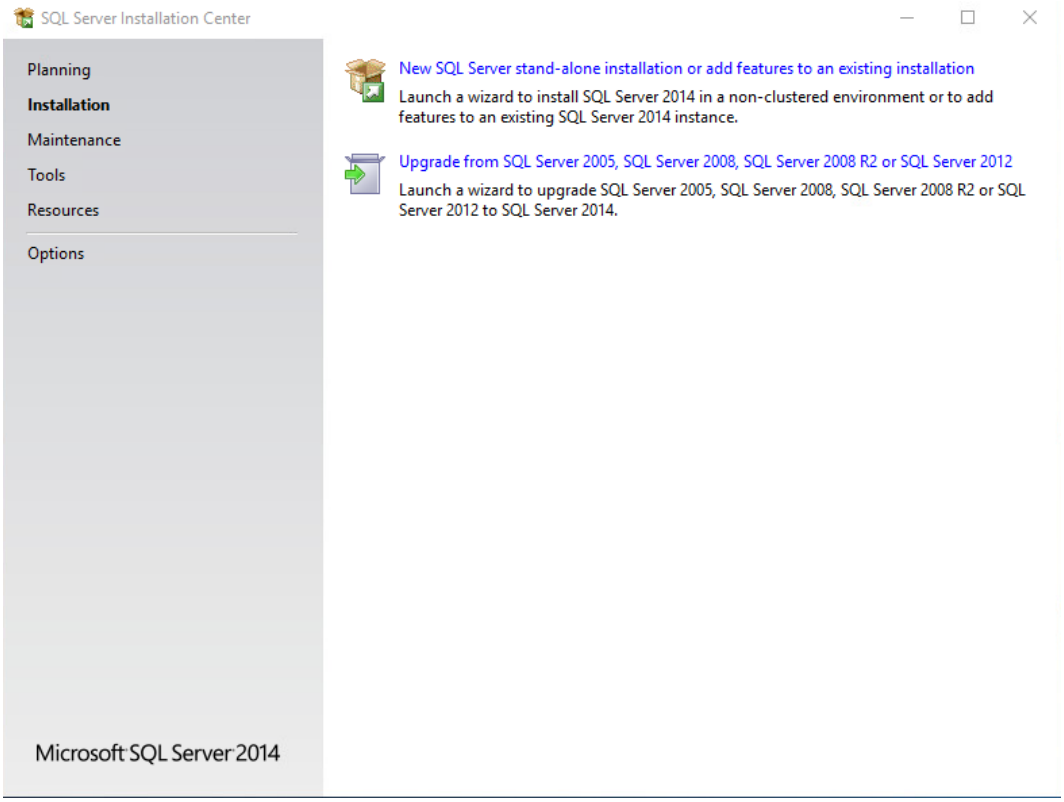

Рисунок 3 – Установка БД SQL

Ставим галочку в пункте «I accept the license terms». Далее прожимаем 3 раза ЛКМ «Next» до шага «Feature Selection».

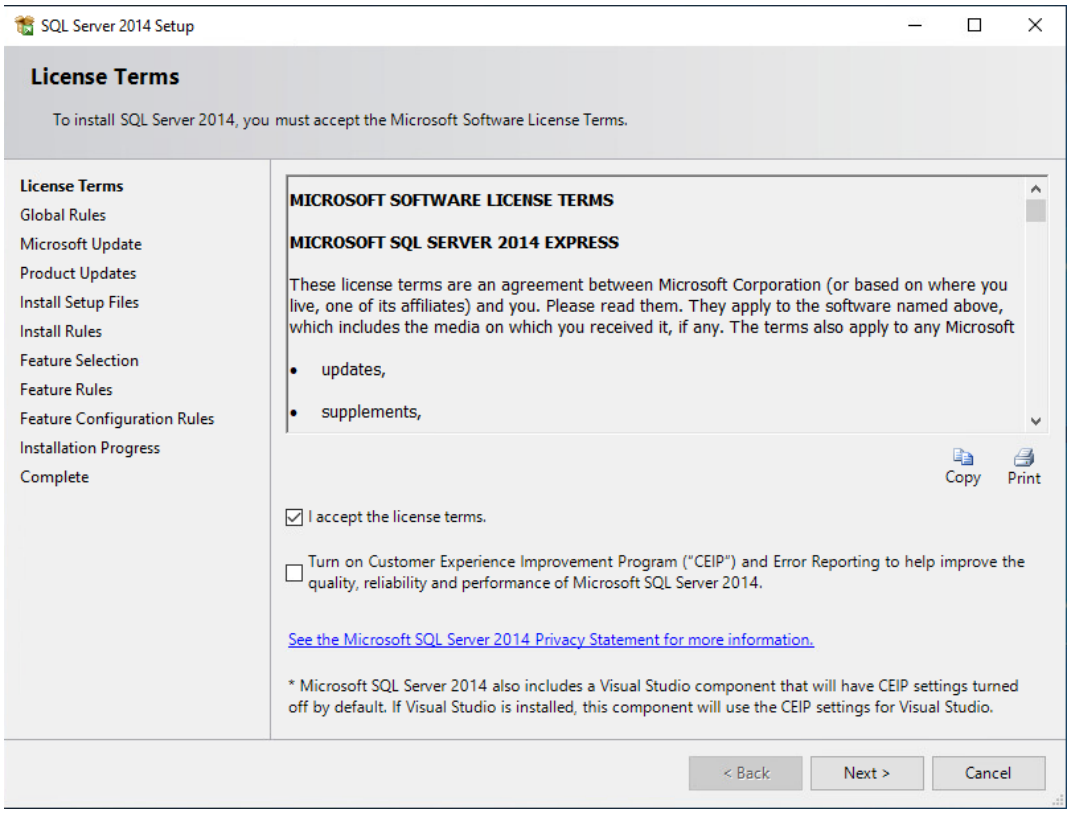

Рисунок 4 – License Terms

Выбираем все функции для нашего экземпляра сервера и продолжаем установку.

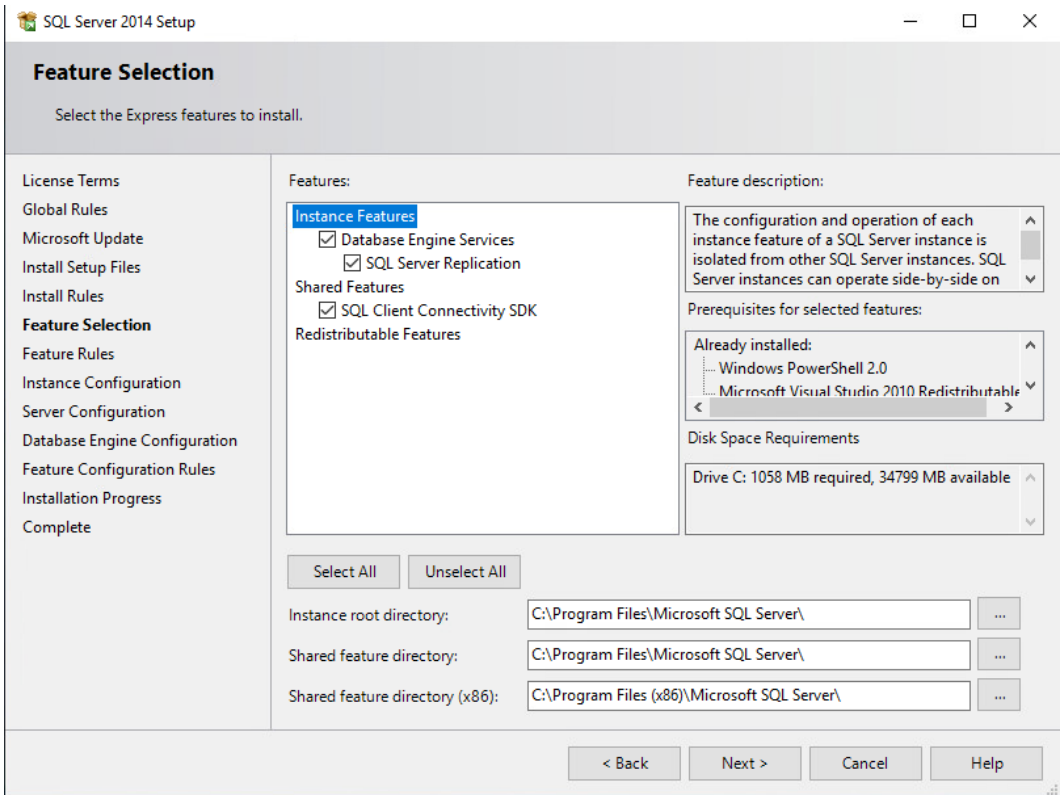

Рисунок 5 – Feature Selection

Выбираем «Named instance» и изменяем наше стандартное имя на «WINNCCSQL».

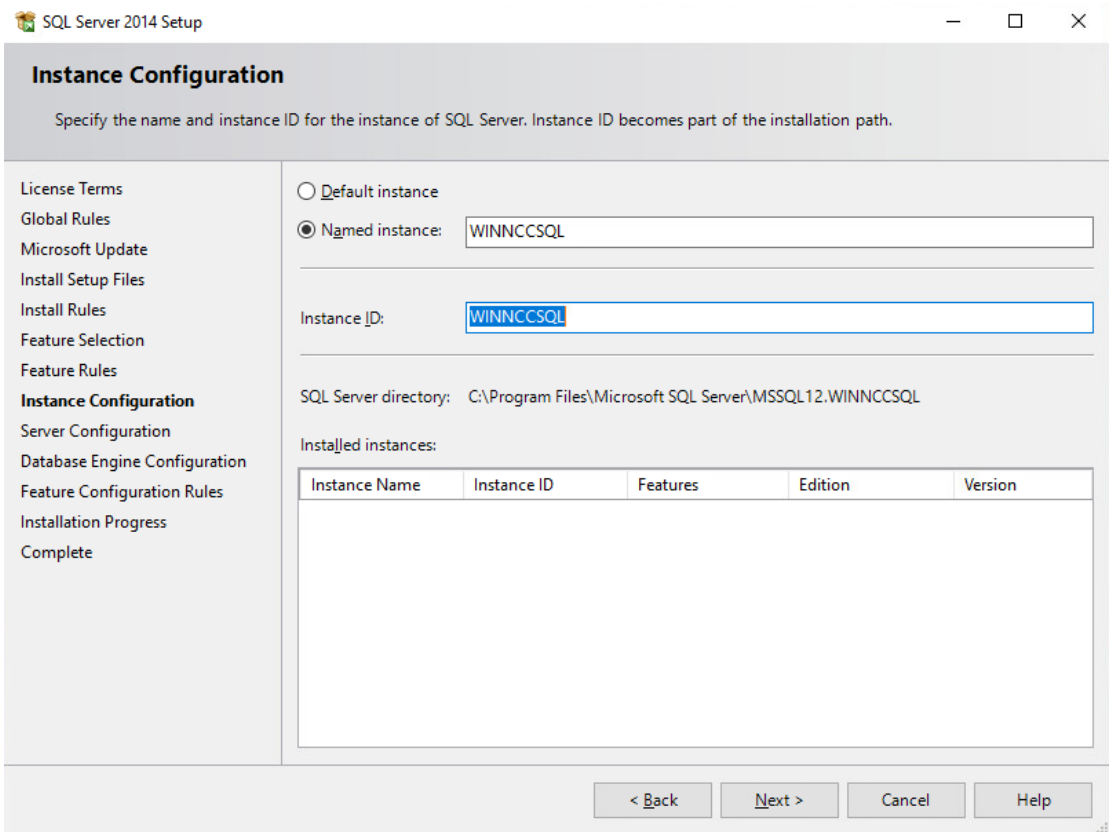

Рисунок 6 – Instance Configuration

Под колонкой «Startup Type» у сервиса «SQL Server Browser» выбираем «Automatic». Эта служба нам понадобится для успешного соединения с экземпляром нашего сервера.

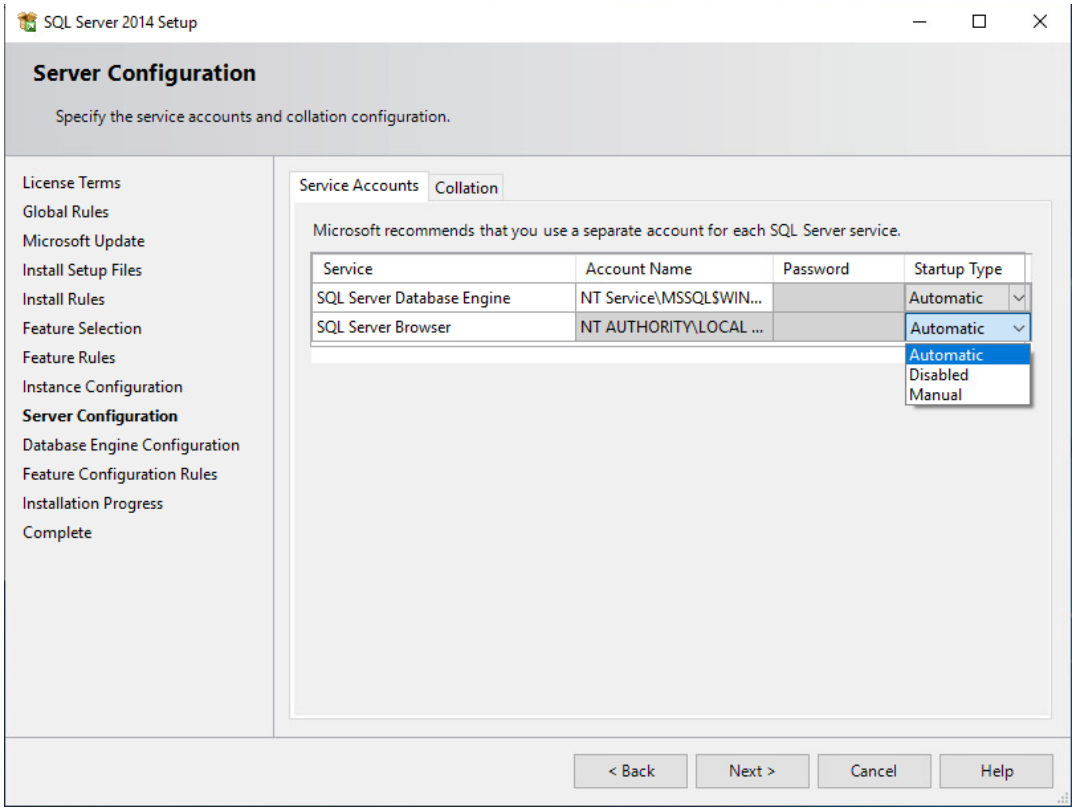

Рисунок 7 – Server Configuration

Выбираем режим аутентификации «Mixed mode», вводим пароль и подтверждаем. Тут же во вкладке «FILESTREAM» везде обязательно ставим галочки, иначе не сможем подключиться к нашему серверу с другой машины.

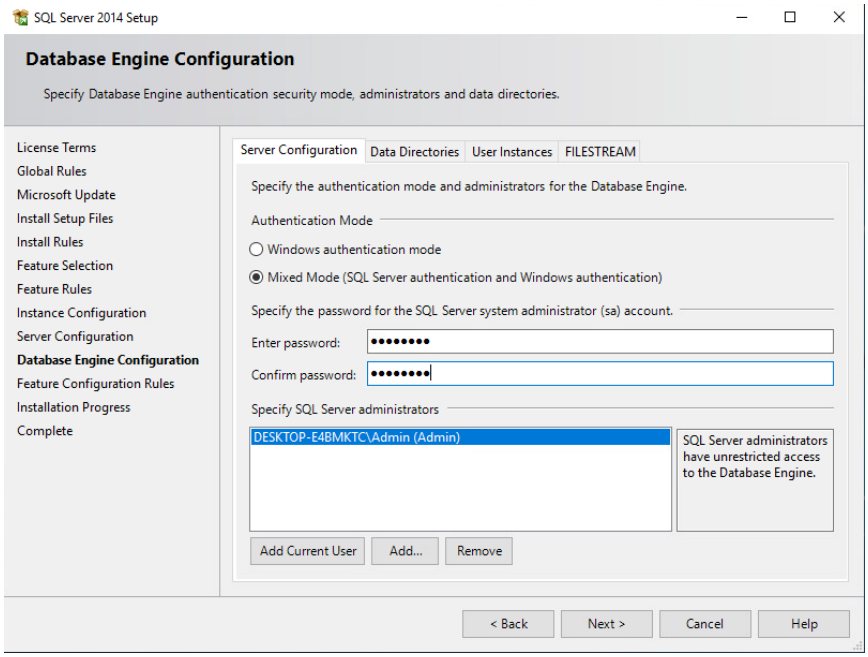

Рисунок 8 – Database Engine Configuration ч.1

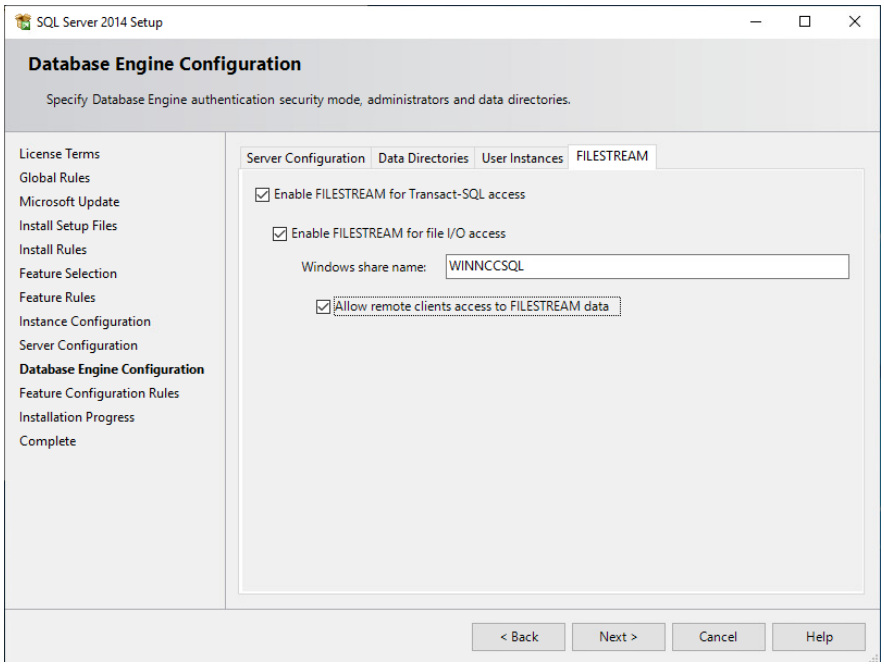

Рисунок 9 - Database Engine Configuration ч.2

Прожимаем «Next» и ждем успех.

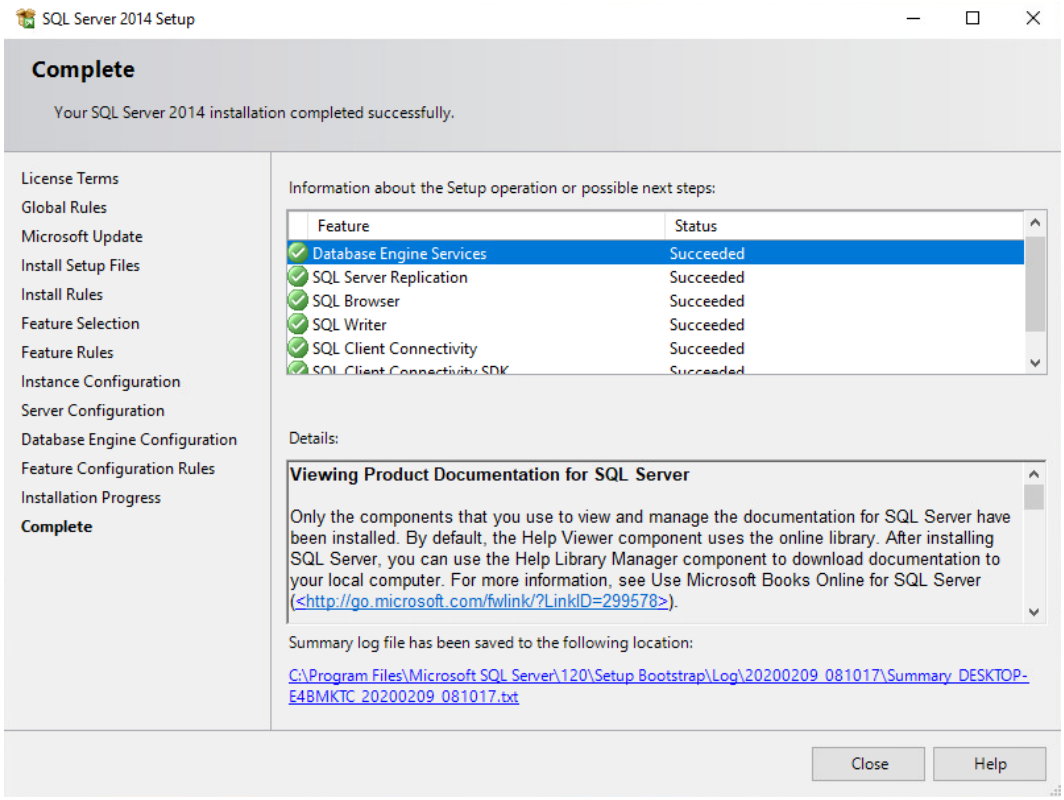

Рисунок 10 – Complete

После установки БД, нам нужно разрешить подключение к ней, для этого нам нужно зайти в «SQL Server 2014 Configuration Manager».

Заходим в «SQL Server Network Configuration» → «Protocols for WINNCCSQL» → «TCP/IP» и ставим у пункта «Enabled»: «Yes». Переходим в «SQL Server Services», находим наш сервер «SQL Server (WINNCCSQL)» кликаем по нему ПКМ и выбираем «Restart». Теперь наши настройки применились, можем подключиться с другой ВМ.

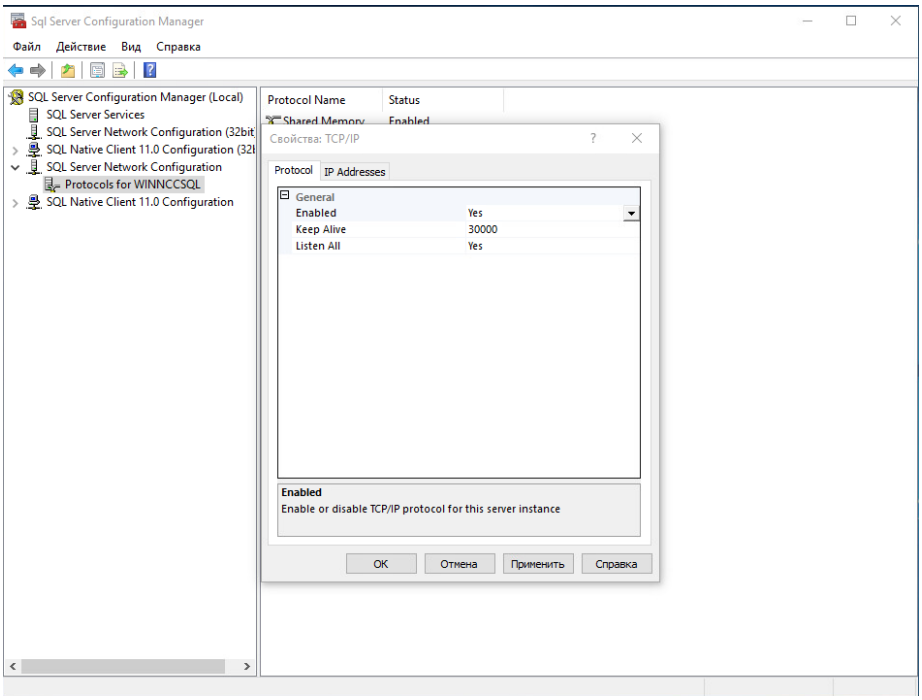

Рисунок 11 – SQL Server Network Configuration

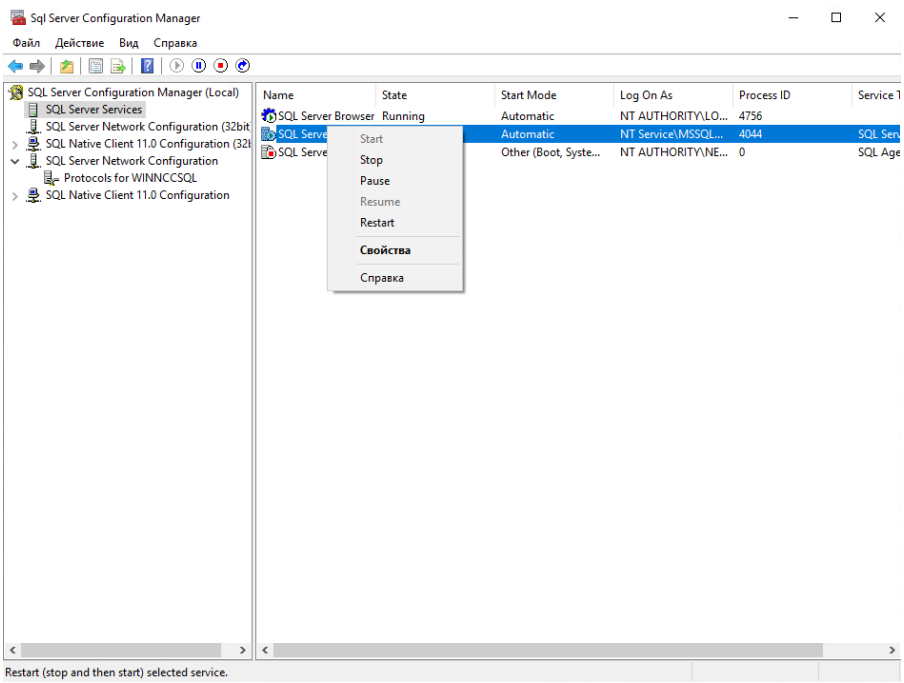

Рисунок 12 – SQL Server Services

Устанавливаем ЦУС (серверное приложение ЦУС) на ВМ Net1-AdminCA.

Запускаем установщик, выбираем язык и принимаем соглашение. Задаем имя сервера, которое состоит из «.»-ip-адрес экземпляра сервера и «\WINNCCSQL»- экземпляра сервера по умолчанию, которое мы задали при установке БД. Данные имени пользователя и пароля мы указываем такие же, которые указывали в режиме аутентификации «Mixed mode».

Проблемы с подключением могут возникнуть из-за неверных данных или не верной установки вашего экземпляра сервера.

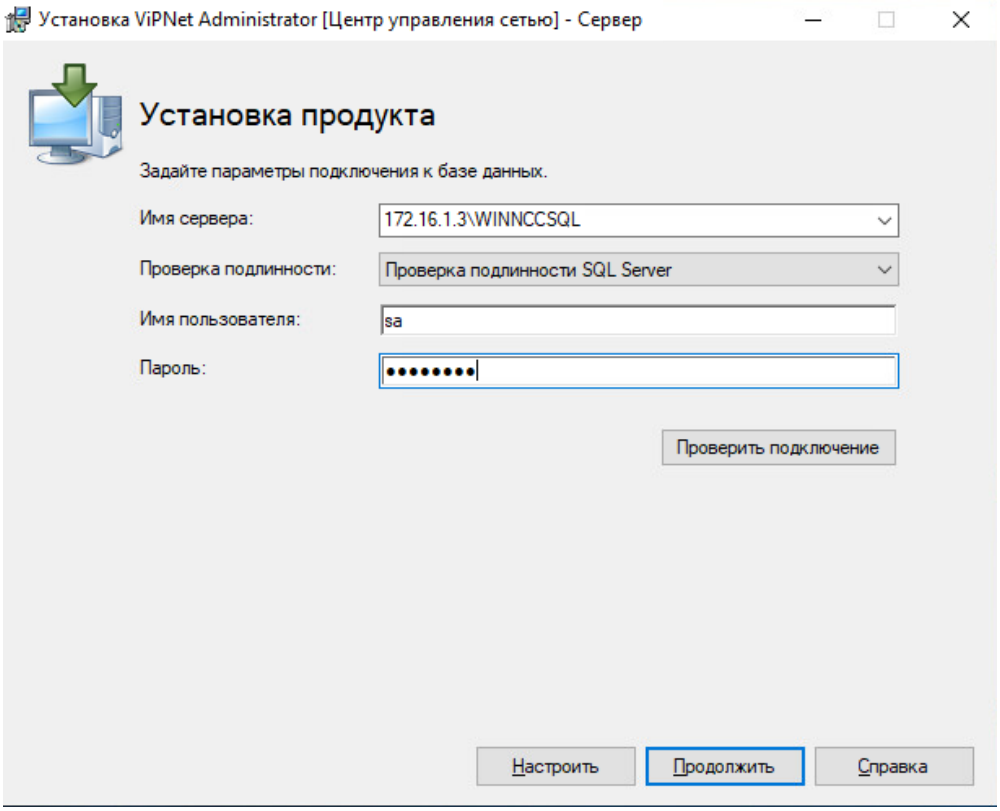

Рисунок 13 – Установка продукта ViPNet Administrator [Центр управления сетью] - Сервер

Устанавливаем ЦУС (клиентское приложение ЦУС) на ВМ Net1-Open

Запускаем установщик, выбираем язык и принимаем соглашение. Никаких параметров установки нет, нажимаем «Установить сейчас».

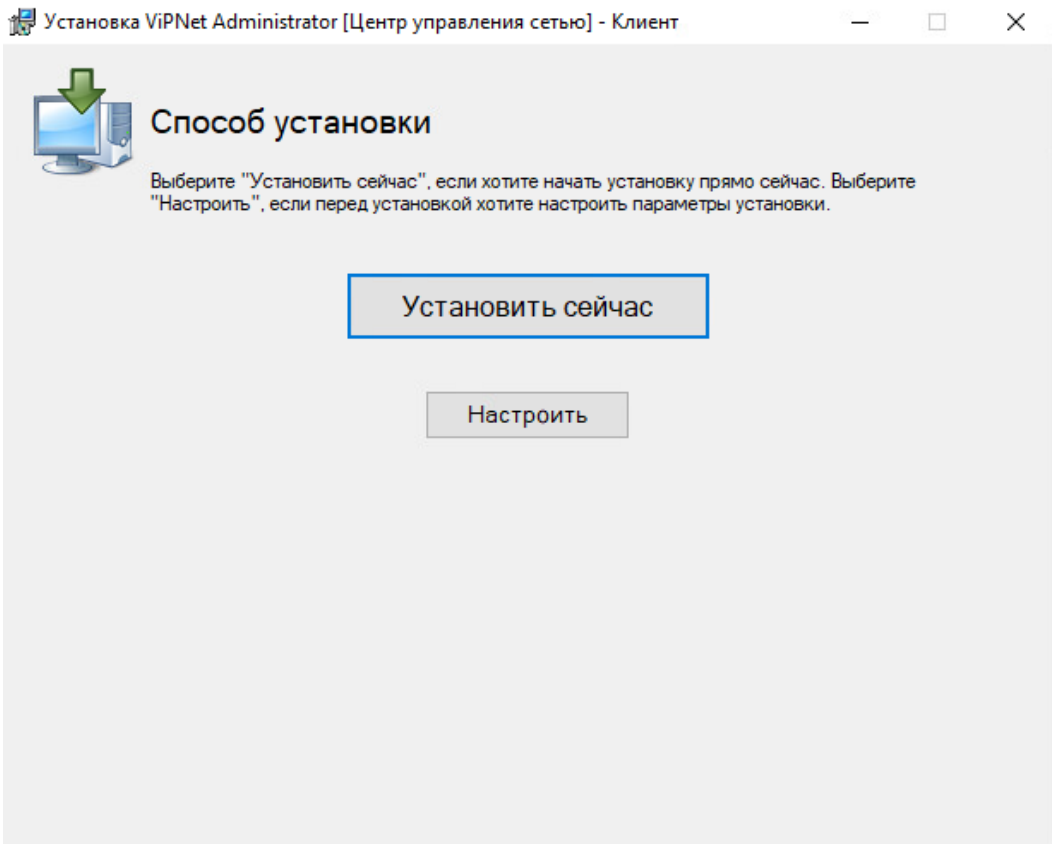

Рисунок 14 – Установка ViPNet Administrator [Центр управления сетью] - Клиент

Указываем ip-адрес сервера ЦУС и кликаем «Продолжить». При неудаче пробуем перезапустить службы отвечающие за функционирование сервера ЦУСа или БД.

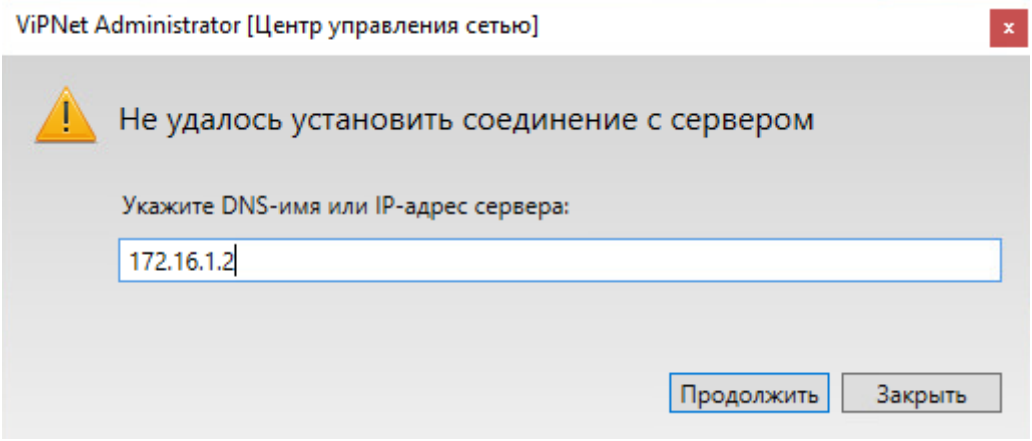

Рисунок 15 – Подключение к серверу ЦУС

Указываем пароль и имя пользователя по умолчанию - «Administrator». В следующем окне потребуется изменить пароль на свой.

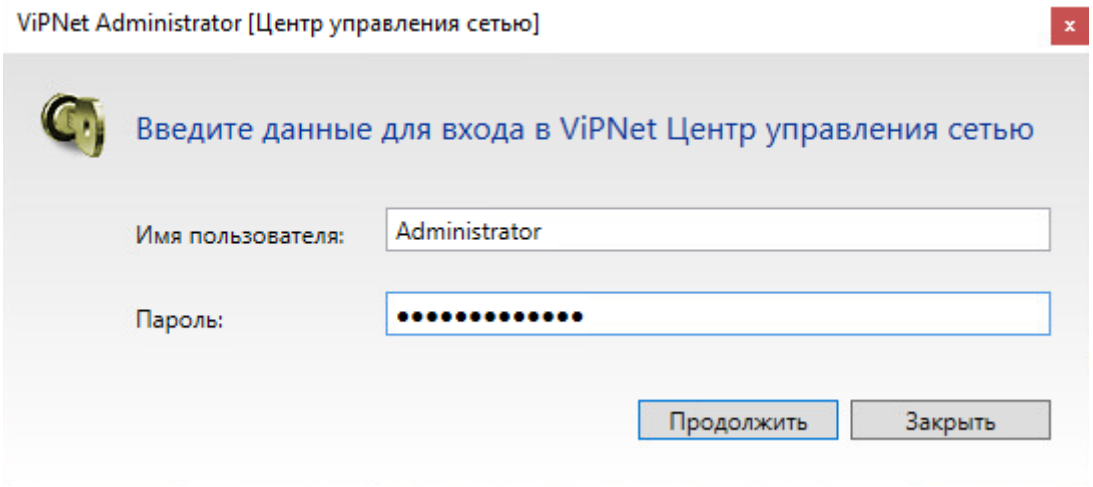

Рисунок 16 – Ввод данных для входа в ViPNet Центр управления сетью

Выбираем файл, содержащий информацию о лицензионных ограничениях (прим. «.itcslic»). Кликаем «Продолжить».

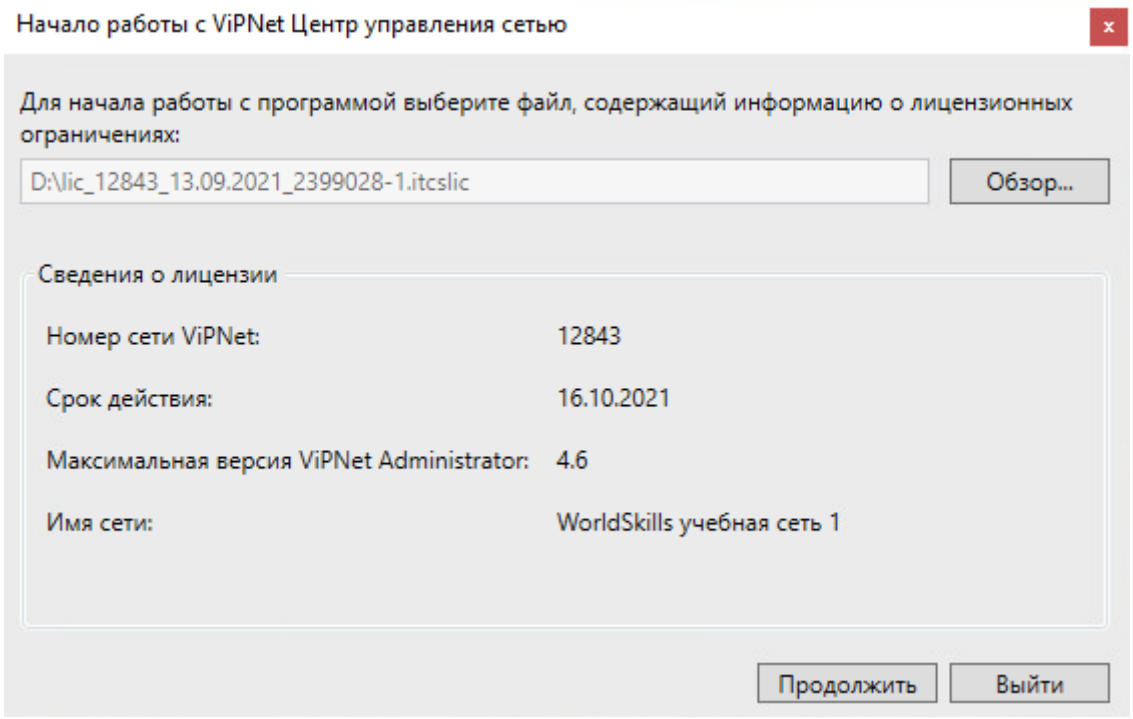

Рисунок 17 – Начало работы с ViPNet Центр управления сетью

Устанавливаем УКЦ на ВМ Net1-AdminCA.

Установка подобную клиенту, без параметров. Принимаем соглашение и нажимаем «Продолжить». Далее нажимаем «Установить сейчас».

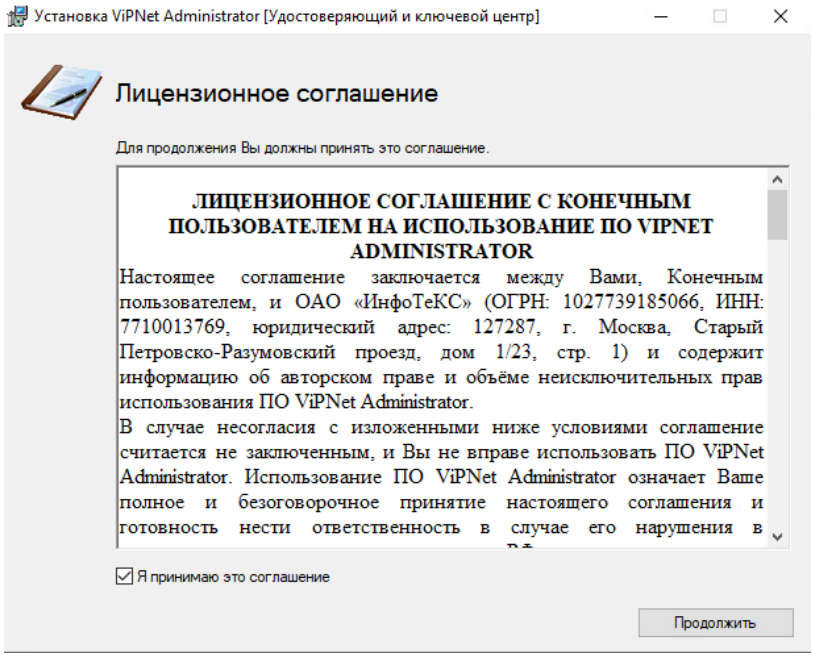

Рисунок 18 – Установка ViPNet Administrator [Удостоверяющий и ключевой центр] – Лицензионное соглашение

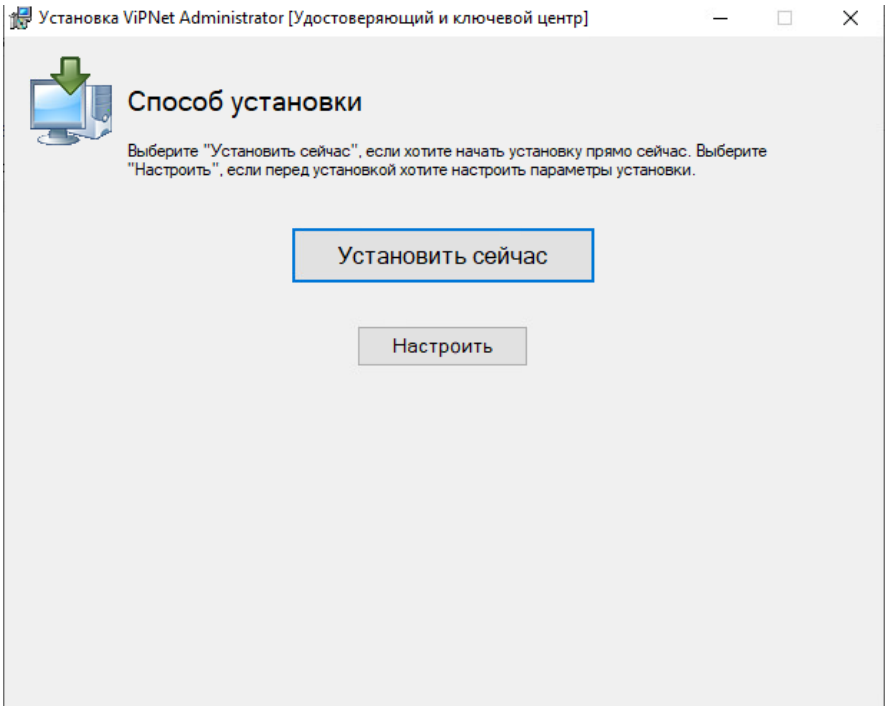

Рисунок 19 – Установка ViPNet Administrator [Удостоверяющий и ключевой центр] – Способ установки

Задача 1.2. Установка ПО VPN Coordinator и ПО VPN Client для Certification Authority

1. установить ПО Client, рабочее место администратора;

2. установить и инициализировать ПО Coordinator HW-VA;

Задача 1.2: Решение

Устанавливаем ПО Client на Net1-AdminCA.

Запускаем установщик, принимаем соглашение. Никакие параметры не меняем, нажимаем «Установить». После установки перезагружаем компьютер.

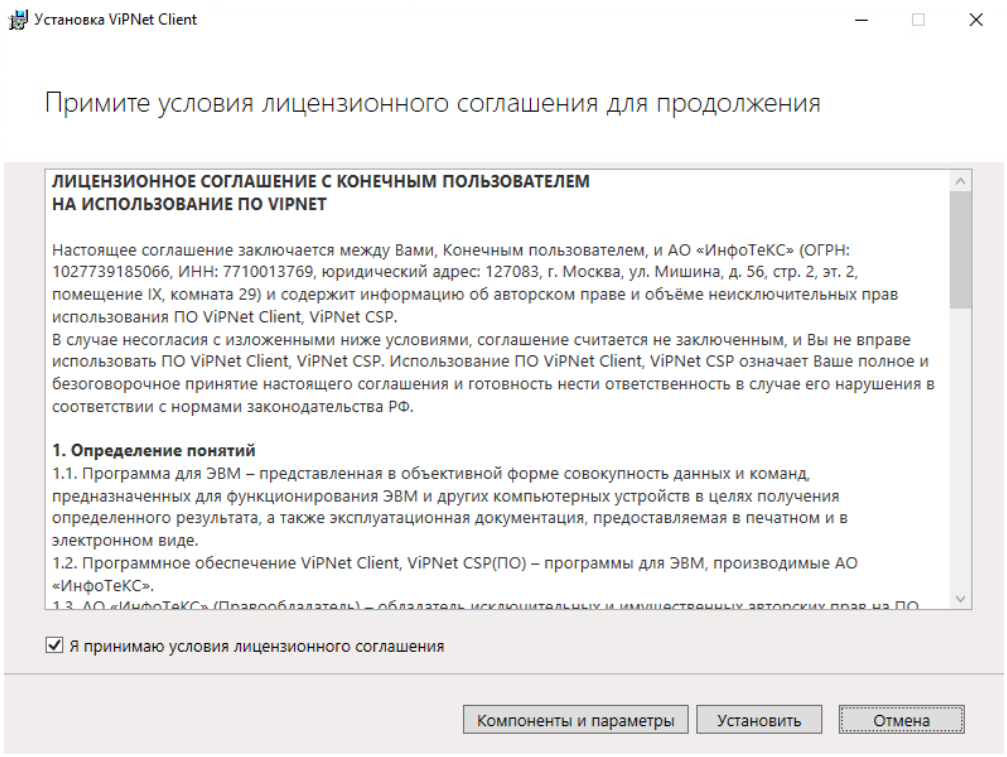

Рисунок 20 – Установка ViPNet Client

Устанавливаем и инициализируем ПО Coordinator HW-VA для Net1.

Устанавливать ничего не придется, следует только импортировать виртуальную машину из образа «.ova». Вводим логин и пароль, после чего знакомимся с лицензионным соглашением, нажимаем «Yes».

Данные для входа по умолчанию: user; user.

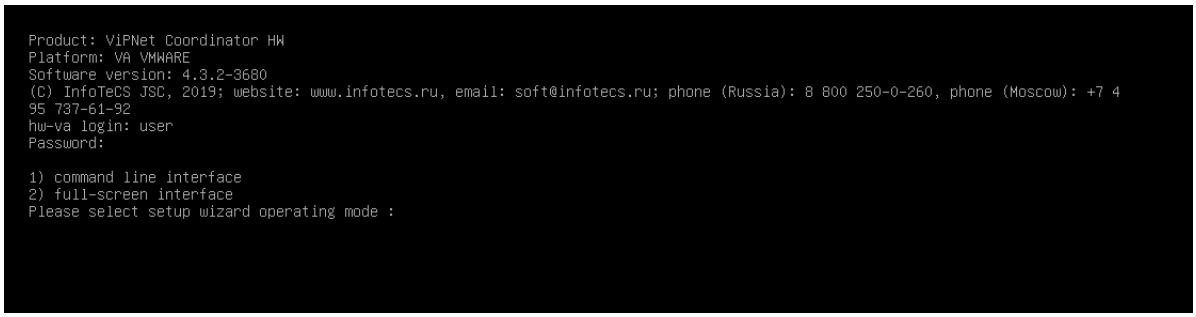

Рисунок 21 – Установка ViPNet Coordinator HW

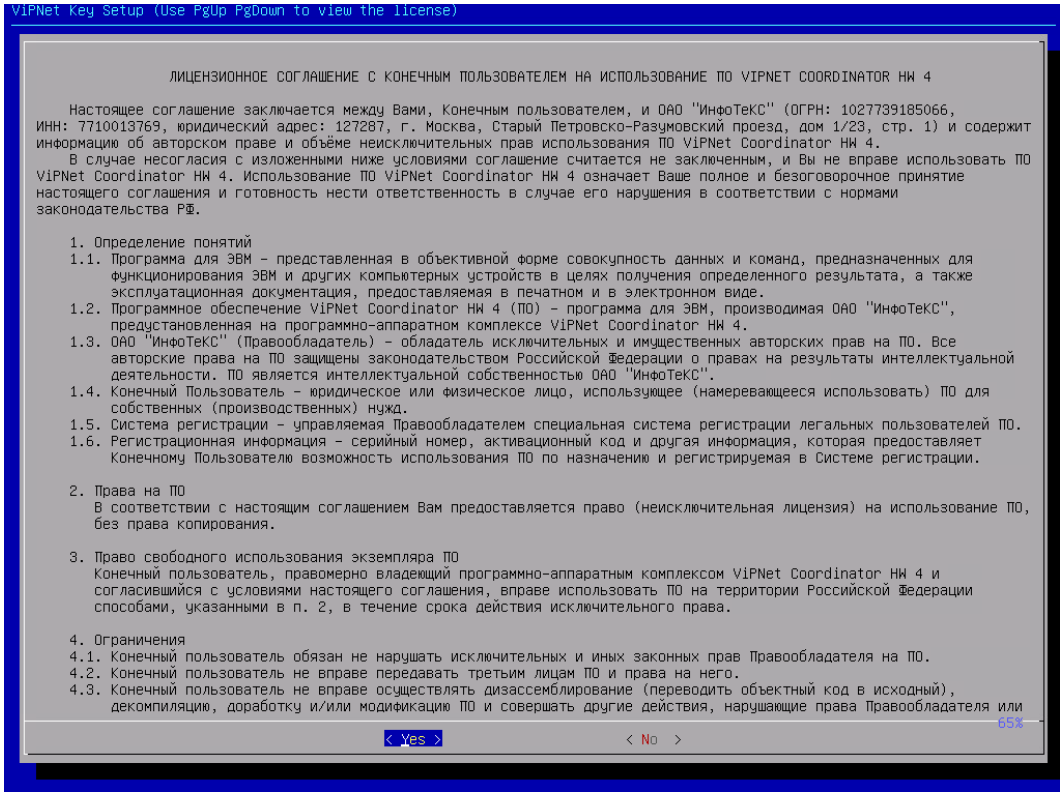

Рисунок 22 – Установка ViPNet Coordinator HW – Лицензионное соглашение

Нажимаем «Next» для продолжения установки ключей. Дату и время важно поставить ту, которая стоит на других машинах, от этого будет зависеть работоспособность вашей сети. Выбирая по очереди континент, страну, часовой пояс, дату и время нажимаем «Next» и «Yes».

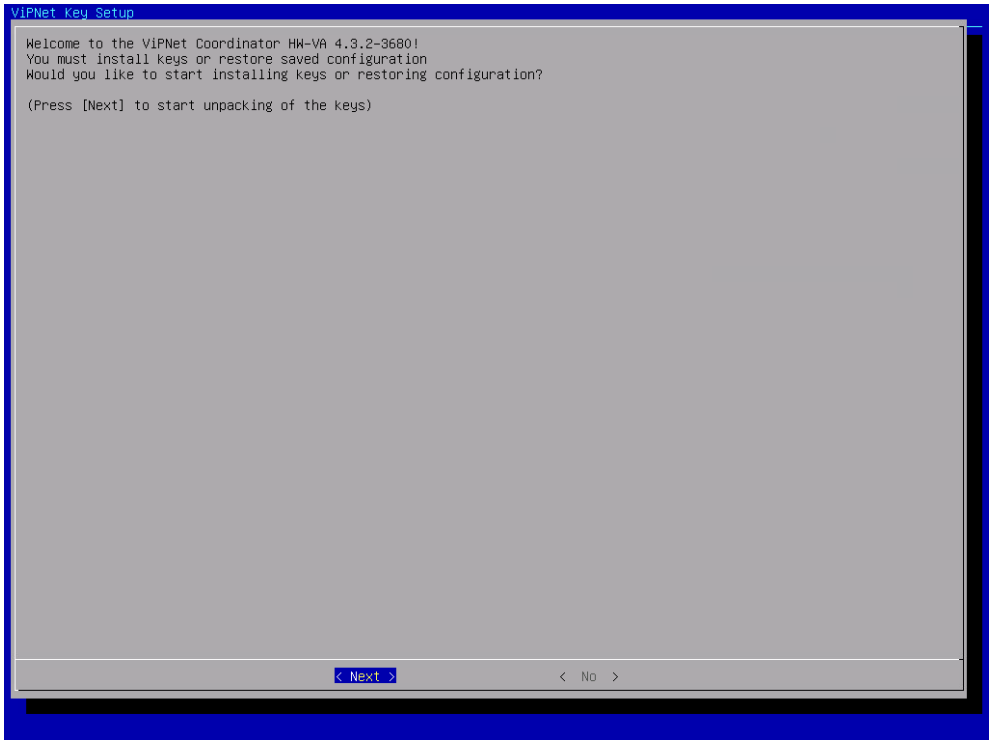

Рисунок 23 – ViPNet Key Setup

Останавливаемся на этапе выбора установки ключей, потому что у нас их попросту пока что нет. Оставляем все как есть и переходим к следующему шагу.

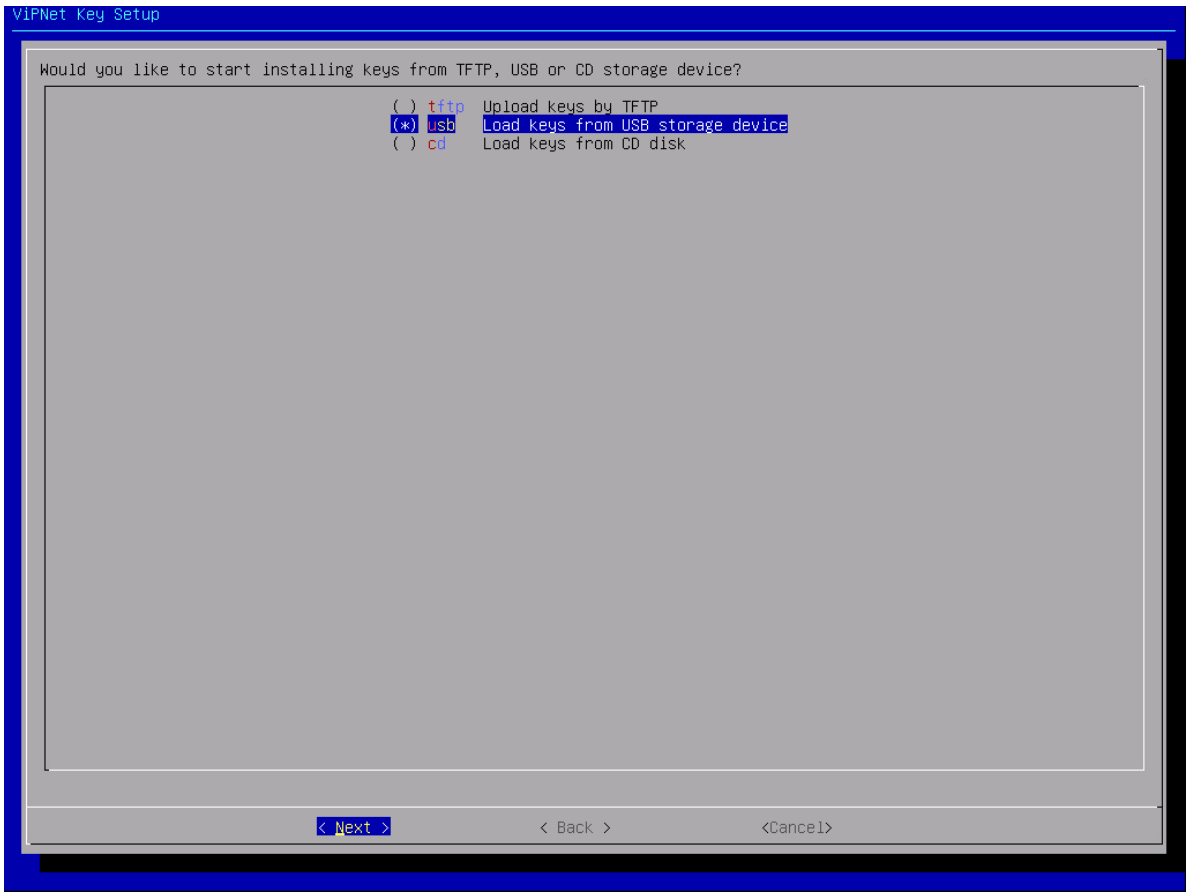

Рисунок 24 – Выбор установки ключей.

Задача 1.3. Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины

1. установить ПО Client.

2. установить ПО Publication Service.

3. установить ПО Registration Point.

4. установить ПО CA Informing

Задача 1.3: Решение.

Устанавливаем ПО Client также, только на ВМ Net1-OperCA.

Устанавливаем ПО Publication Service на ВМ Net1-OperCA.

Запускаем установщик и принимаем соглашение. Нажимаем «Продолжить».

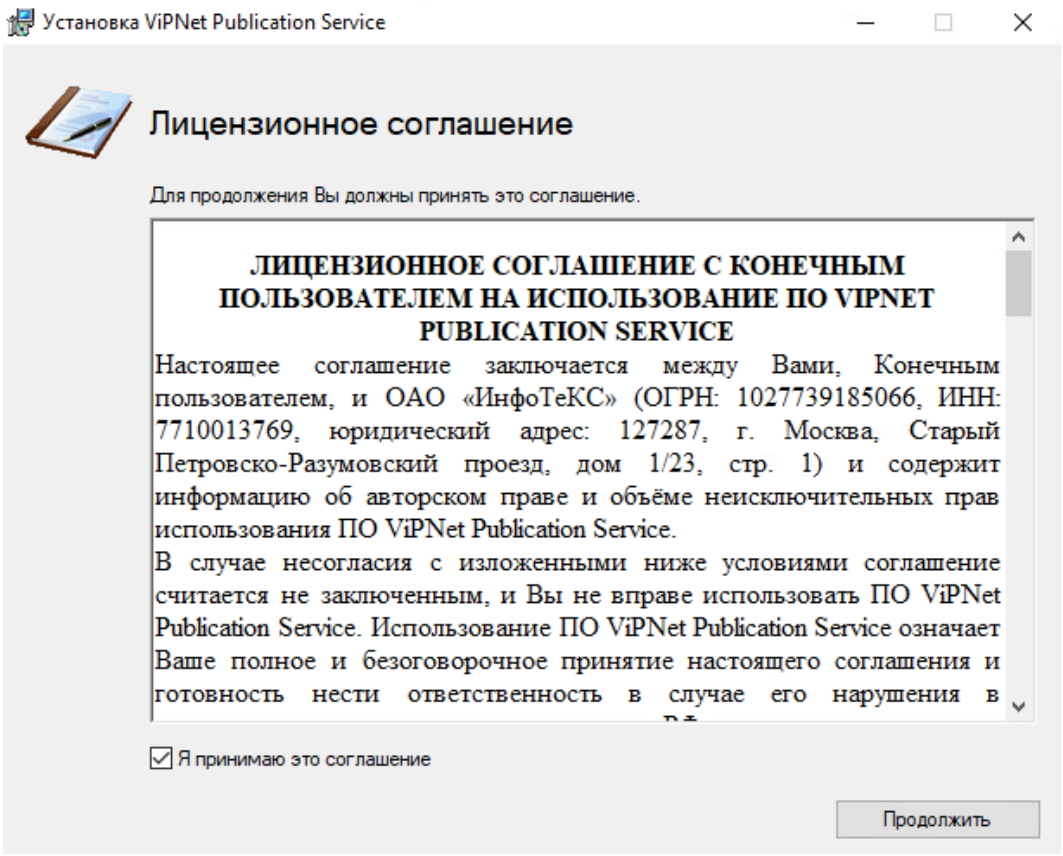

Рисунок 25 – Установка ViPNet Publication Service

Устанавливаем ПО Registration Point на ВМ Net1-OperCA.

Запускаем установщик и принимаем соглашение. Нажимаем «Продолжить» и далее «Установить сейчас».

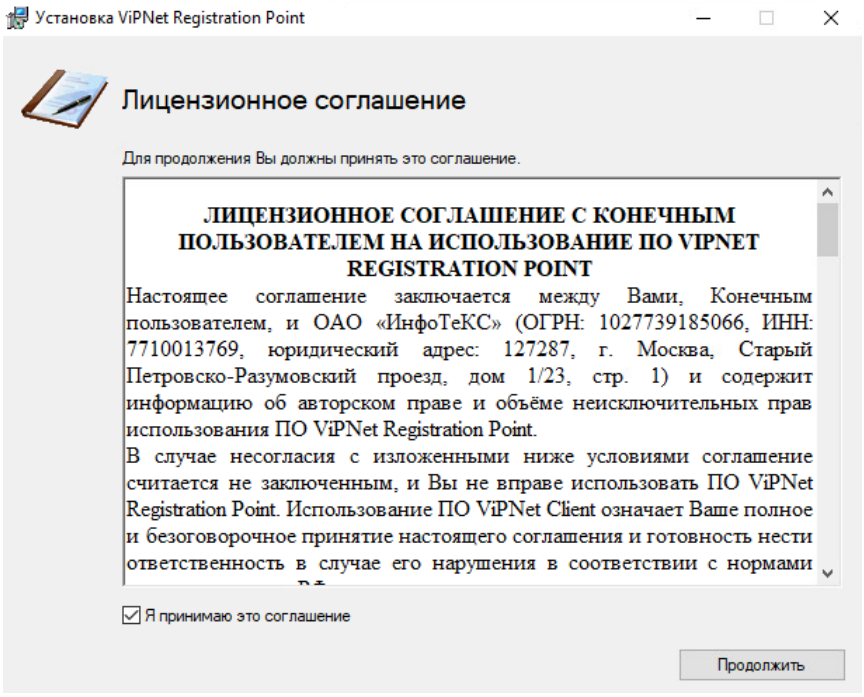

Рисунок 26 – Установка ViPNet Registration Point – Лицензионное соглашение

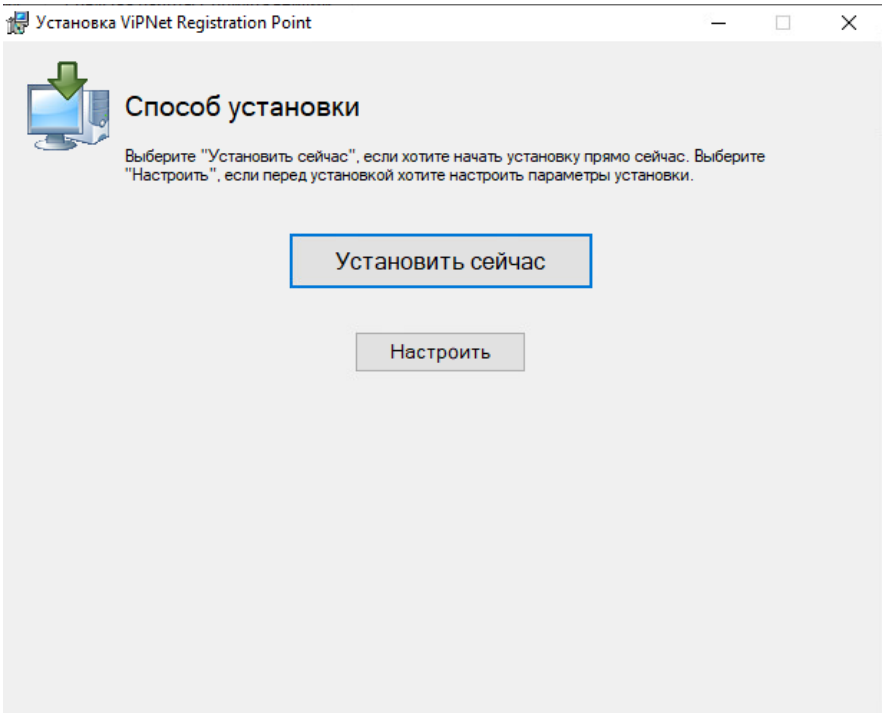

Рисунок 27 – Установка ViPNet Registration – Способ установки

Устанавливаем ПО CA Informing на ВМ Net1-OperCA.

Запускаем установщик, жмем «Далее» и принимаем лицензионное соглашение. Выбираем каталог для установки и кликаем «Далее». После чего нажимаем «Установить».

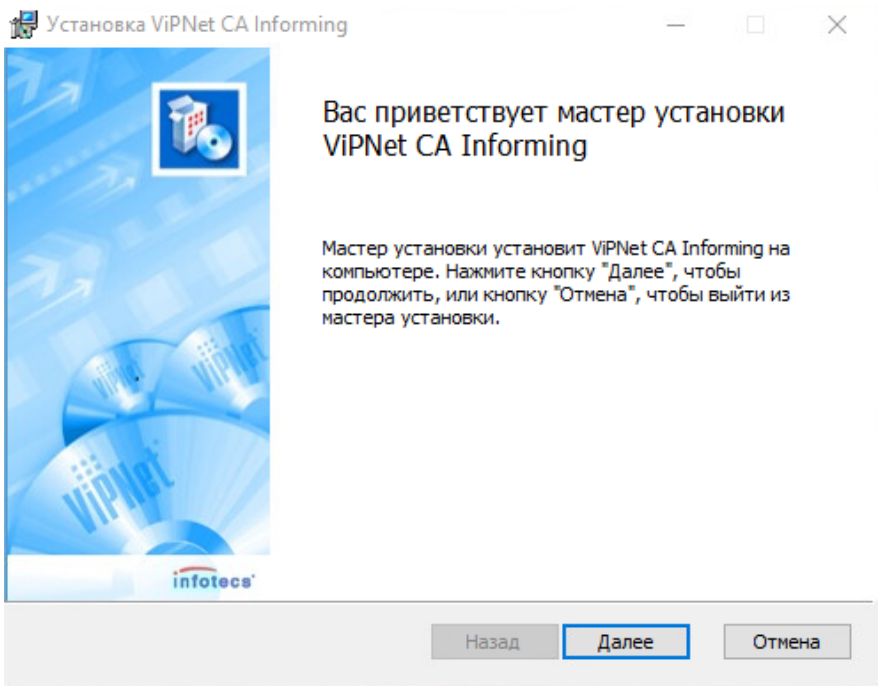

Рисунок 28 – Установка ViPNet CA Informing

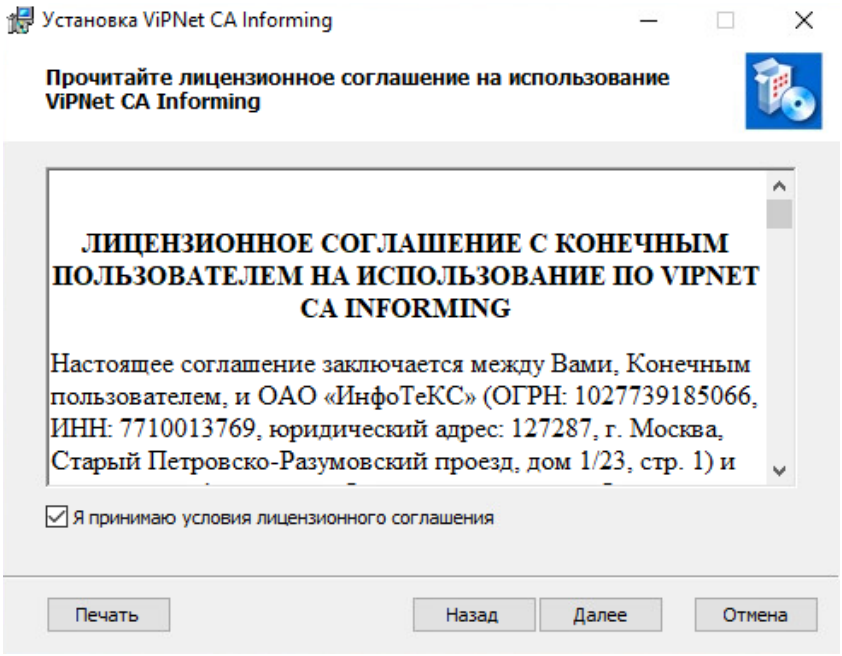

Рисунок 29 – Установка ViPNet CA Informing – Лицензионное соглашение

Задача 1.4. Установка ПО Coordinator и ПО Client для организации сети филиала

1. установить и инициализировать ПО Coordinator HW-VA.

2. установить ПО Client, рабочее место пользователя.

Необходимо зафиксировать процесс установки скриншотами форм + сделать скриншот директории, в которую установлено ПО, и скриншот первого запуска приложения.

Задача 1.4: Решение

Принцип установки ничем не отличается от «Задача 1.2». Устанавливаем на соответствующие машины.

Задача 1.5. Развертывание удостоверяющего центра в составе сети

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена далее.

IP адреса сетей перечислены в начале задания (по названию сетей)

Задача 1.6. 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 папке (создать подпапку Задача 1.6), 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 (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.

Задача 1.5;1.6: Решение

Инициализируем УКЦ на ВМ Net1-AdminCA.

Запускаем установленный нами ранее УКЦ. Выбираем «Настройка новой базы данных», далее «Продолжить». Для продолжения нажимаем «Далее».

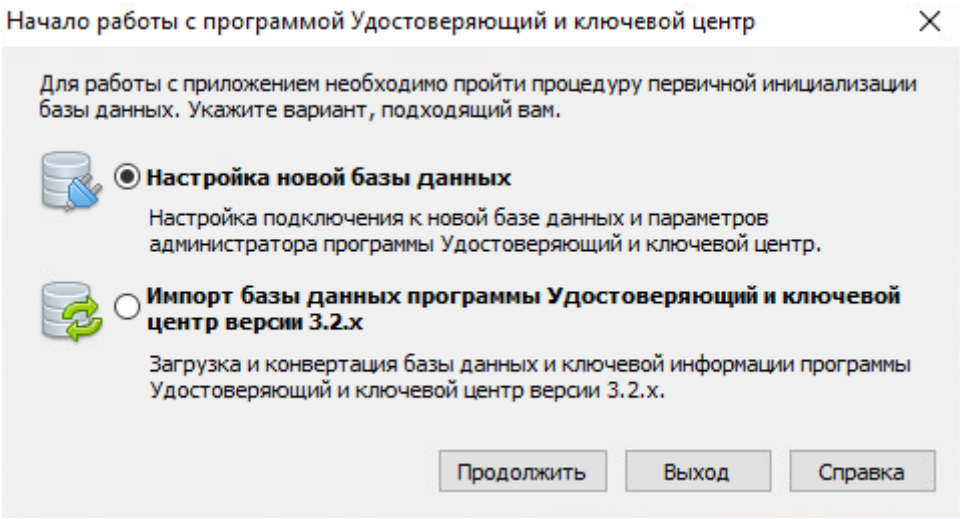

Рисунок 30 – Начало работы с программой Удостоверяющий и ключевой центр

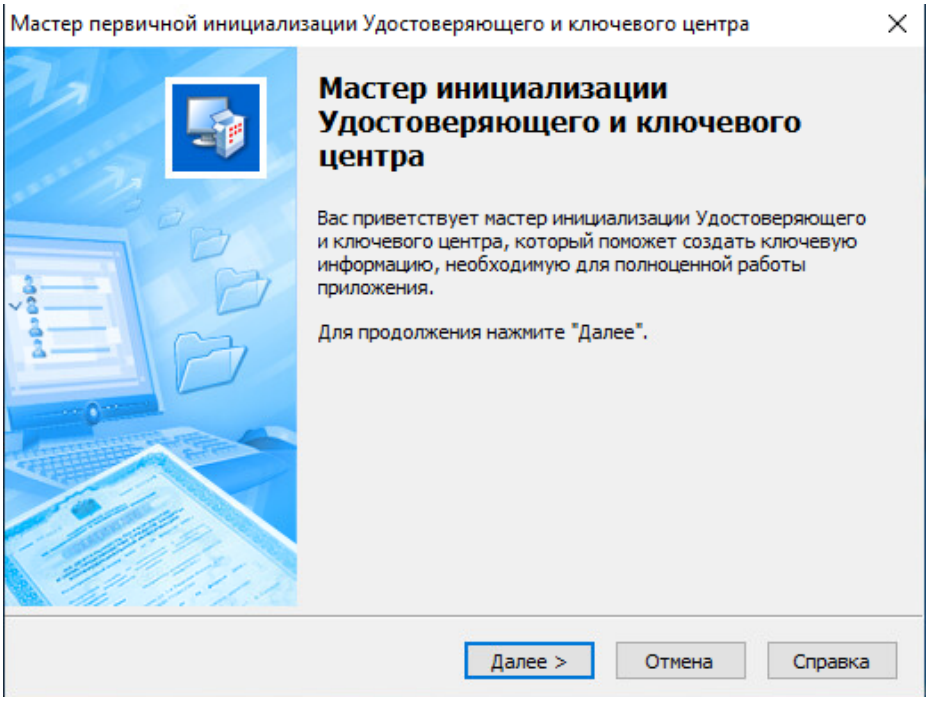

Рисунок 31 – Мастер первичной инициализации Удостоверяющего и ключевого центра

Перемещаем указатель мыши в пределах окна до 100%.

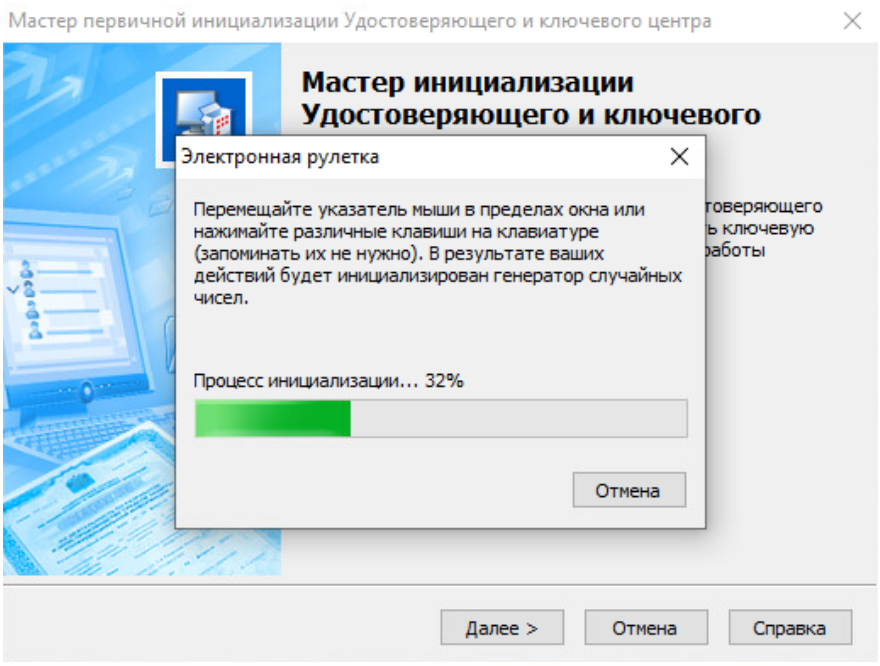

Рисунок 32 – Электронная рулетка

Указываем ip-адрес и имя нашего экземпляра сервера. Имя базы данных оставляем по умолчанию.

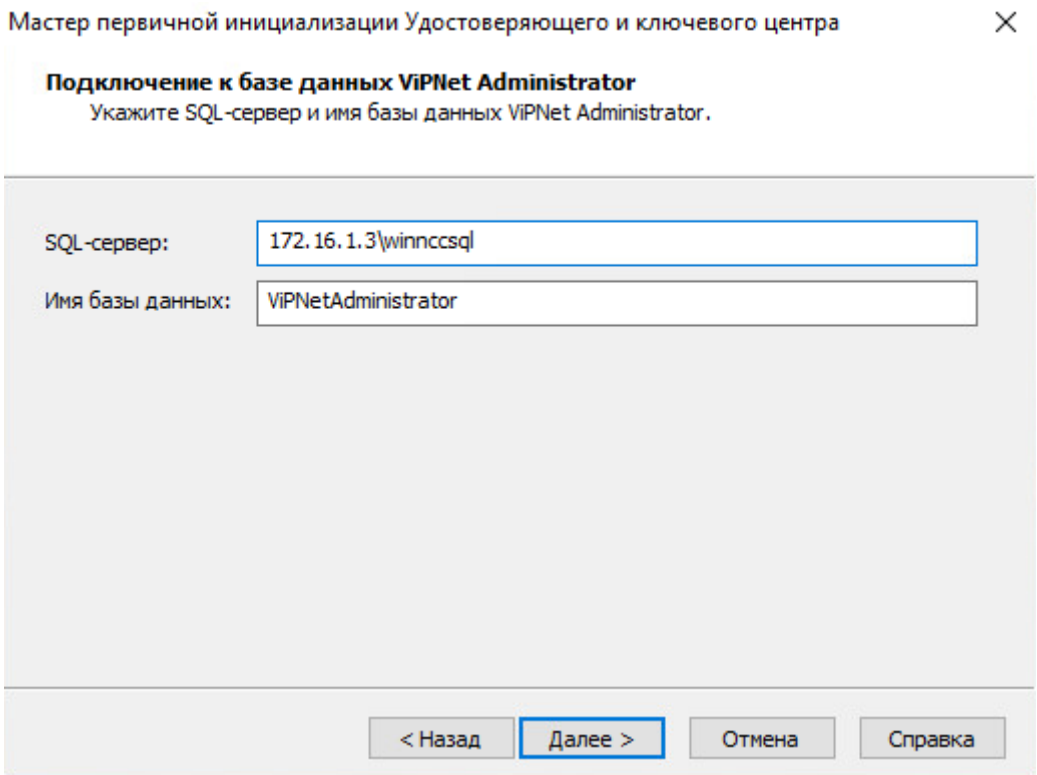

Рисунок 33 – Подключение к базе данных ViPNet Administrator ч.1

Выбираем тип проверки «По имени и паролю пользователя SQL-сервера». Заполняем такими же данными как и при подключении ЦУСа.

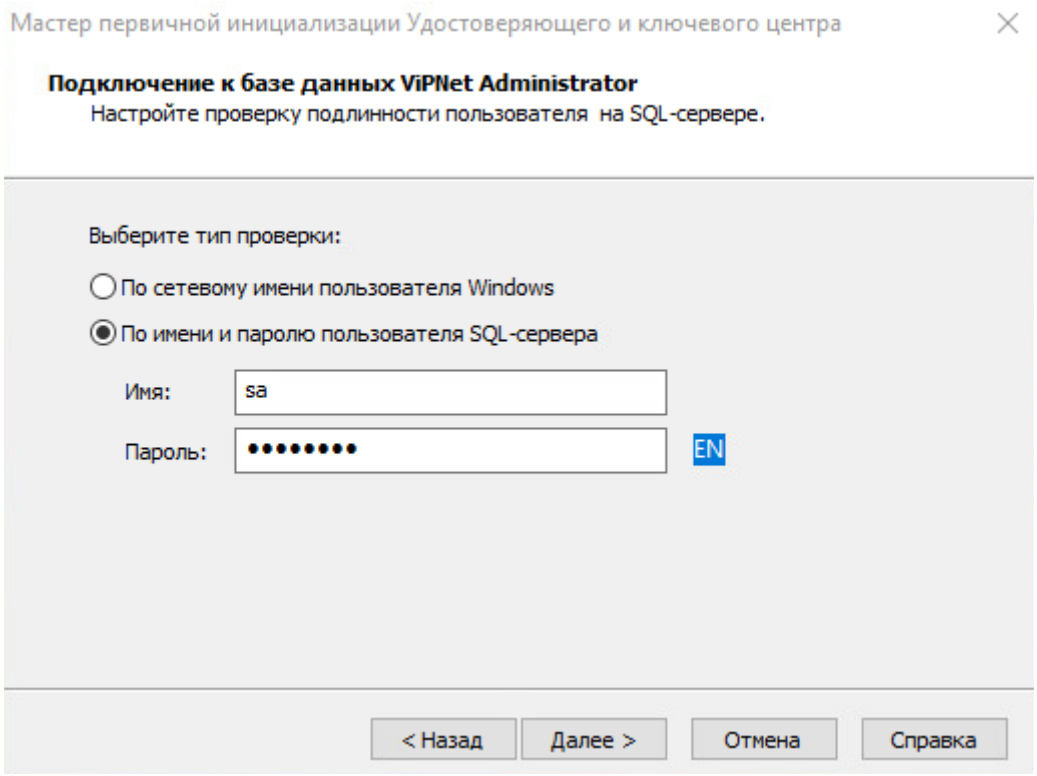

Рисунок 34 - Подключение к базе данных ViPNet Administrator ч.2

После успешного подключения следует создание администратора и заполнение сведений о сертификате в виде:

• Имя: <Имя пользователя или узла>

• Электронная почта

• Город

• Область

• Организация

• Подразделение

• Почтовый индекс

Заполняйте соответствующе, смотря на задание.

Кроме заполнения сведений о сертификате, необходимо настроить их параметры после перевода УКЦ в режим аккредитованного удостоверяющего центра, указав:

• сведения о средствах УЦ,

• средство электронной подписи издателя

• средства удостоверяющего центра

• сертификат на средство электронной подписи издателя

• сертификат на средство удостоверяющего центра

• класс защищенности, которому соответствуют программные средства УЦ,

• место хранения контейнеров ключа ЭП и ключа защиты УКЦ

После перевода УКЦ в аккредитованный режим необходимо выпустить:

• Корневой квалифицированный сертификат.

• Квалифицированную электронную подпись для пользователя

• Квалифицированную электронную подпись для пользователя

Эти шаги делаются под «Задача 1.7. Настройка работы удостоверяющего центра в аккредитованном режиме», их можно сделать сразу же при инициализации УКЦ, не расходуя лишнего времени.

Ставим автоматический режим работы, жмем «Далее».

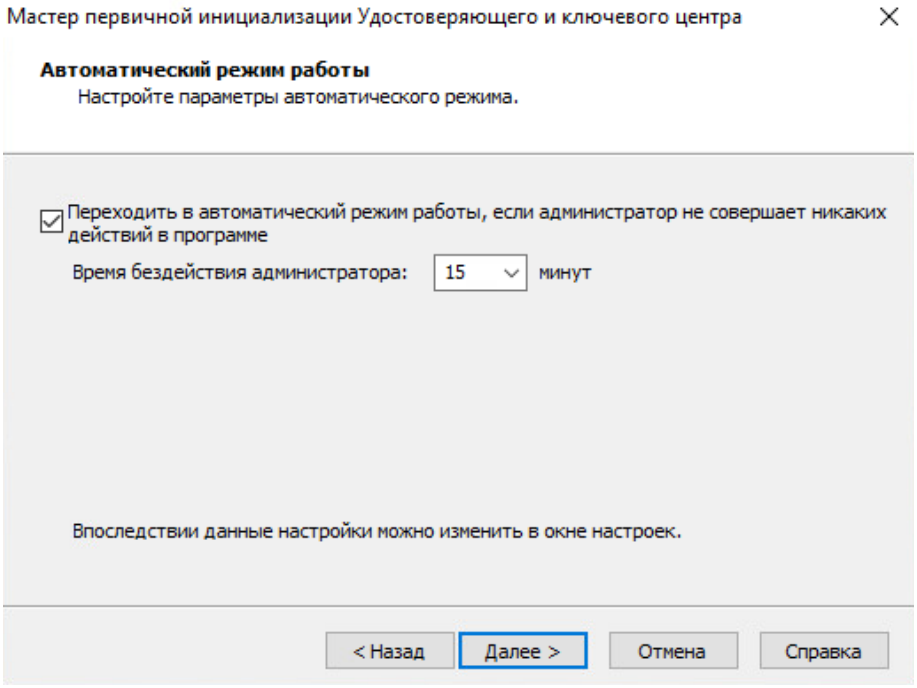

Рисунок 35 – Автоматический режим работы.

Указываем тип создаваемого пароля «Собственный пароль», нажимаем «Далее».

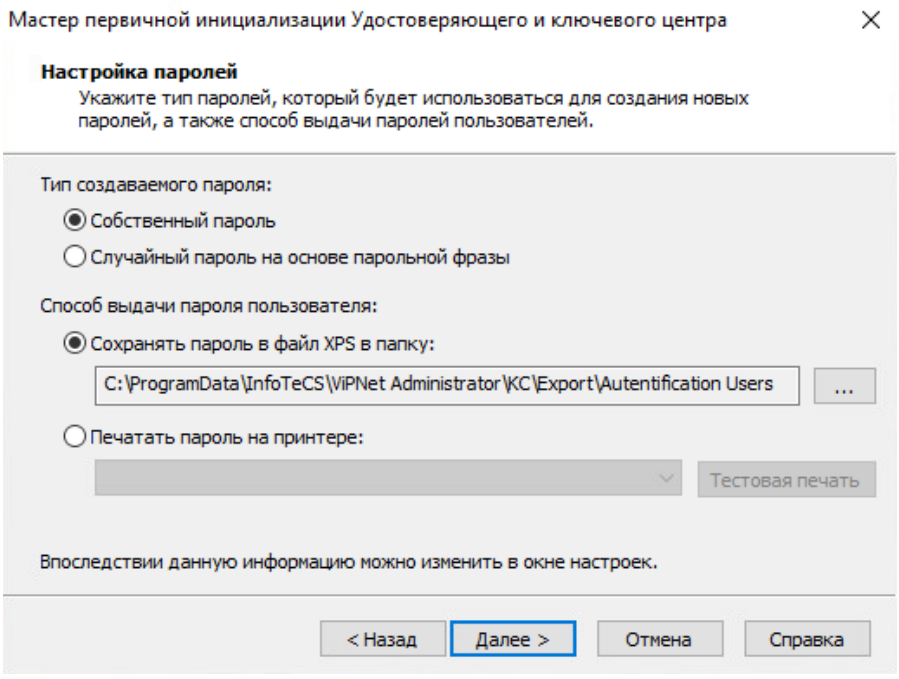

Рисунок 36 – Настройка паролей

Вводим пароль и подтверждаем его. Жмем «Далее»→»Далее».

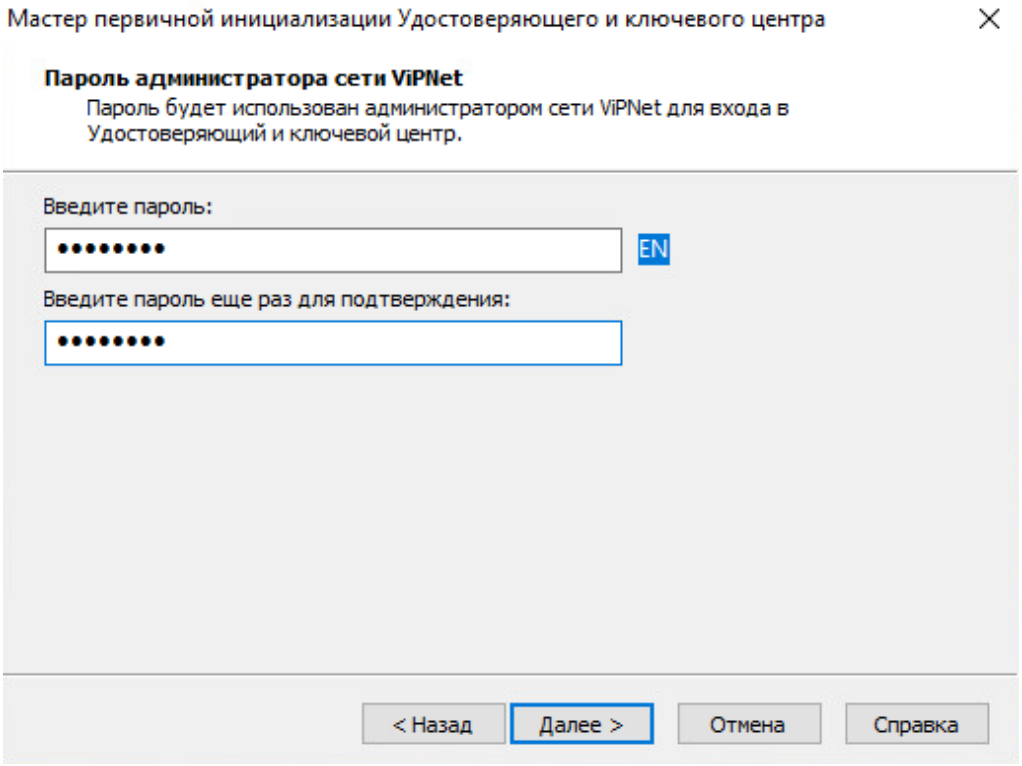

Рисунок 37 – Пароль администратора ViPNet

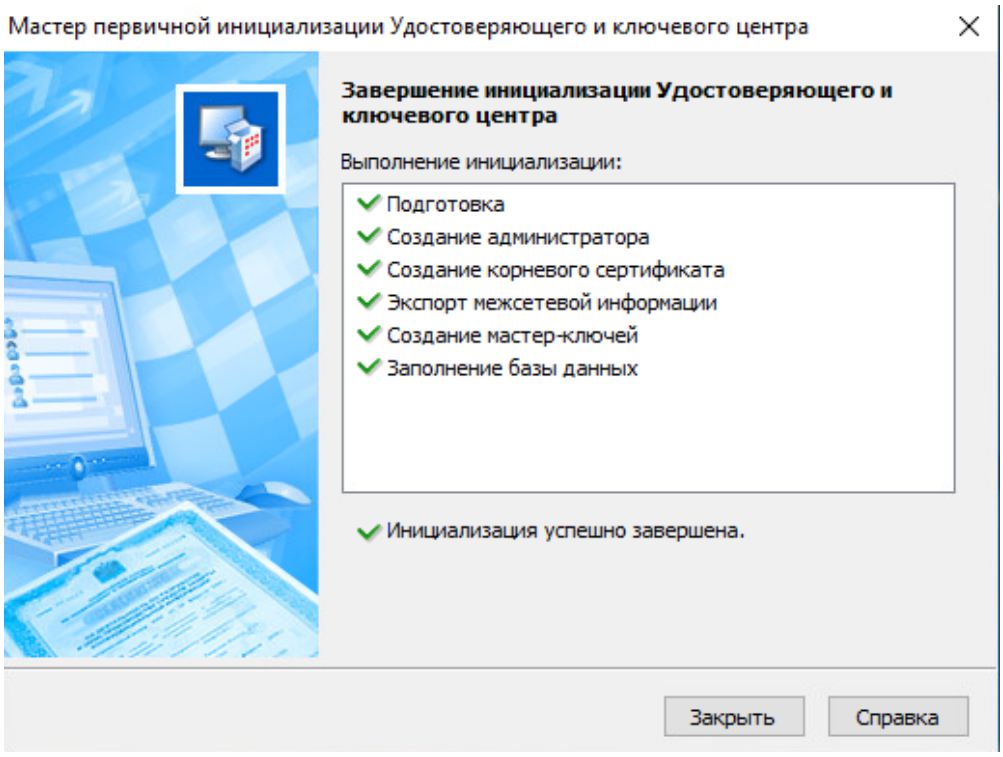

Рисунок 38 – Инициализация успешно завершена

Создаем структуру ЦУС на ВМ Net1-Open.

Начнем с координаторов. В левой панели заходим в «Координаторы», кликаем на зеленый квадрат «Новый координатор». Указываем имя, оставляем режим работы «Выполняет функции VPN-сервера». Нажимаем «Создать».

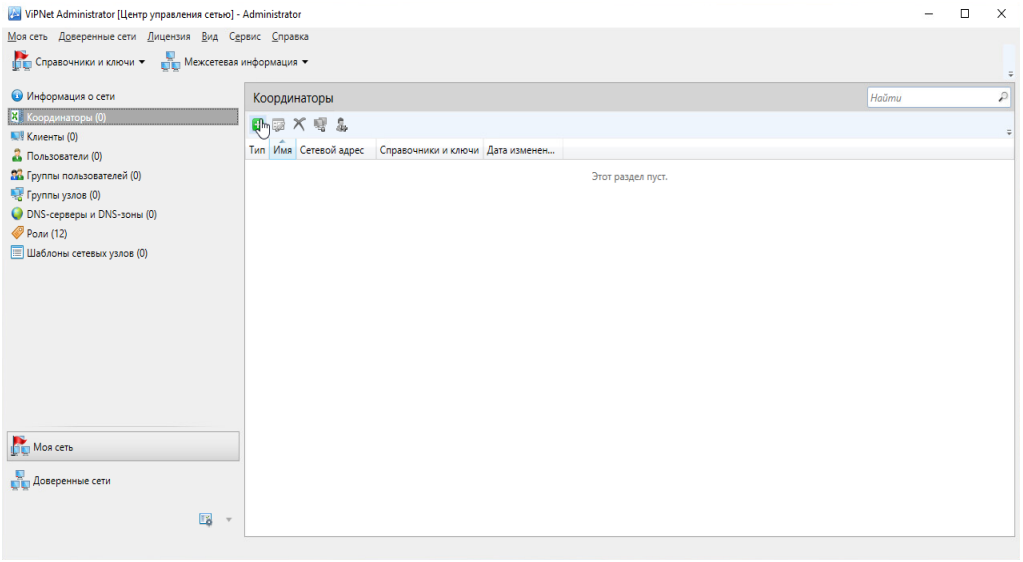

Рисунок 39 – Создание координатора

Кликаем ПКМ по созданному координатору и выбираем «Свойства», находим «Роли узла». Далее выбираем все существующие роли и удаляем их, нажав кнопку «Удалить».

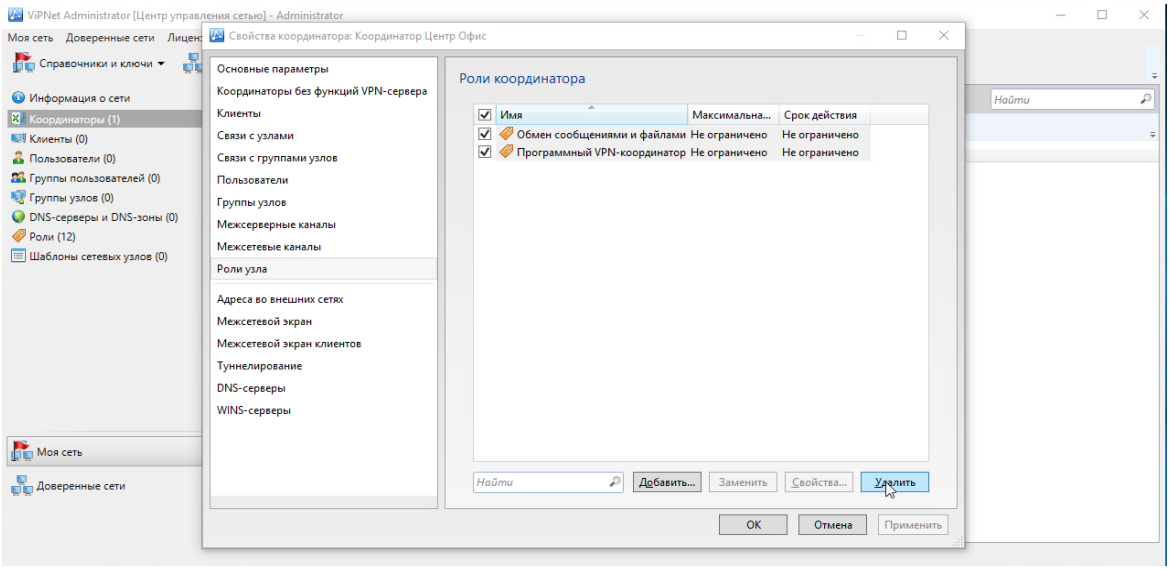

Рисунок 40 – Роли координатора ч.1

Нажимаем «Добавить» и выбираем из перечисленного роль «Coordinator HW-VA», затем повторно нажимаем «Добавить».

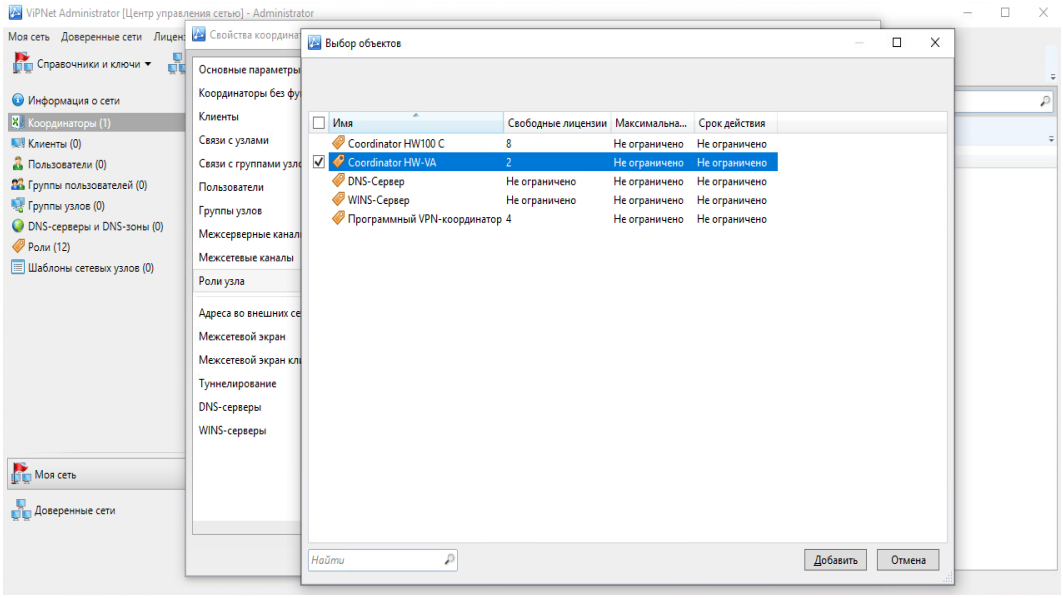

Рисунок 41 – Роли координатора ч.2

Создаем требующее кол-во координаторов. Далее требуется создать между координаторами межсерверный канал для взаимодействия двух сетей.

Заходим в свойства координатора и ищем «Межсерверные каналы». Добавляем нужный нам координатор для образования межсерверного канала.

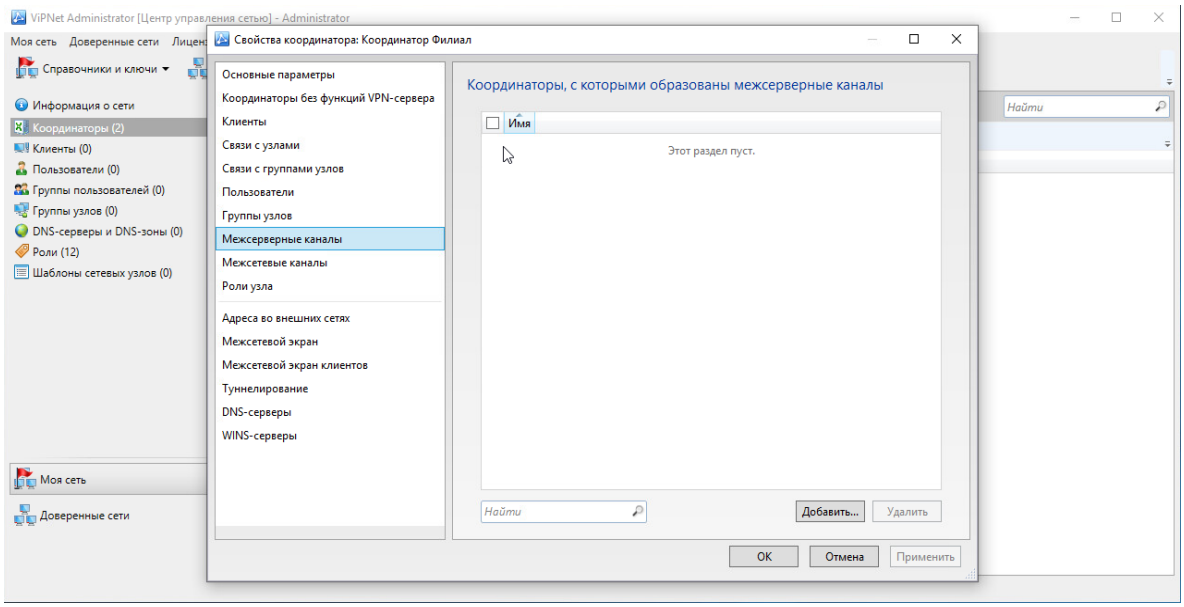

Рисунок 42 – Добавление межсерверного канала ч.1

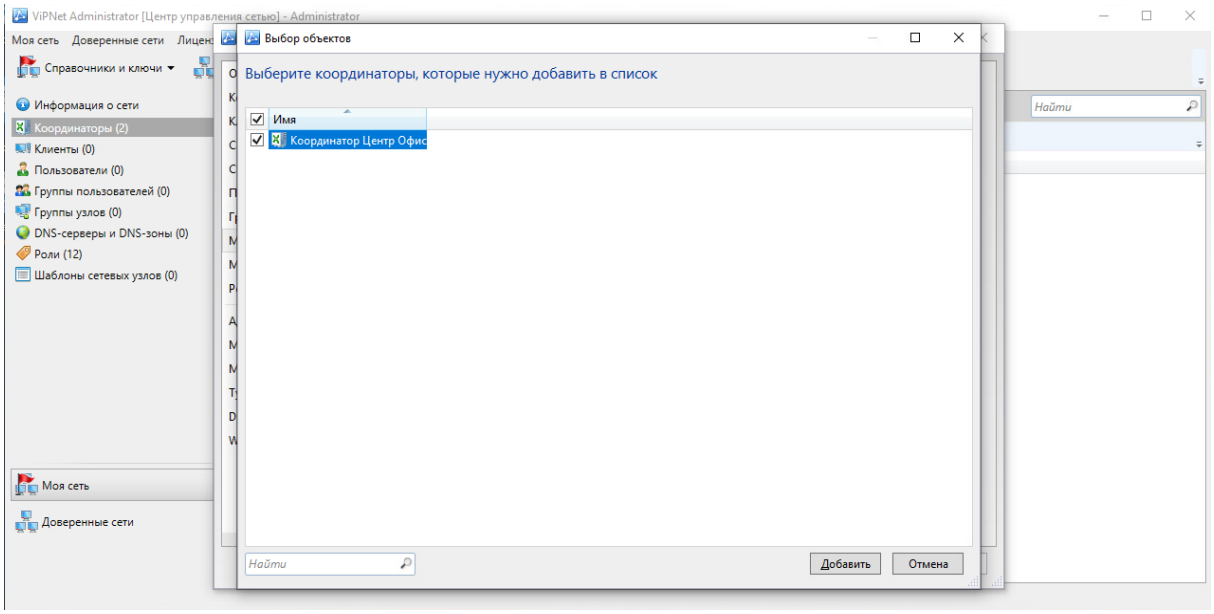

Рисунок 43 – Добавление межсерверного канала ч.2

Переходим в «Клиенты»→«Создать новый сетевой узел». Вводим имя, нажимаем «Выбрать» для выбора координатора, соответствующего по схеме. После выбора координатора нажимаем «Создать». Создаем другие клиенты, не забываем установить роль «Registration Point» на сетевой узел OperCA.

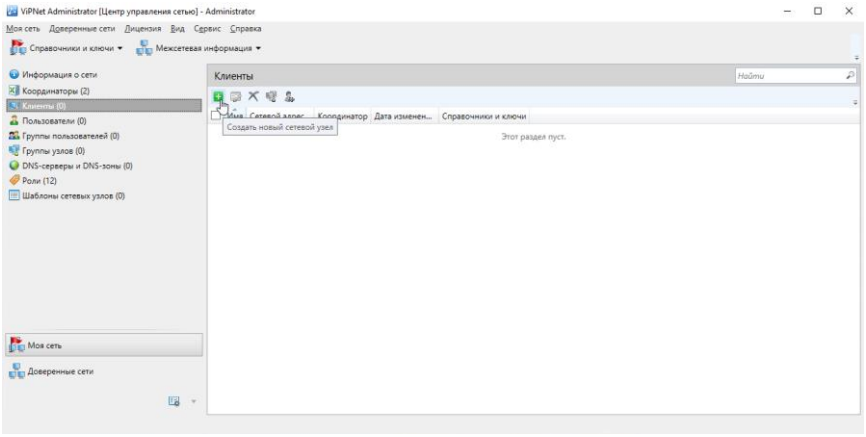

Рисунок 44 – Создание клиента ч.1

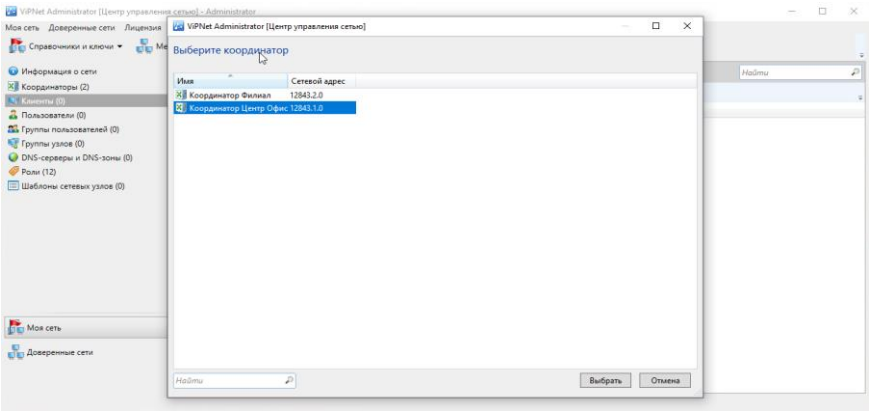

Рисунок 45 – Создание клиента ч.2

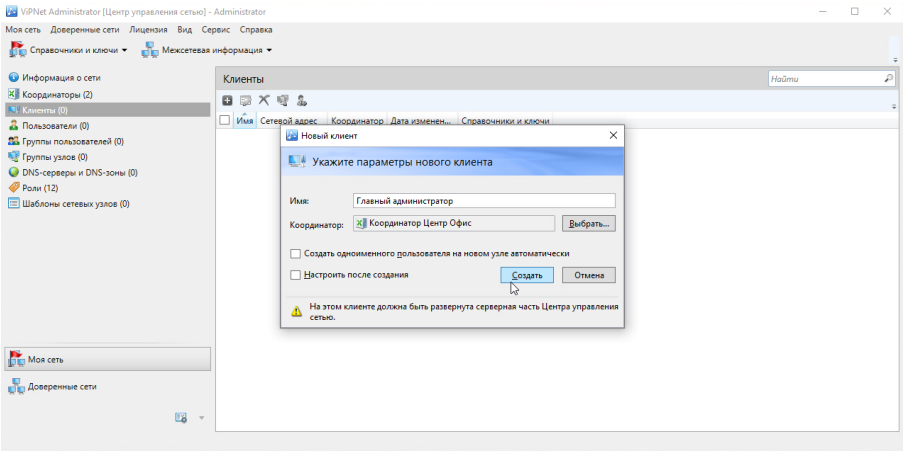

Рисунок 46 – Создание клиента ч.3

Теперь нам нужно создать пользователей для наших координаторов и клиентов. Этого не требуется, если мы не убирали галочку с пункта «Создать одноименного пользователя на новом узле автоматически».

Переходим в «Пользователи»→«Создать нового пользователя». Выбираем сетевой узел для нашего пользователя и нажимаем «Выбрать» → «Создать». Создаем для всех сетевых узлов.

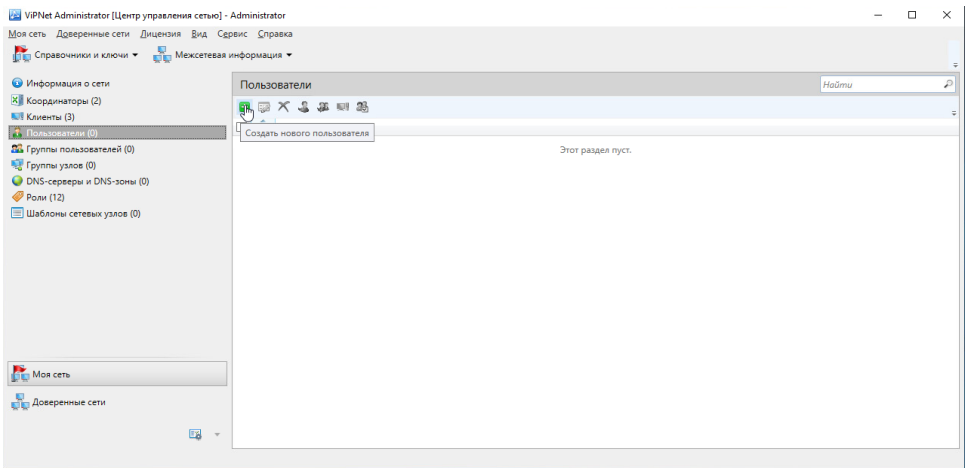

Рисунок 47 – Создание нового пользователя ч.1

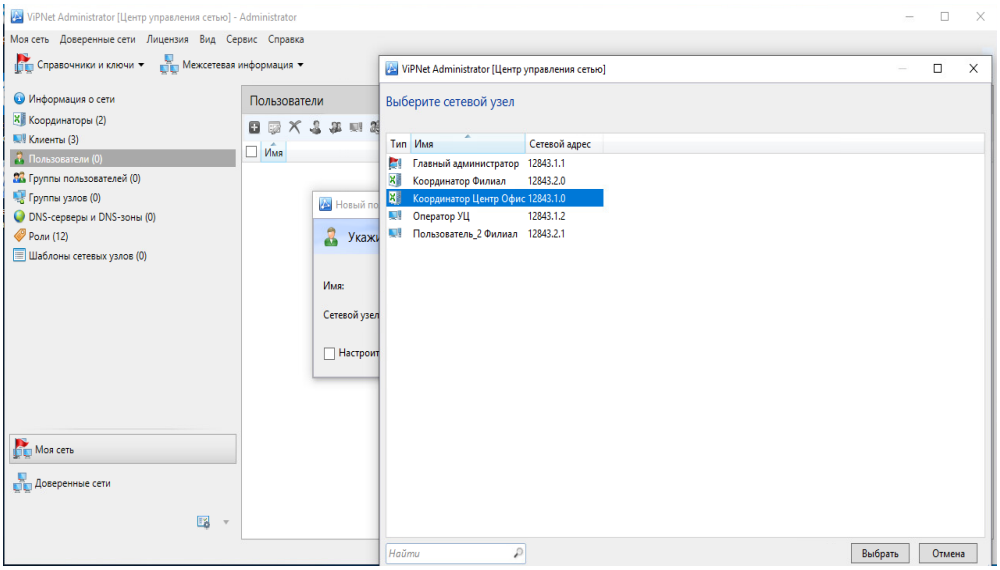

Рисунок 48 – Создание нового пользователя ч.2

Остается настроить связи между пользователями, ищем в заданиях табличку. Для установления связи нажимаем на пользователя ПКМ «Свойства» → «Связи с пользователями». Нажимаем «Добавить», смотрим внимательно на табличку и выбираем нужных нам пользователей.

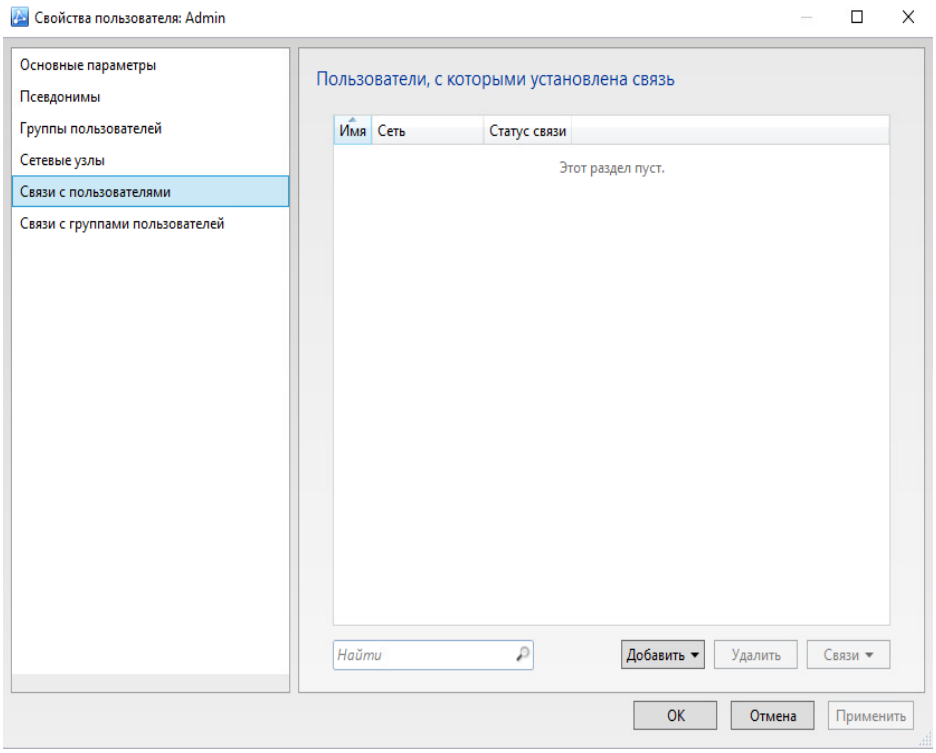

Рисунок 49 – Связи с пользователями

По заданию может потребоваться выгрузка HTML нашей созданной структуры. Нажимаем «Моя сеть» → «Сохранить отчет о структуре сети в файл» и выбираем формат HTML.

Создание структуры ЦУС завершено, нам потребуются справочники для наших сетевых узлов. Нажимаем «Моя сеть» → «Создать справочники» → «Создать для всего списка».

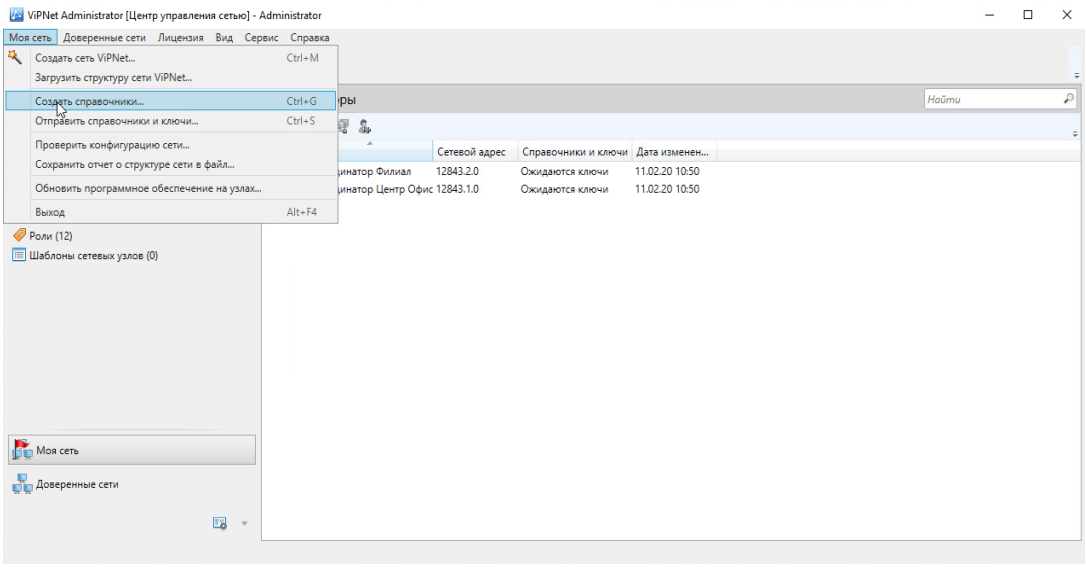

Рисунок 50 – Создание справочников ч.1

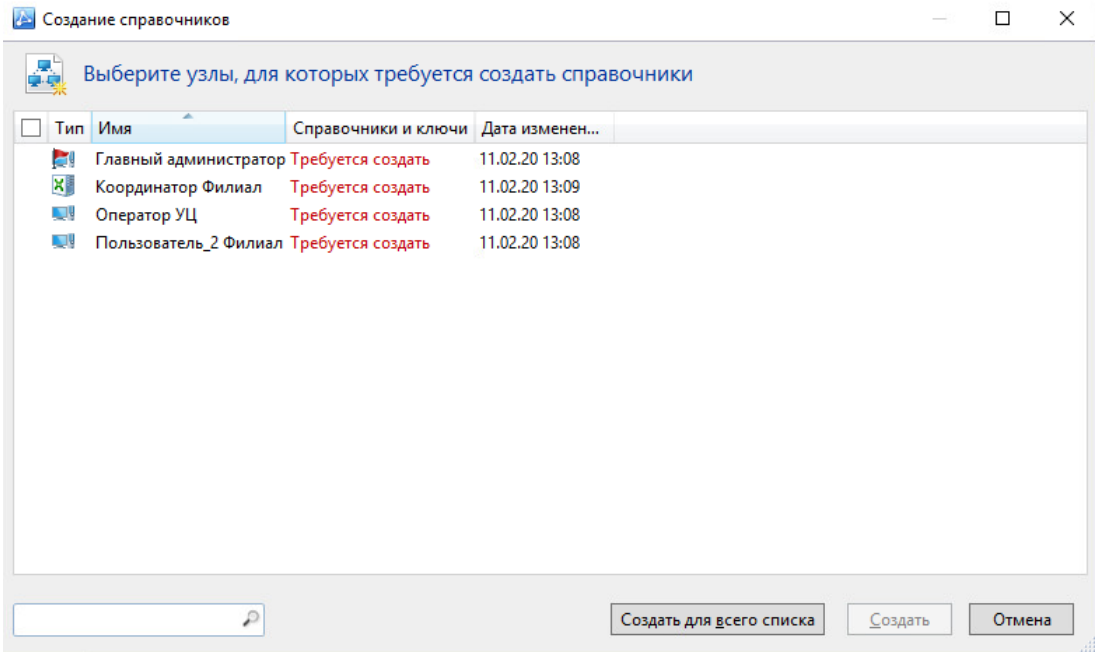

Рисунок 51 – Создание справочников ч.2

Заходим в УКЦ.

В УКЦ переходим в «Сетевые узлы», выделяем все сетевые узлы и нажимаем ПКМ → «Выдать новый дистрибутив ключей». Задаем пароль каждому сетевого узлу и подтверждаем его. Повторно вводить сведения о сертификате не нужно, если при инициализации УКЦ вы их уже указали, они автоматически заполняться.

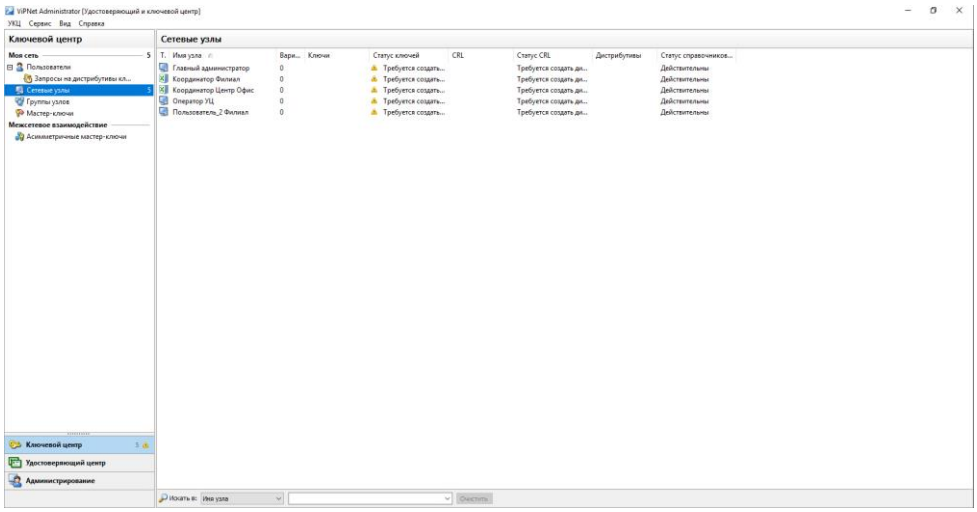

Рисунок 52 – Выдача дистрибутива ключей ч.1

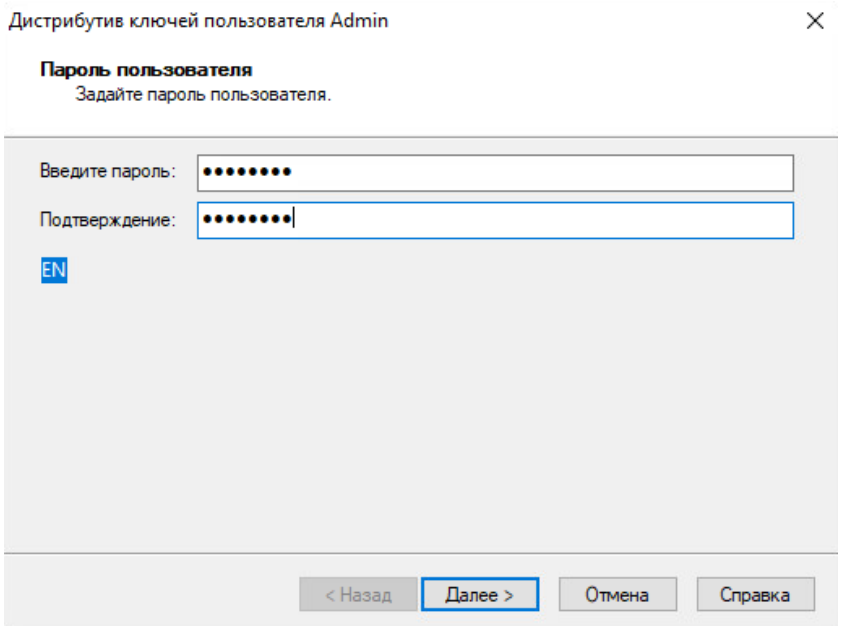

Рисунок 53 – Выдача дистрибутива ключей ч.2

Теперь на всех клиентах (в том числе и координаторах) мы сможем провести первичную инициализацию, требуемую по заданию. Переходим к нашему забытому координатору.

Оставляем по умолчанию «usb», нажимаем «Next». Убеждаемся, что флешка присоединена к нашей ВМ и нажимаем «Next».

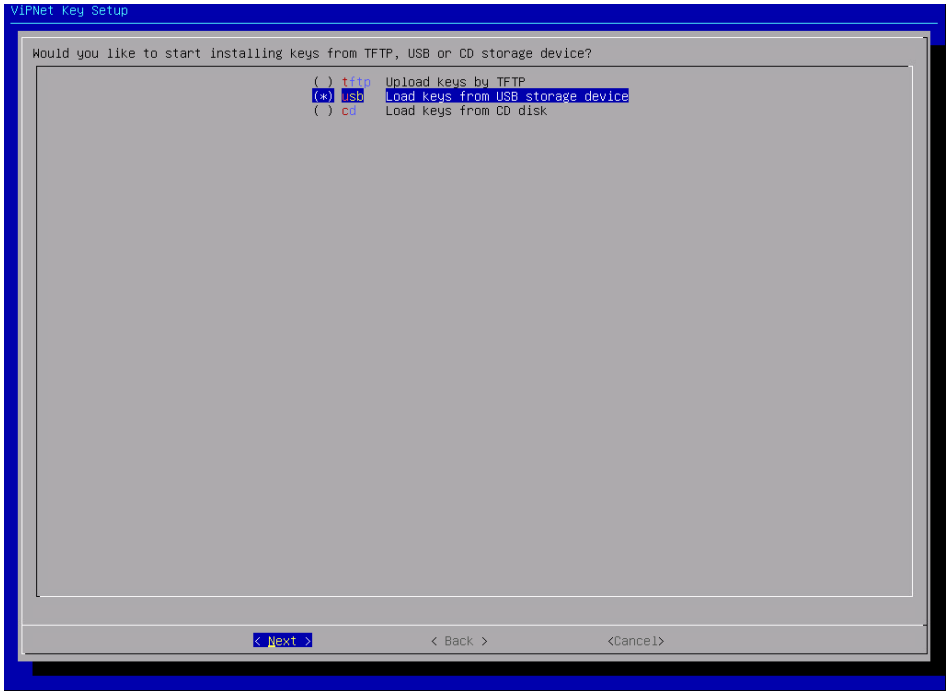

Рисунок 54 – Первичная инициализация (Coordinator HW-VA) ч.1

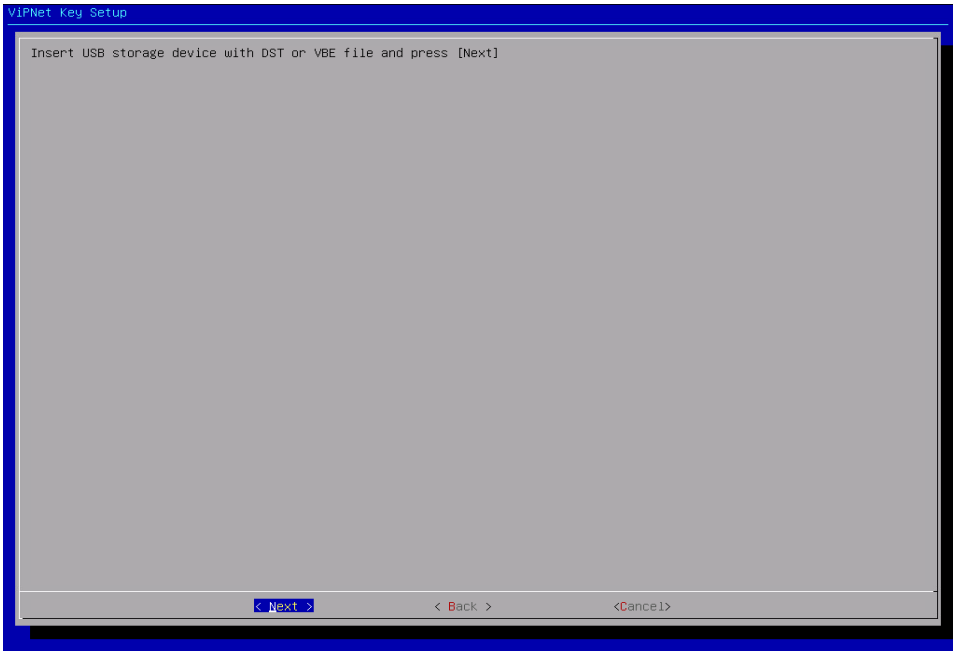

Рисунок 55 – Первичная инициализация (Coordinator HW-VA) ч.2

Внимательно смотрим и находим наш дистрибутив ключей, нажимаем «Next». Вводим пароль → «Next». Далее идет настройка сетевых интерфейсов. Поднимаем все используемые (Net1 и интернет), выбирая «UP», на других оставляем «DOWN». Между «DHCP» и «Static IP» выбираем «Static IP». Задаем Ip-адреса, маски, согласно вашим сведениям. Шлюз для интернета указываем ip-адрес второго координатора.

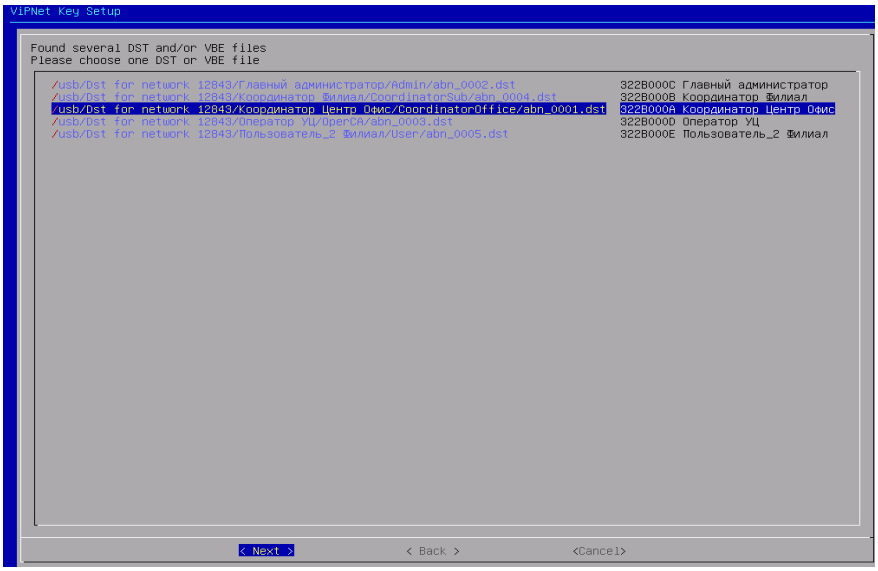

Рисунок 56 – Первичная инициализация (Coordinator HW-VA) ч.3

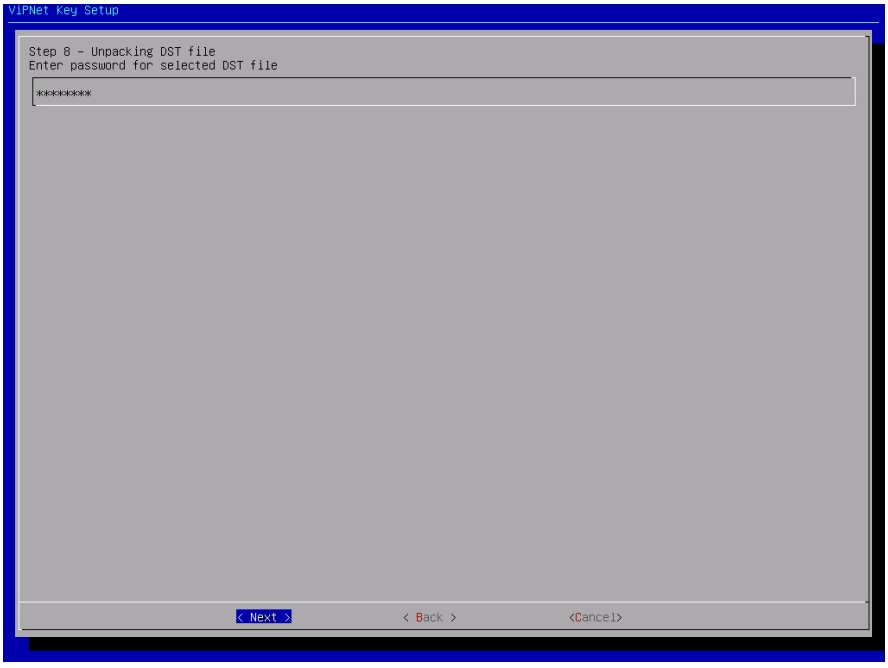

Рисунок 57 – Первичная инициализация (Coordinator HW-VA) ч.4

Большинство из функций по типу DNS-сервера и NTP нам не понадобятся, везде оставляем «OFF» и «No». Добираем до окончания, где нас спрашивают про старт VPN служб, нажимаем «Yes» → «Finish».

Рисунок 58 - Первичная инициализация (Coordinator HW-VA) ч.5

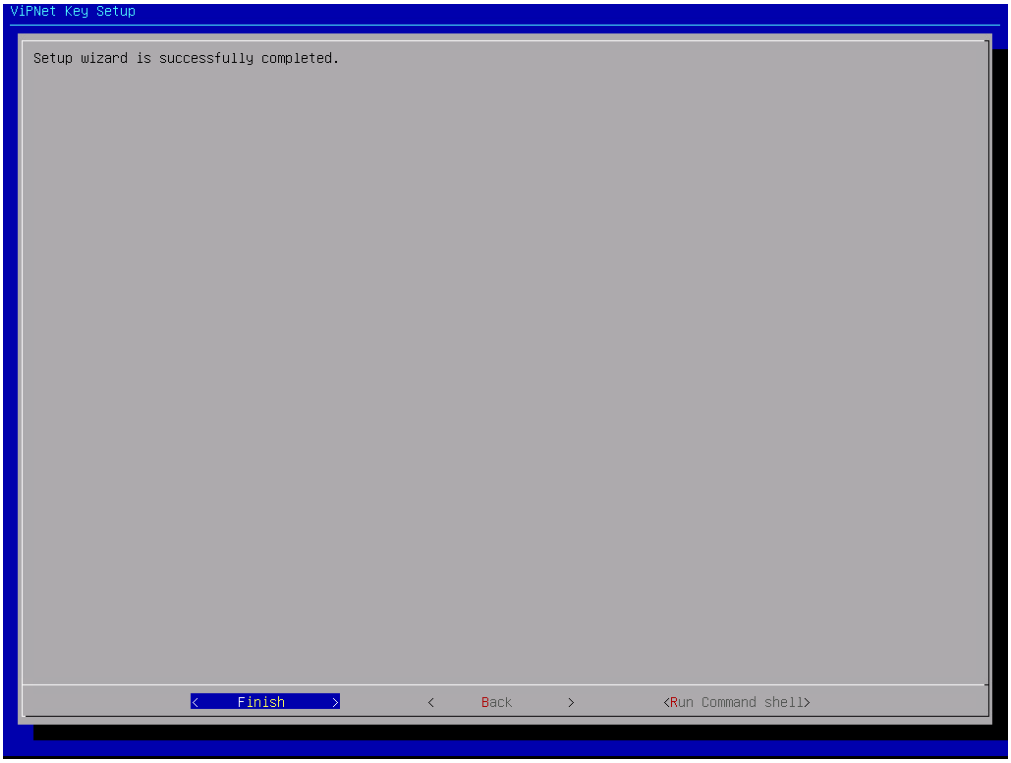

Рисунок 58 - Первичная инициализация (Coordinator HW-VA) ч.6

Первичная инициализация клиентов проходит быстро и не так долго, открываем установленную программу ViPNet Client. Нажимаем в открывшемся окне «Настройка» → «Установить ключи». Присоединяем флешку с дистрибутивом ключей к нашей ВМ. Указываем путь и нажимаем «Установить». Ключи должны быть успешно установлены.

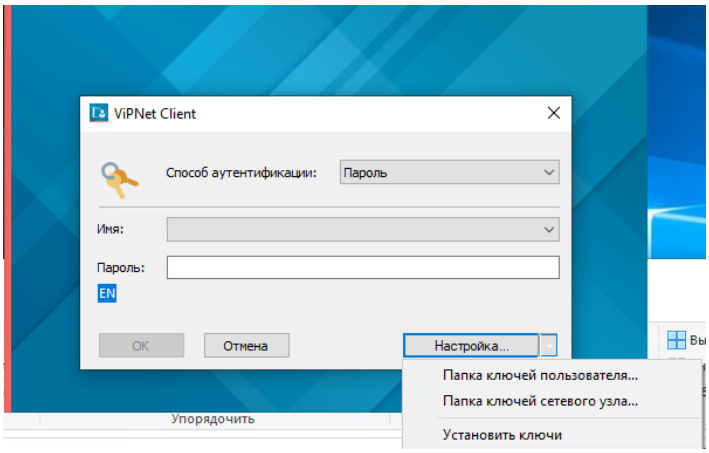

Рисунок 59 – Первичная инициализация (ViPNet Client) ч.1

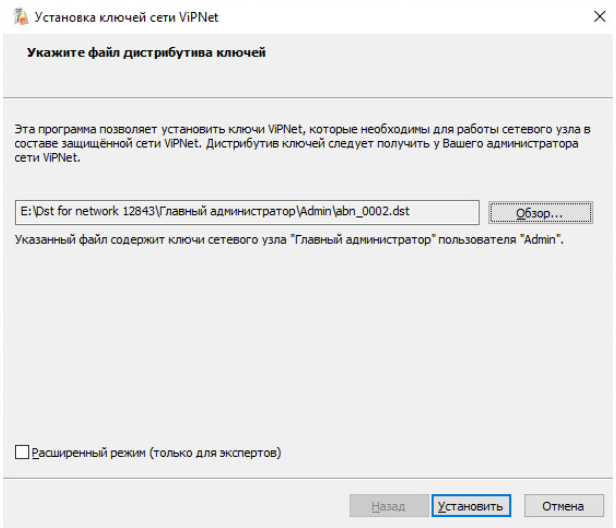

Рисунок 60 – Первичная инициализация (ViPNet Client) ч.2

БОЛЬШЕ дистрибутивы ключей не выдаем (кроме определенных задач, где это потребуется). Когда с нас потребуют ключи, в том же меню вместо выдачи дистрибутива ключей выбираем «Создать и передать ключи в ЦУС», а уже потом в ЦУСе в меню выбираем «Отправить справочники и ключи».

ВАЖНО!!! После того, как вы установили ViPNet Client на ВМ с серверным ЦУС, вам нужно будет разрешить подключение к БД, т.к. клиент блокирует все входящие и исходящие подключения. Делается это в самом клиенте. Заходим в «Сетевые фильтры» → «Фильтры открытой сети», нажимаем «Создать». Ставим у пункта «Действие» : «Пропускать трафик» → «ОК». Не забываем нажать «Применить». Теперь все должно работать как надо.

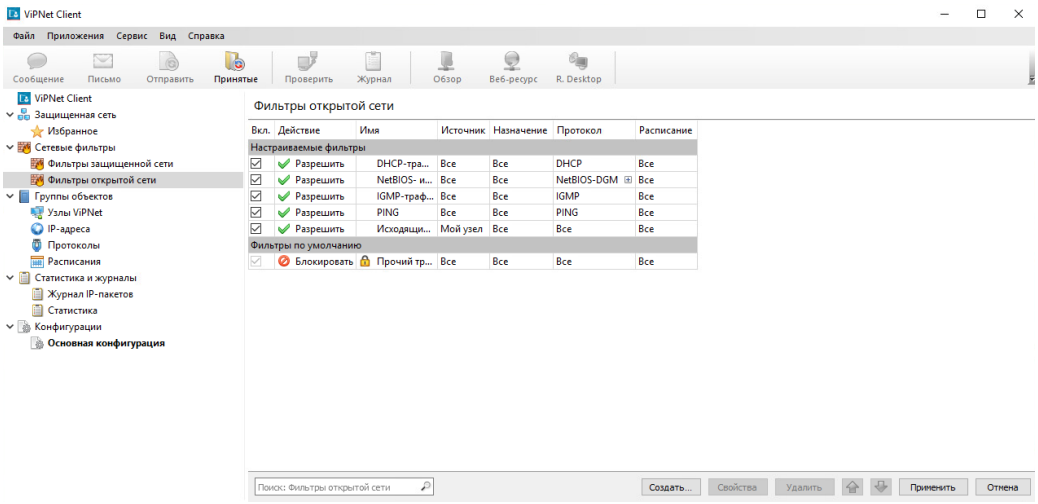

Рисунок 61 – Фильтры открытой сети ч.1

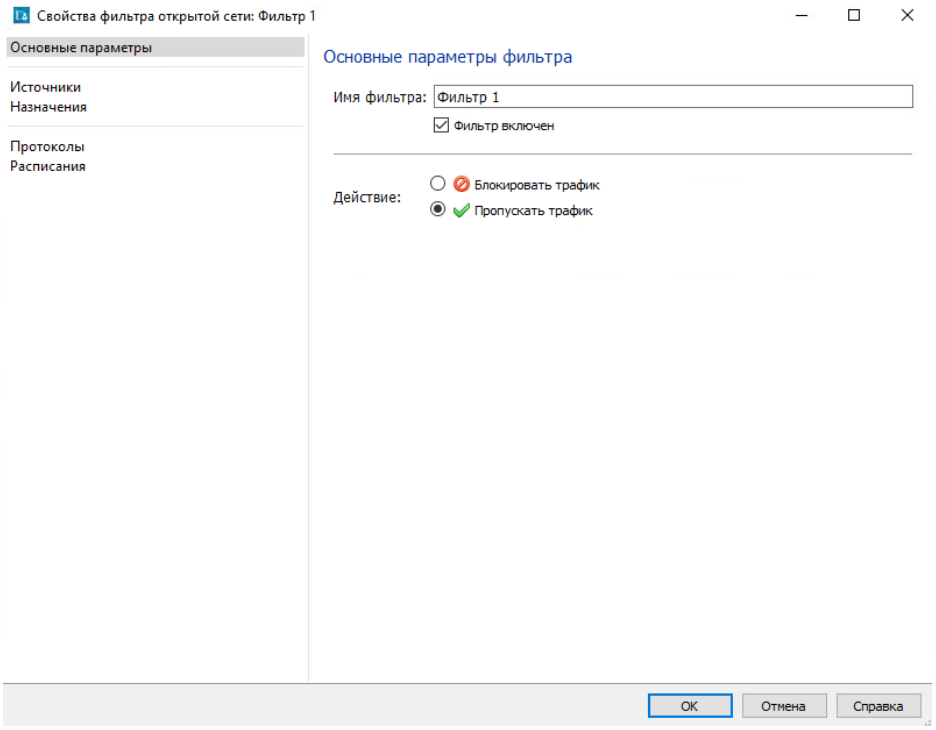

Рисунок 62 – Фильтры открытой сети ч.2

Выполняем оставшиеся задания, а именно:

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети. Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service).

Реализовать автоматическую публикацию сертификатов.

Посредством Центра Регистрации (Registration Point):

1. зарегистрировать пользователя;

2. отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос;

3. отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос.

Посредством Сервиса Информирования (CA Informing):

4. настроить способ выдачи уведомлений;

5. сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов

К сожалению, к написанию методички лицензии включающую роль Publication Service у меня нет.

Registration Point на ВМ с установленными ViPNet программами работает не совсем некорректно, при установке ключей придется потрудиться и почитать другие документации. Если же вы решитесь делать, то:

Заходим в установленный клиент, используем дистрибутив ключей сетевого узла OperCA на котором стоит роль «Registration Point». В окне выбора выбираем «ViPNet Registration Point». При появлении ошибки следует изменить каталог, кликаем на значок рядом с «Настройки», выбираем пункт «Папка ключей сетевого узла» и меняем на путь к идентификатору узла C:\ProgramData\Infotecs\<идентификатор сетевого узла >

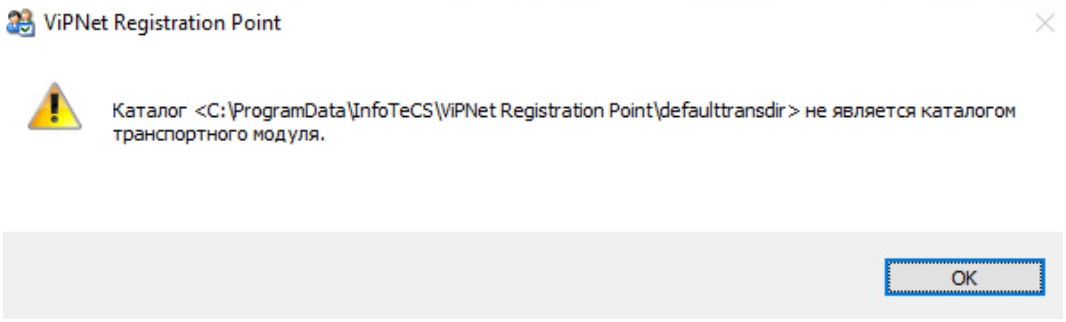

Рисунок 63 – Ошибка ViPNet Registration Point

Ошибка должна пропасть, а окно с программой открыться.

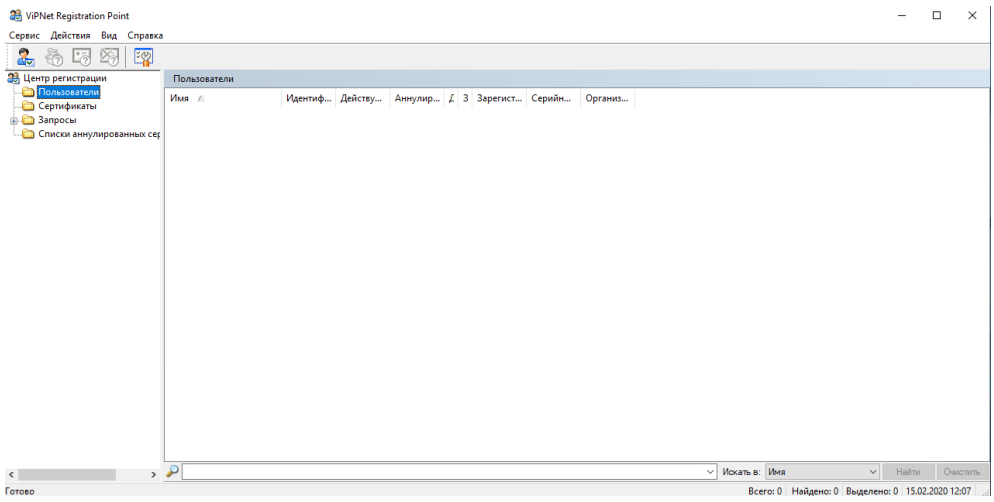

Рисунок 64 – ViPNet Registration Point

Нажимаем в левом углу «Зарегистрировать пользователя». После регистрации нажимаем на нашего пользователя ПКМ «Сертификаты» → «Создать запрос». После создания запроса переходим в «Запросы» → «Запросы на сертификаты» → «Отправленные». Находим наш сертификат, нажимаем дважды ЛКМ и заходим в «Статус».

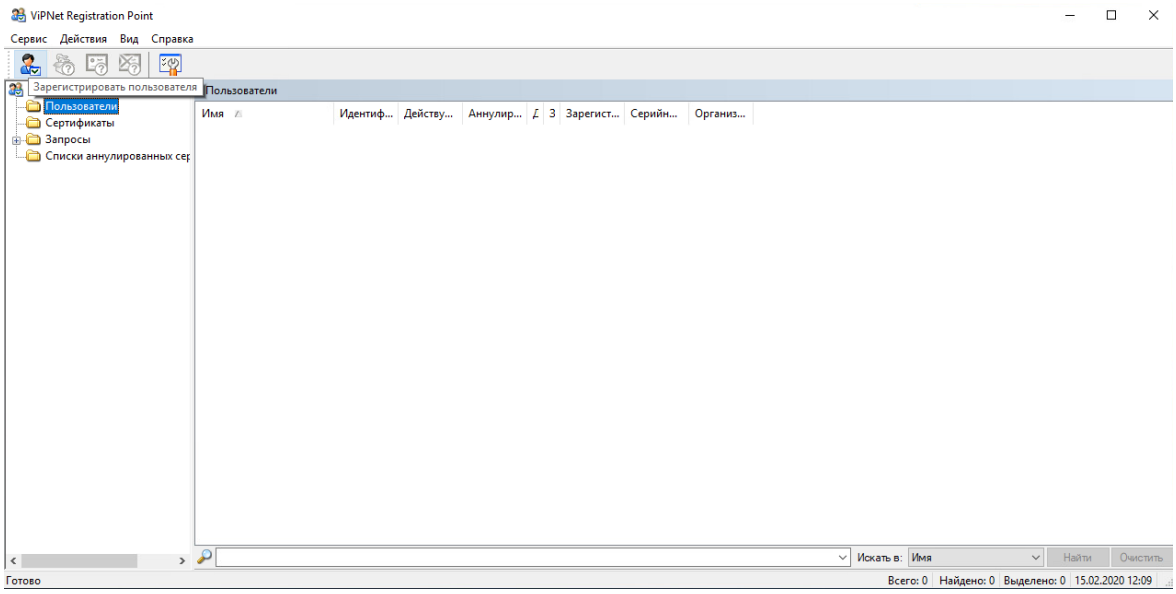

Рисунок 65 – Регистрация пользователя

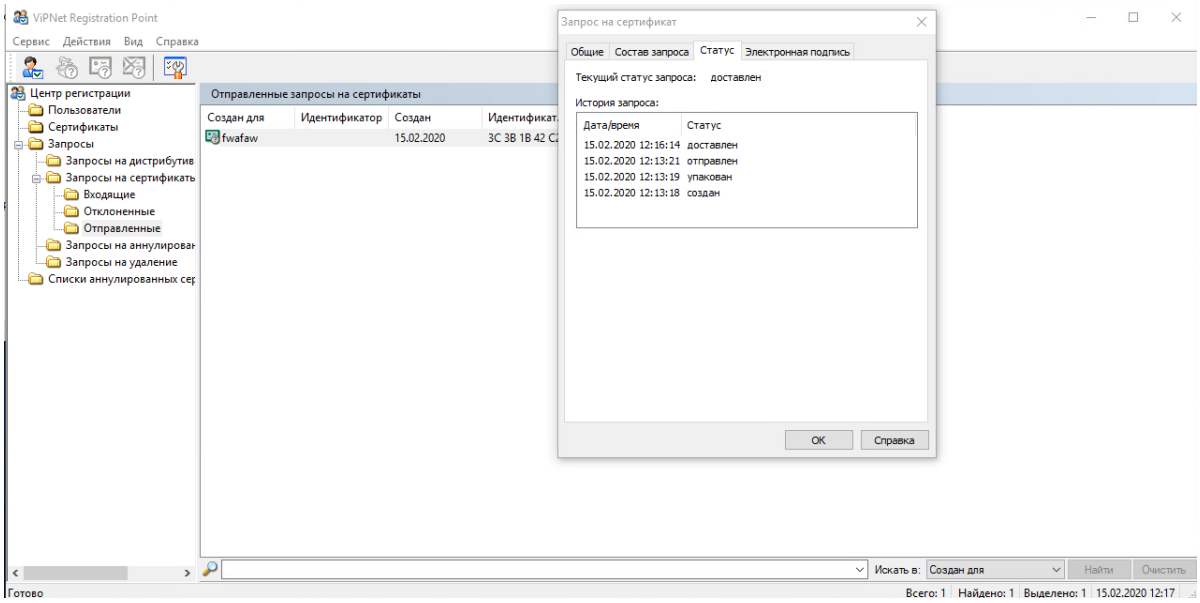

Рисунок 66 – Запрос на сертификат

Следим за нашим статусом, после того как статус станет «доставлен» переходим в УКЦ и удовлетворяем запрос. Тыкаем на сертификат и нажимаем «Удовлетворить» → «Да».

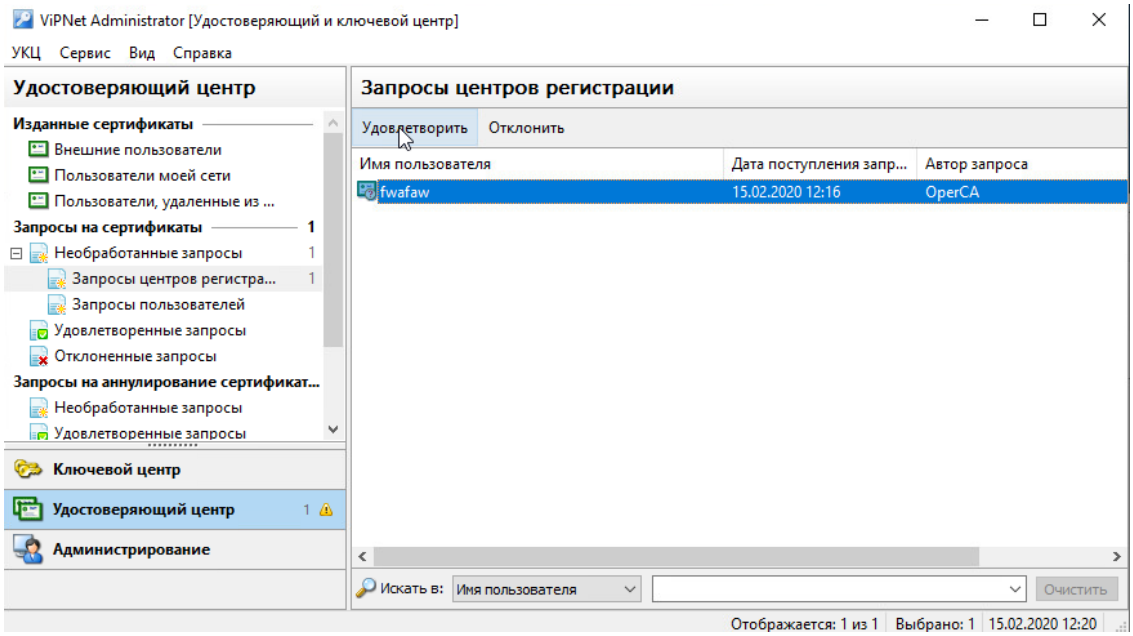

Рисунок 67 – Удовлетворение сертификата

Ожидаем некоторое время, когда наш сертификат станет действующим в ViPNet Registration Point. После чего, аннулируем наш действующий сертификат. Переходим в «Сертификаты», находим наш сертификат, ПКМ «Аннулировать» → «Да». Переходим в «Запросы на аннулирование» и следим.

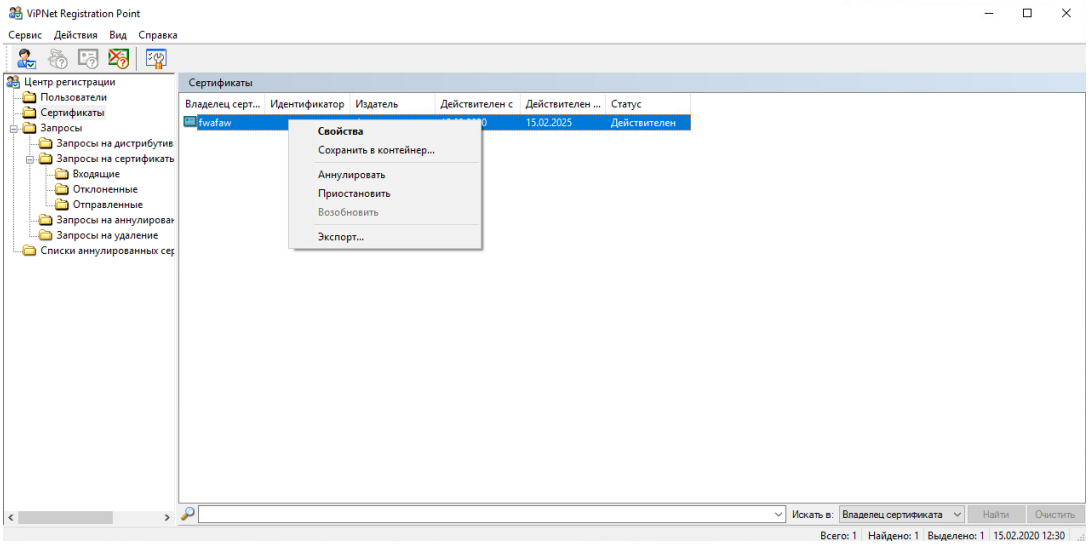

Рисунок 68 – Запрос на аннулирование сертификата

В УКЦ заходим в «Запросы на аннулирование сертификатов» → «Необработанные запросы». Выбираем наш сертификат и нажимаем «Удовлетворить» → «Да».

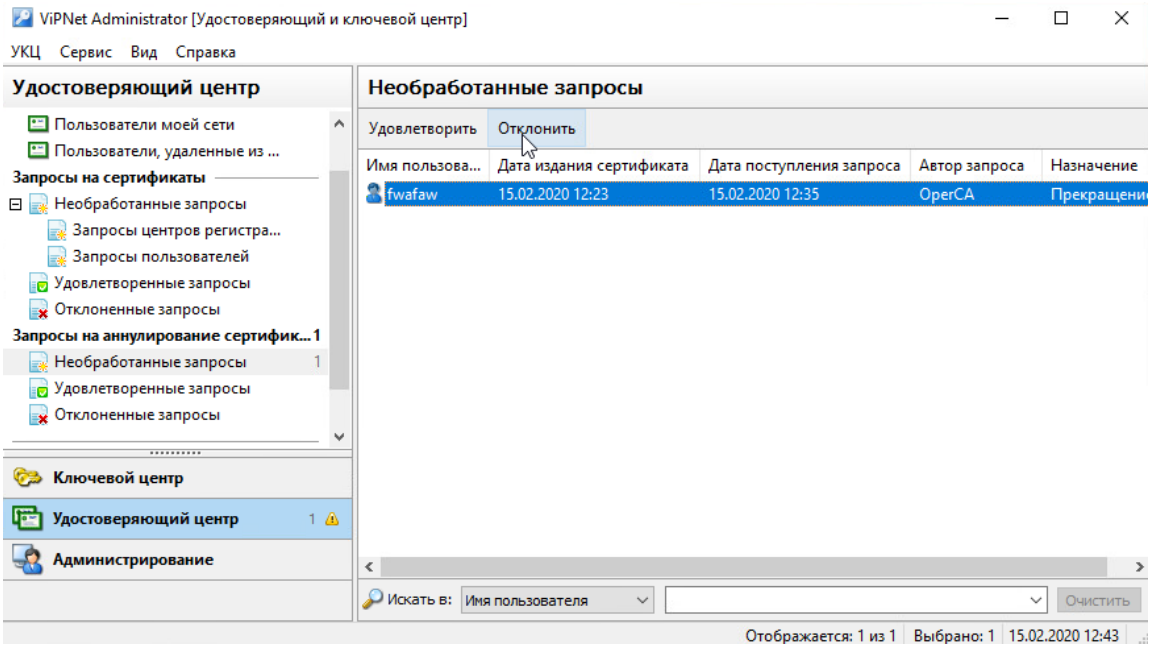

Рисунок 69 – Аннулирование сертификата.

Заходим в ранее установленный CA Informing на ВМ Net1-AdminCA.

Для начала настроим его, нажимаем «Действия» → «Настройки».

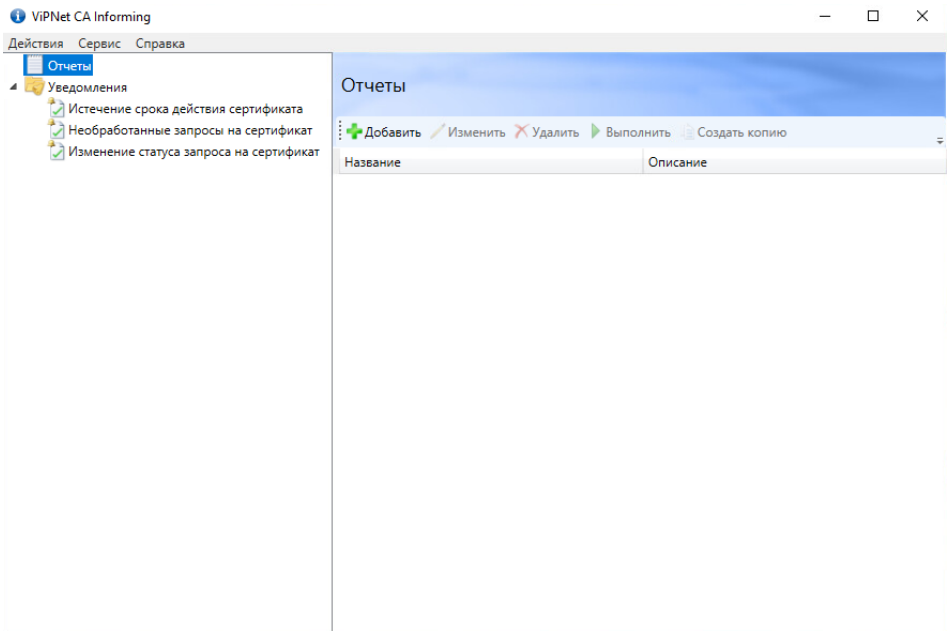

Рисунок 70 – CA Informing

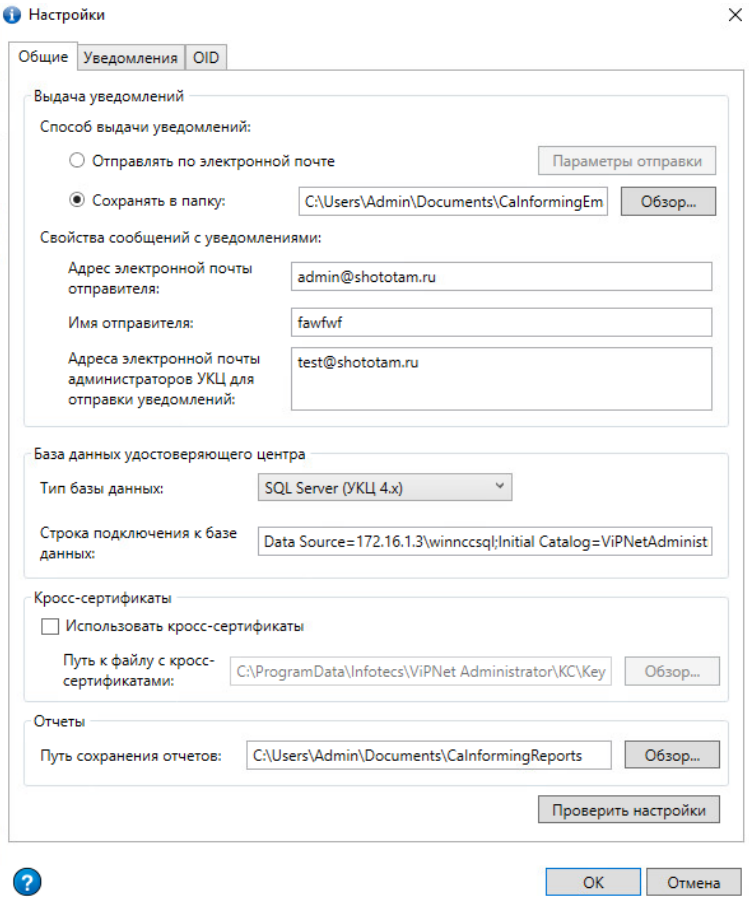

Рисунок 71 – Настройки CA Informing

Заполняем:

Сохранять в папку – C:\Users\Admin\Documents\CaInformingEmails Любой корректный адрес электронной почты отправителя: Имя: Любой корректный адрес электронной почты для отправки уведомлений: Строка подключения: Data Source=<ваш ip бд>\winnccsql;Initial Catalog=ViPNetAdministrator;User Id=sa;Password=xxXX1234; Путь сохранения отчетов: C:\Users\Admin\Documents\CaInformingReports

После заполнения нажимаем «ОК» и добавляем отчет. Нажимаем «Добавить» → «ОК».

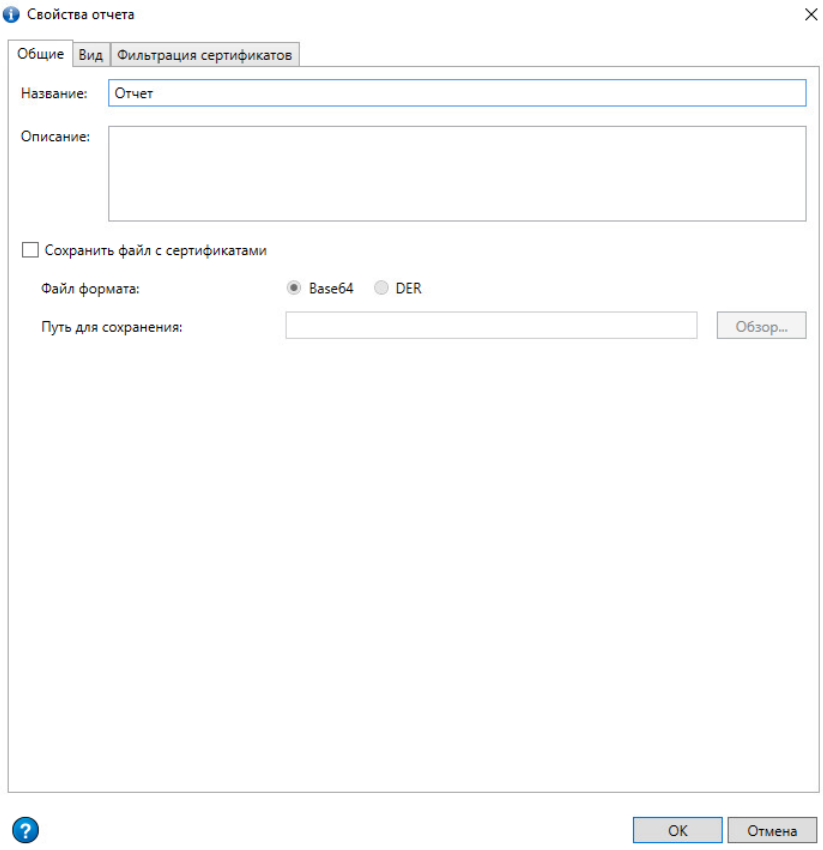

Рисунок 72 – Свойства отчетов ч.1

В задании могут попросить указать за какой-то промежуток времени, переходим в «Фильтрация сертификатов». Ставим галочки на «Начало» и «Окончание».

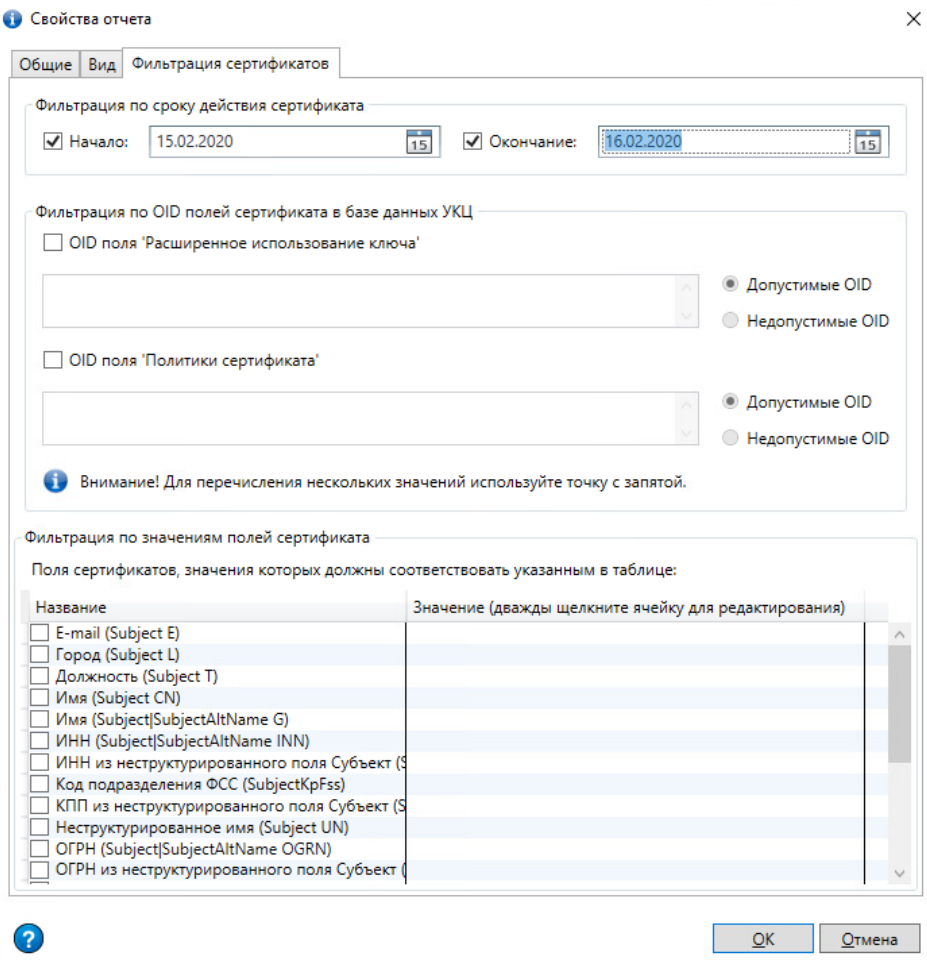

Рисунок 73 – Свойства отчета ч.2

Нажимаем «Выполнить».

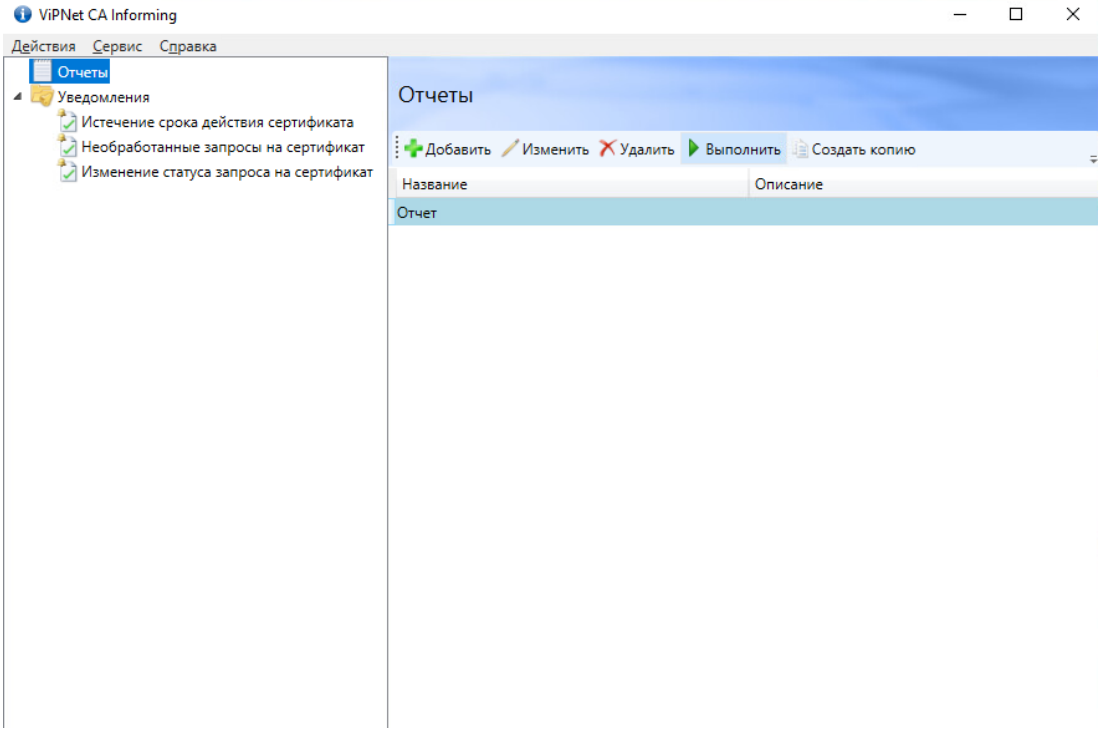

Рисунок 74 – Выполнение созданного отчета

Если в указанной нами папке для сохранения отчетов, появился сам отчет вместе с сертификатами, то задание выполнено успешно.

Задача 1.8. Модификация структуры защищенной сети

Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.

Модификация структуры сети:

1. добавить новый сетевой узел и пользователя за координатором (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем. На указанных узлах проверить появление нового узла;

2. Добавить пользователя на узле Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи;

3. отправить письмо по Деловой почте пользователю.

4. отправить текстовое сообщение пользователю

Необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

• скриншоты деловой почты на отправителе и получателе (при отправке письма);

• скриншоты текстового сообщения на отправителе и получателе;

• 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

Задача 1.8: Решение

ВАЖНО!!! При любом изменении структуры сети ЦУСу потребуются справочники, а также возможно и ключи. Ключи (не путать с дистрибутивами ключей) создаем в УКЦ и отправляем в ЦУС, после чего отправляем справочники вместе с ключами на узлы.

Создаем новый сетевой узел и пользователя точно также как и при создании самой структуры сети. Выдаем новый дистрибутив ключей для сетевого узла «Пользователь_2 Филиал», так как у нас нет дистрибутива для нашего нового пользователя.

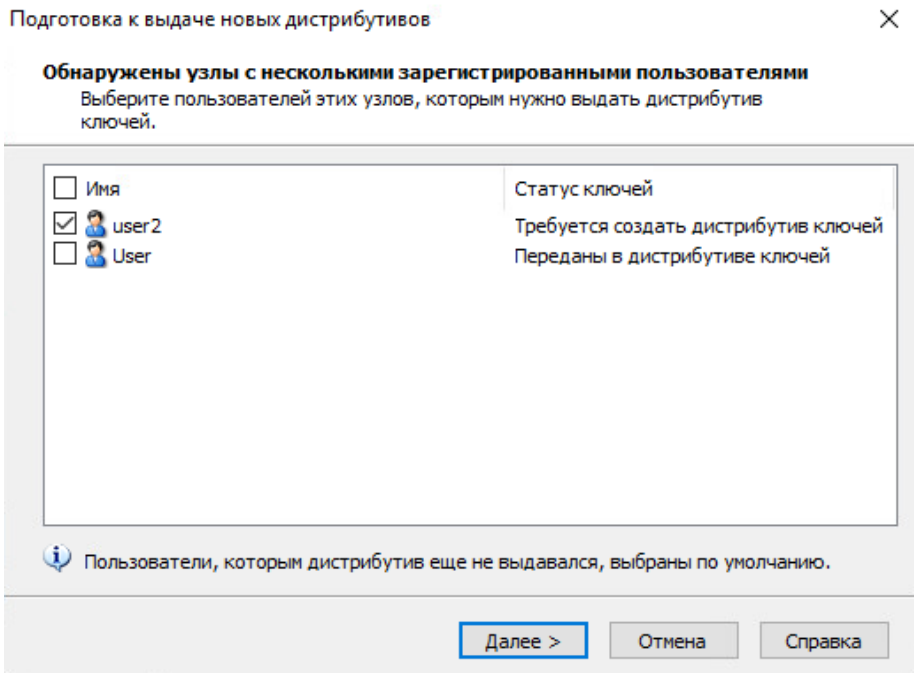

Рисунок 75 – Новый дистрибутив ключей

После выполнения заданий, потребуется проверить добавления пользователей и узлов.

Проверяем появление узла.

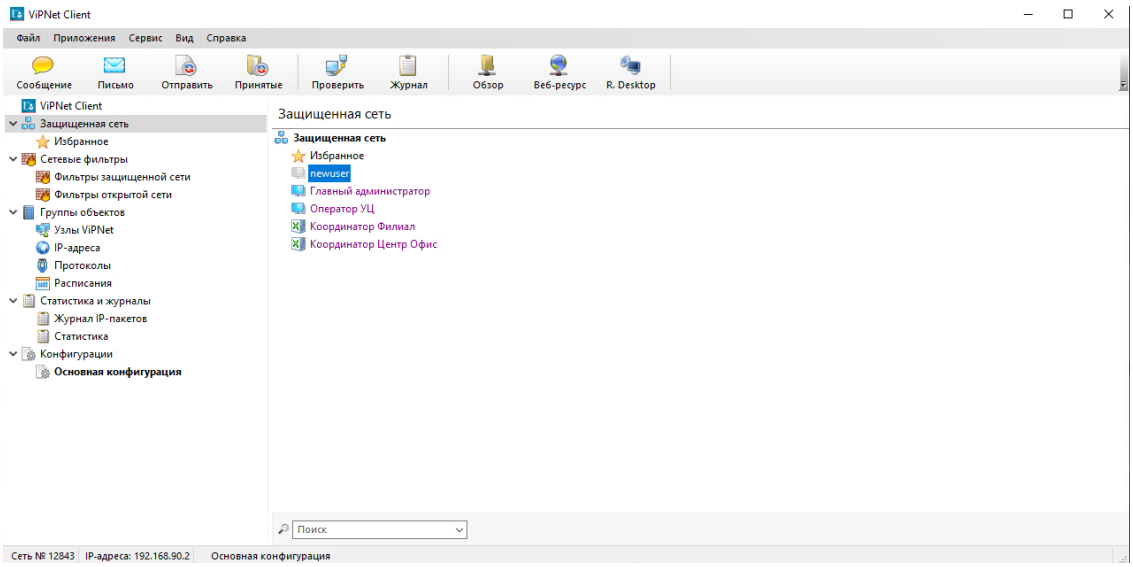

Рисунок 76 – Появление сетевого узла

Устанавливаем новые ключи для нашего созданного пользователя и заходим в ViPNet Client.

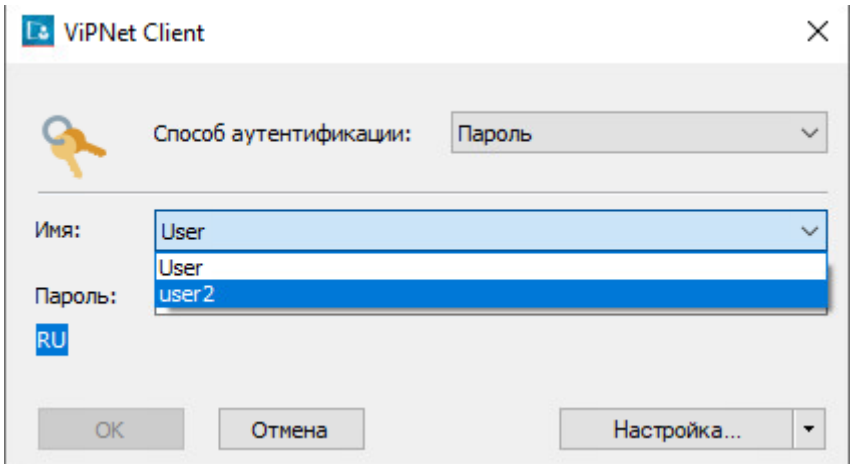

Рисунок 77 – Установка ключей

С любого сетевого узла заходим в деловую почту. Нажимаем «Создать новое письмо» → «Получатели». Дважды нажимаем по пользователю, которому хотим отправить письмо, после чего кликаем «ОК».

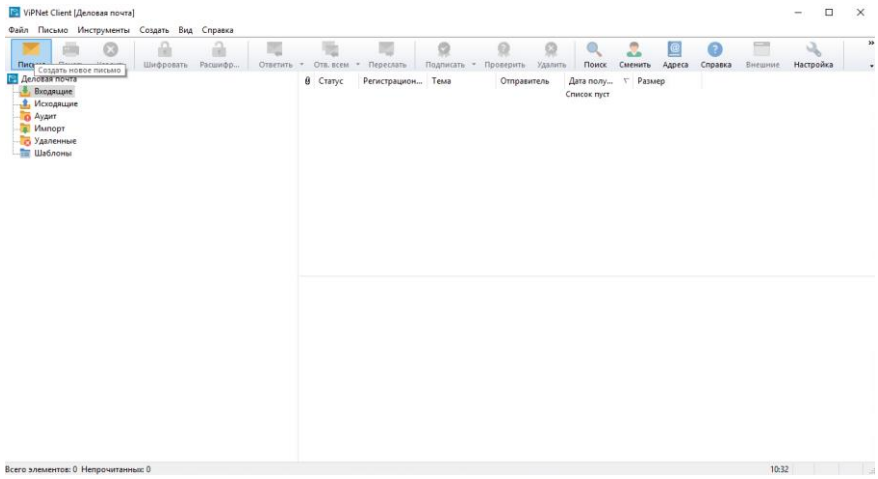

Рисунок 78 – Создание нового письма

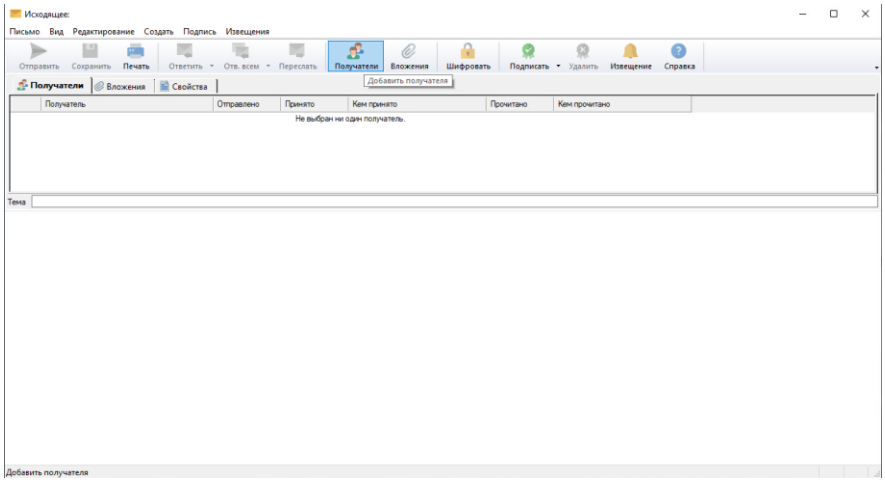

Рисунок 79 – Получатели

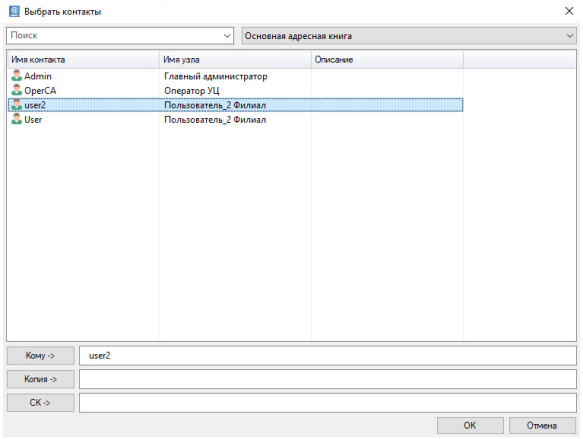

Рисунок 80 – Выбор контактов

Задаем название темы и заполняем содержимое письма для отправки. Нажимаем «Отправить» → «ОК».

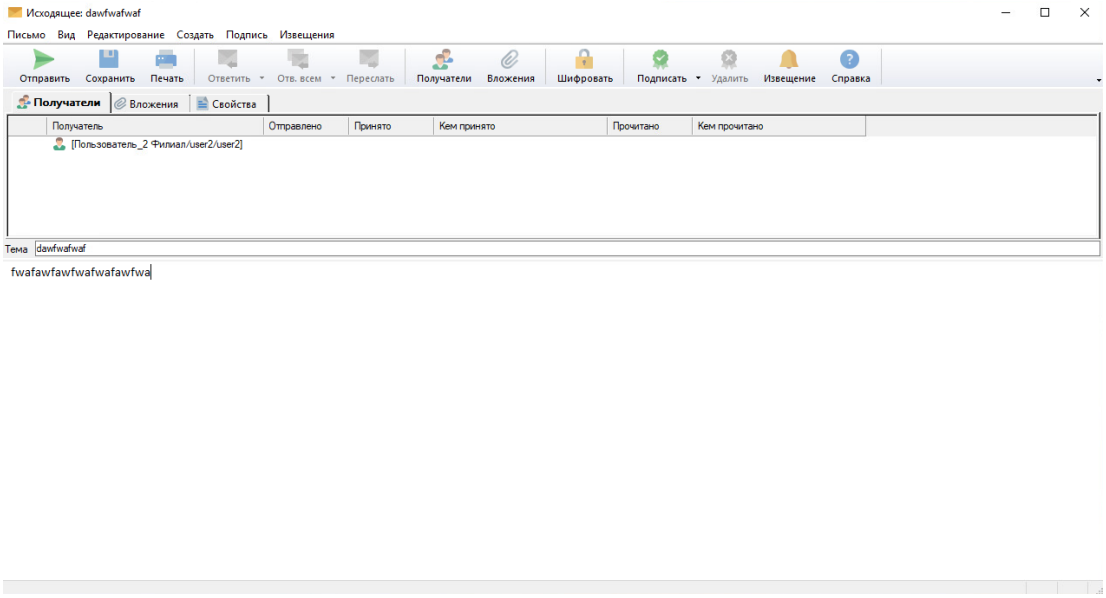

Рисунок 81 – Отправка письма

Заходим на деловую почту нашего нового пользователя для проверки наличия письма. После некоторого времени письмо дошло до нашего клиента.

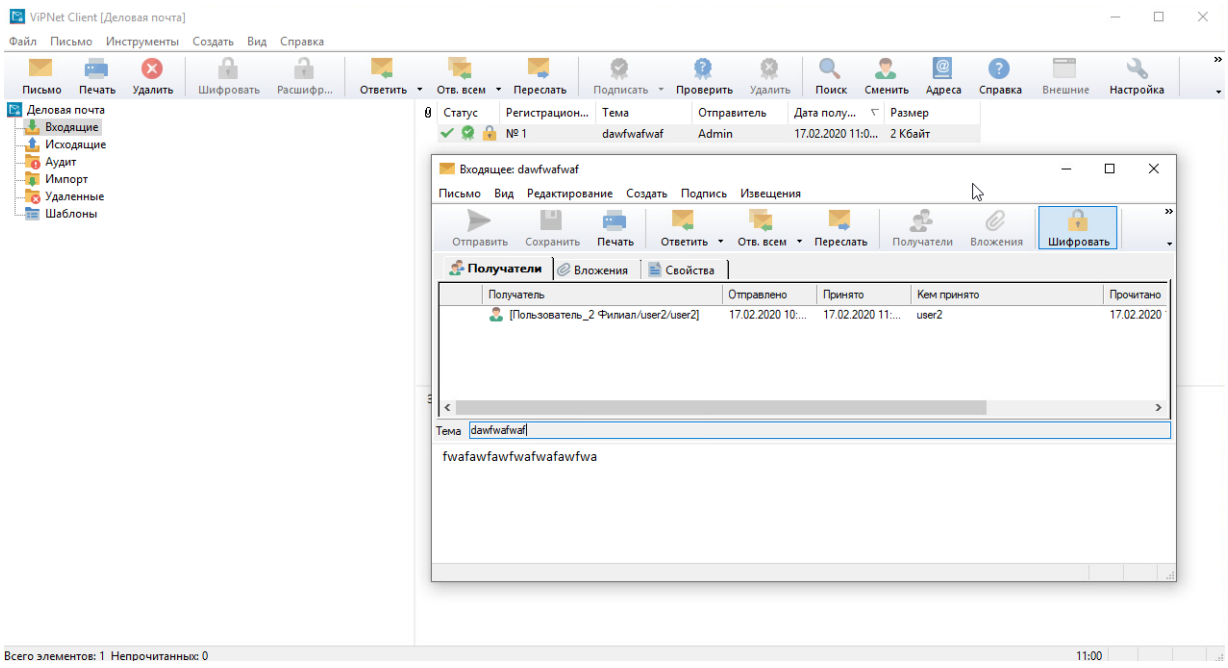

Рисунок 82 – Получение письма

Осталось проверить отправку текстового сообщения в ViPNet Client.

Заходим в ViPNet Client, нажимаем в левом углу «Сообщение». Если в получателях нет пользователя, добавляем его, нажав «Добавить» → Выбрать».

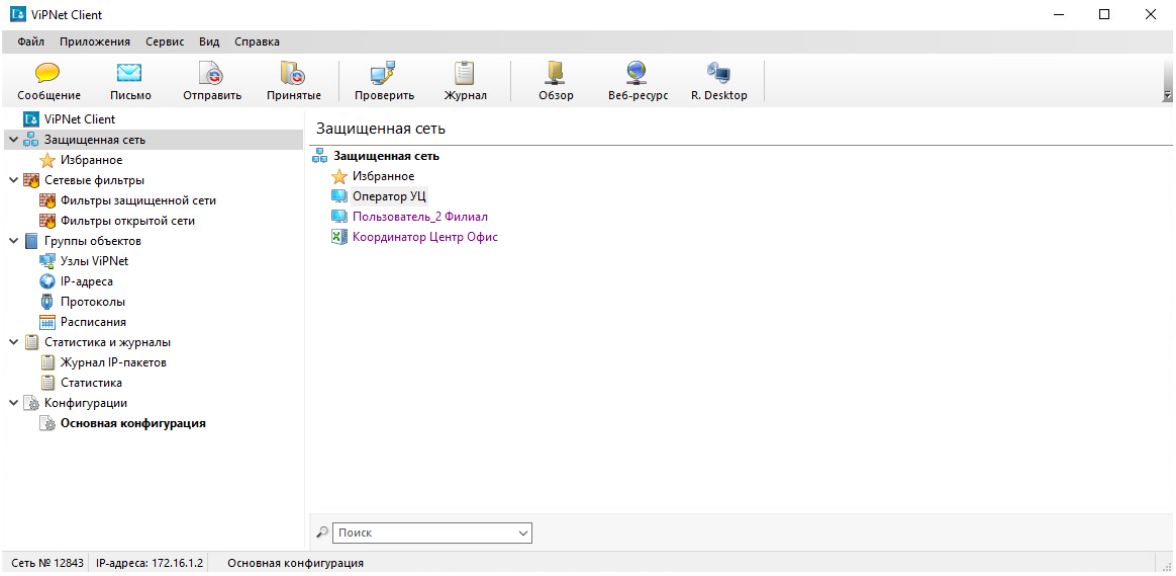

Рисунок 83 – ViPNet Client

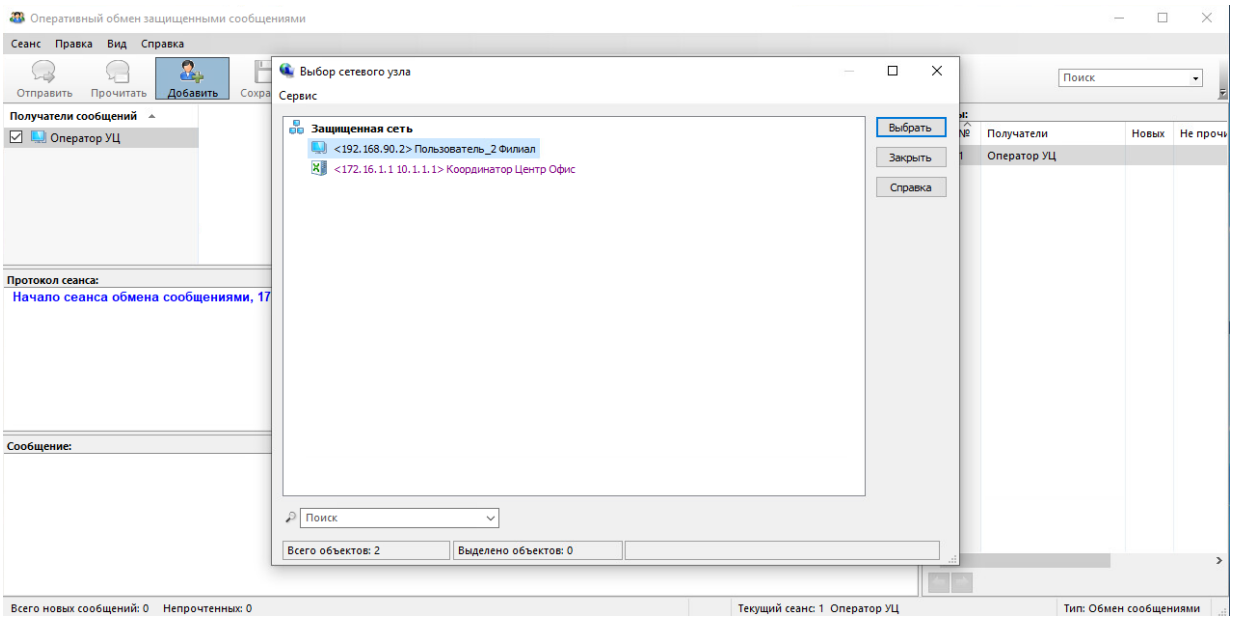

Рисунок 84 – Выбор сетевого узла

Заполняем содержимое текстового сообщения и нажимаем «Отправить». Переходим к ViPNet Client нашего нового пользователя и проверяем сообщение.

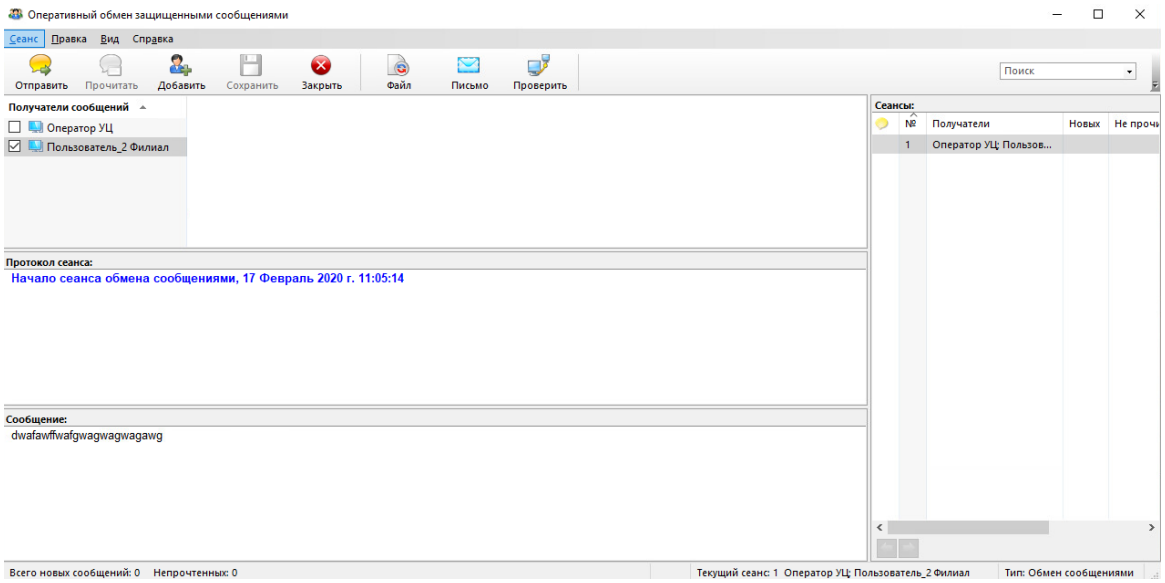

Рисунок 85 – Отправка текстового сообщения

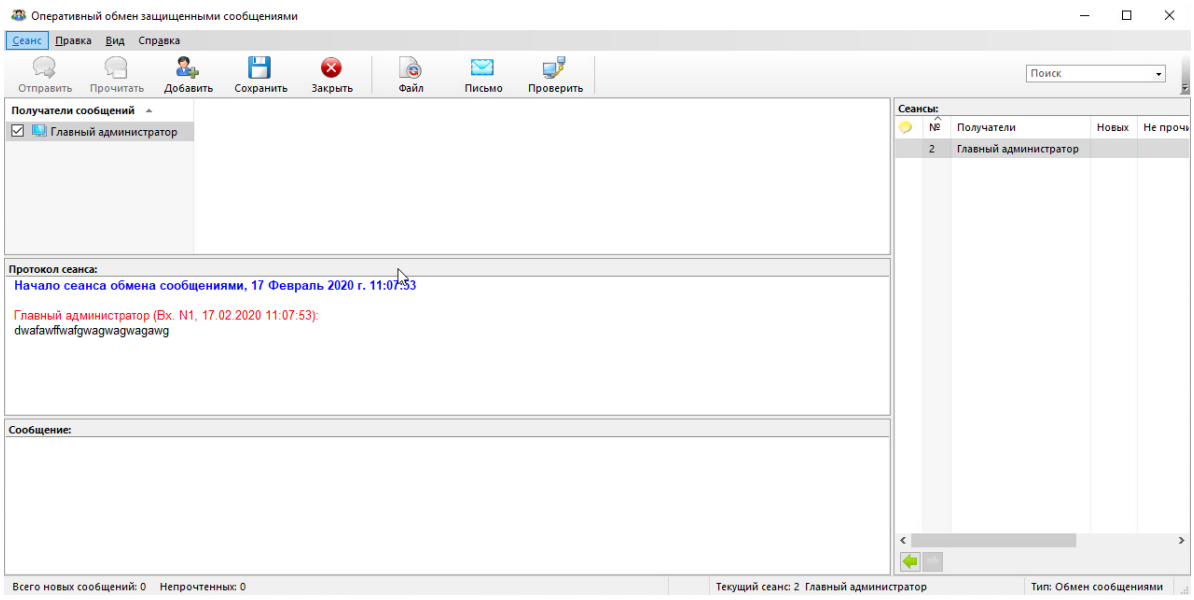

Рисунок 86 – Проверка отправленного текстового сообщения