Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА №51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ст. преподаватель		Ильина Д.В.
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №1

Развертывание защищенной сети VipNet

по курсу: Защита информационных процессов в компьютерных системах

РАБОТУ ВЫПОЛНИЛ:

СТУДЕНТ ГР. 5722		Е.Д. Энс
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2020

1. Содержание работы.

1. Установка программного комплекса VipNet Administrator 4.
2. Создание структуры защищенной сети.
3. Настройка резервного копирования данных и восстановление данных в ПО
4. VipNet Administrator.
5. Развертывание рабочего места помощника глав. администратора.

2. Подготовка виртуальных машин.

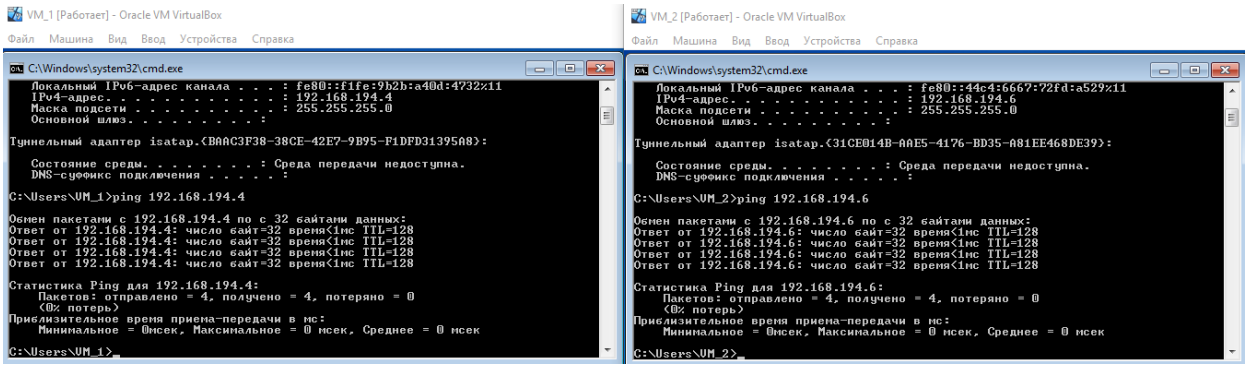
Для выполнения данной лабораторной работы потребуются две виртуальные машины. На каждой из виртуальных машин должно быть поднято по одному сетевому адаптеру, находящихся в одной подсети.

Номер сети: 192.168.194.0/28

IPVM 1: 192.168.194.4

IPVM 2: 192.168.194.6

Перед началом работы следует проверить корректность работы системы, используя утилиту ping.

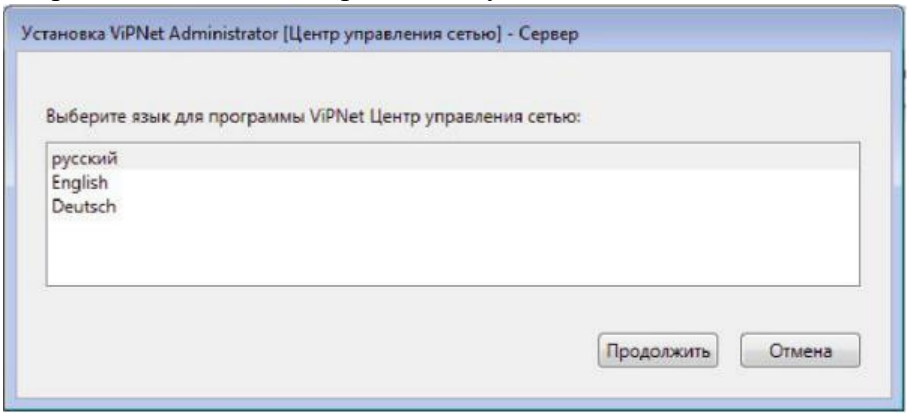


3. Ход работы

1. *Установка ПК VipNet AdTinistrator 4*

1.1 Установка серверного приложения VipNet ЦУС.

1) Для установки серверного приложения VipNet Центр управления сетью необходимо запустить файл \VipNet\ViPNet Administrator\Программное обеспечение\Центр управления сетью\Server Installer\Setup.exe».
2) В открывшемся окне выбираем язык установки.



3) Необходимо принять Лицензионное соглашение.

4) На странице Установка продукта оставляем пустыми поля «Имя пользователя» и «Пароль», т. к. если на компьютере не установлен SQL-сервер, то он будет установлен с указанным именем сервера.

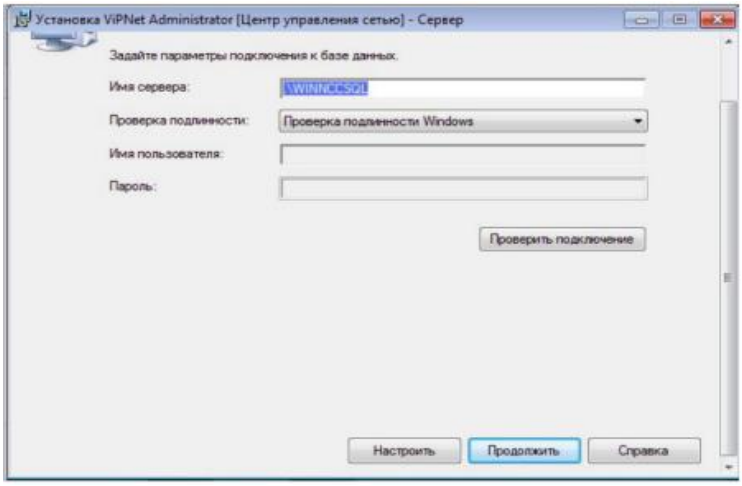


Рисунок 3 - Страница Установка продукта

5) После проверки введенных параметров необходимо нажать Установить сейчас (рис. 4). После создание сервера базы данных требуется перезагрузка компьютера. После перезагрузки установка ЦУС будет продолжена автоматически. По завершении установки следует нажать кнопку Закрыть.

В результате серверное приложение ЦУС будет установлено на машину (рис. 5).

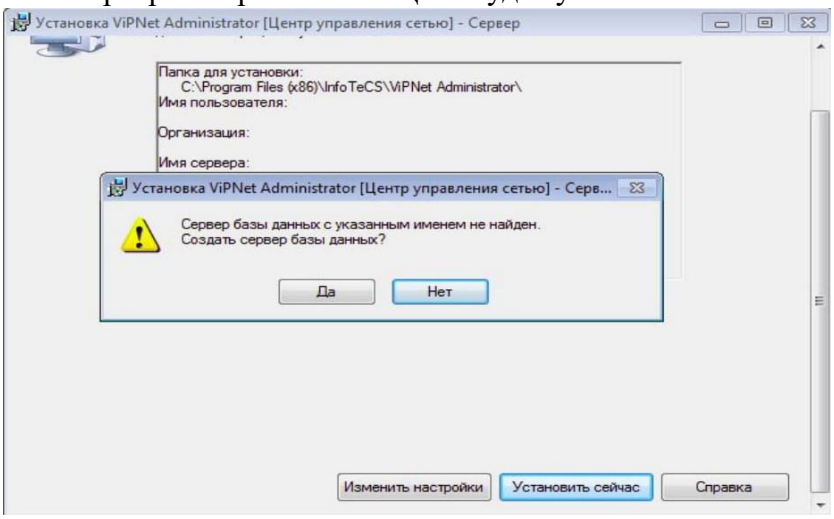


Рисунок 4 - Установка сервера базы данных

1.2 Установка клиентского приложения VipNet ЦУС.

Установка производится на ту же виртуальную машину.

1) Для установки клиентского приложения VipNet Центр управления сетью необходимо запустить файл файл \VipNet\ViPNet Administrator\Программное обеспечение\Центр управления сетью\Server Installer\Setup.exe Setup.exe».

2) При установке необходимо указать файл лицензии, выданный для выполнения лабораторных работ.

Далее установка аналогично пункту 1.1.

1.3 Установка VipNet Удостоверяющий и ключевой центр

Установка производится на ту же виртуальную машину.

1) Для установки приложения VipNet Удостоверяющий и ключевой центр необходимо запустить файл \VipNet\ViPNet Administrator\ Программное обеспечение\ Удостоверяющий и ключевой \Setup.exe».
2) Установка производится аналогично пунктам 1.1 и 1.2.

2. Создание структуры защищенной сети

№	Название СУ	Имя пользователя на СУ
1	Главный администратор	Глав админ Петров
2	Помощник глав админа	Помощник глав админа Иванов
3	Сотрудник 1 Центр офис	Сотруд_1 Центр Кузнецов
4	Сотрудник_2 Филиал	Сотруд_2 Филиал Попов

Таблица L Пользователи и сетевые узлы(клиенты)

Связи пользователей	Координатор Центр офис	Глав админ Петров	Помощник глав админа Иванов	Сотру Центр Кузнецов	Координатор Филиал	Сотру Филиал Попов
Координатор Центр офис		●	●	●	●	
Глав админ Петров	●		●			
Помощник глав админа Иванов	●	●				
Сотруд_1 Центр Кузнецов	●					●
Координатор Филиал	●					●
Сотруд_2 Филиал Попов				●	●	

Таблица 2. Матрица связей пользователей

Первый запуск VipNet Центр управления сетью.

1. При первом запуске приложения VipNet Центр управления сетью появится окно для ввода Имени пользователя и пароля. Необходимо в оба поля ввести — Administrator.
2. После запуска программы будет предложено сменить пароль (рис. 6). В данном случае пароль устанавливается равным восьми единицам -11111111.

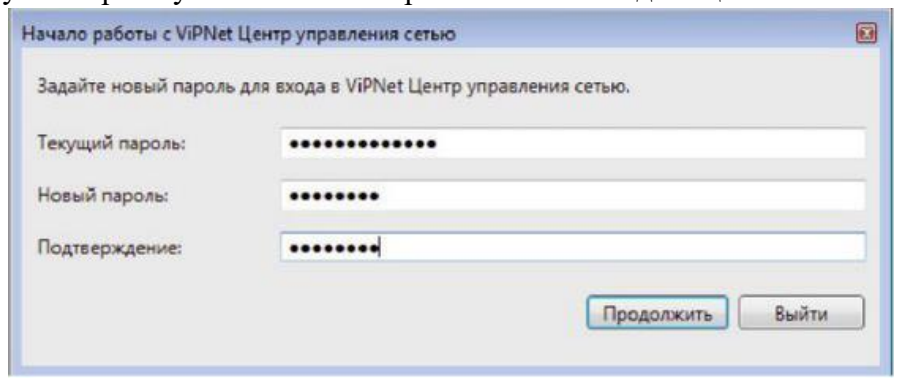


Рисунок 6 - Смена пароля при запуске Центра управления сетью

3. В следующем окне необходимо указать файл лицензии, выданный для выполнения лабораторных работ (рис. 7).

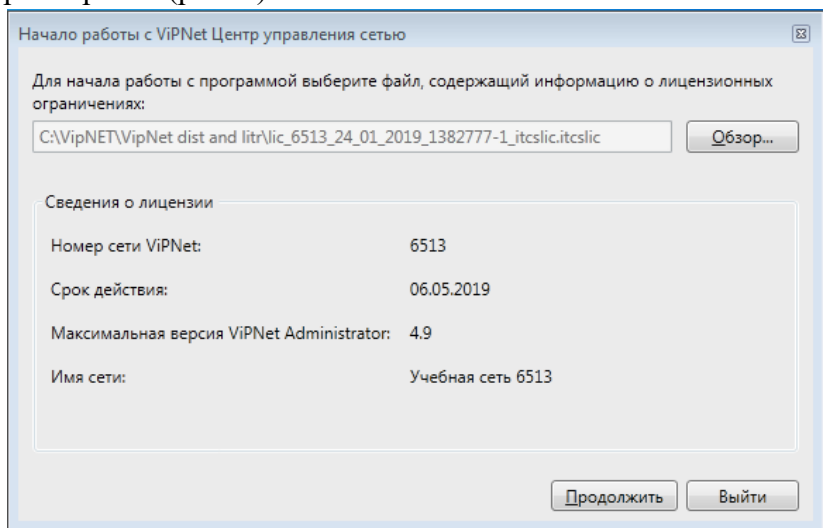


Рисунок 7 - Выбор лицензии при установке ЦУС

4. В следующем окне необходимо выбрать вариант Настроить структуру защищенной сети самостоятельно.
5. После открытия программы необходимо проверить первоначальные настройки (рис. 8).

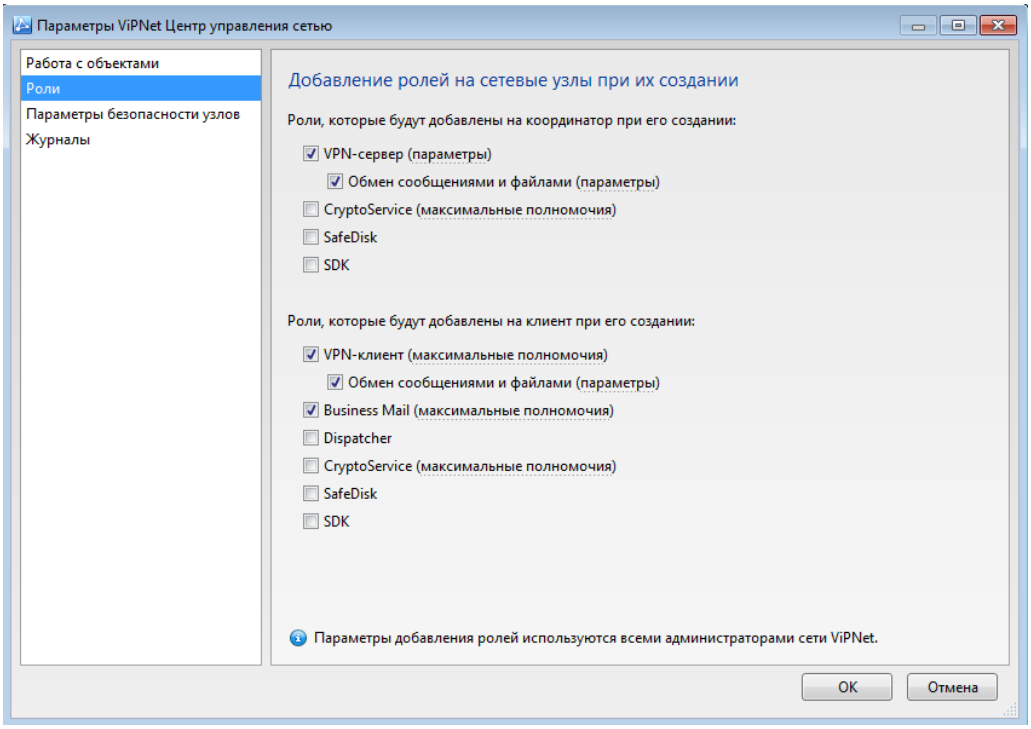


Рисунок 8 – Первоначальные настройки координаторов

2.1. Создание координаторов.

Для добавления координаторов необходимо выбрать представление Моя сеть, на панели навигации выбрать раздел Координаторы, нажать кнопку Создать и ввести имена координаторов. Результат добавления представлен на рисунке 9.

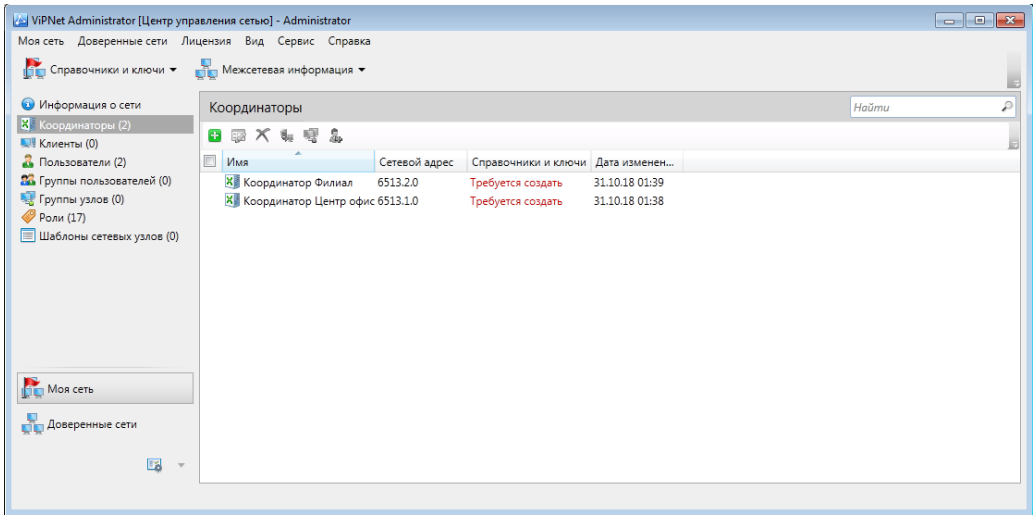


Рисунок 9 – Результат добавления координаторов

2.2. Создание клиентов.

Для добавления клиентов необходимо выбрать представление Моя сеть, на панели навигации выбрать раздел Клиенты, нажать кнопку Создать и ввести имена клиентов, выбрать им координатора (рис. 10). Результат добавления представлен на рисунке 11.

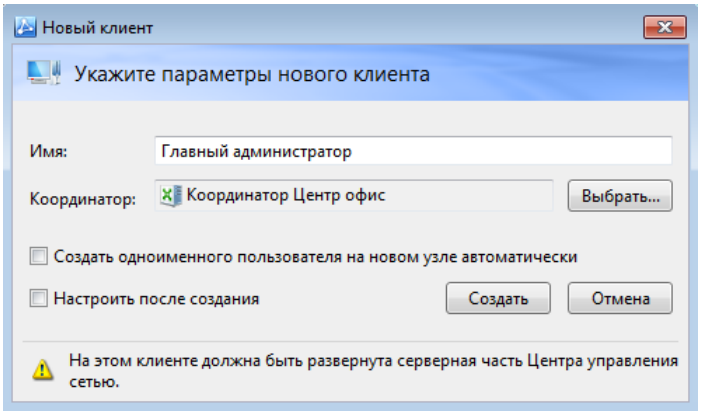


Рисунок 10 – Создание клиента

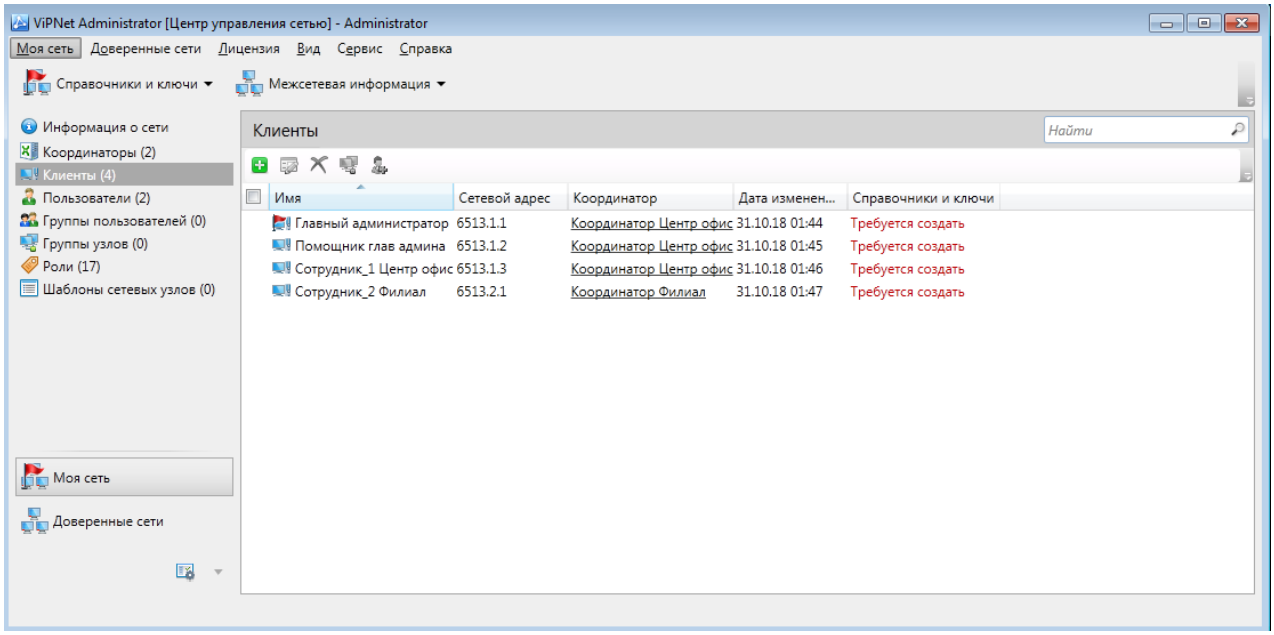


Рисунок 11 – Результат добавления клиентов

Созданным клиентам автоматически назначаются роли — ИРМ-клиент, Business Mail и Обмен сообщениями и файлами, а для первого созданного клиента дополнительно системные роли Network Control Center и Policy Manager. В этом можно убедиться зайдя в свойства клиентов.

Для создания пользователей и регистрации их на клиентах необходимо выбрать представление Моя сеть, на панели навигации выбрать раздел Пользователи, нажать кнопку Создать, ввести имена пользователей и выбрать сетевой узел в соответствии с таблицей 1. Результат создания пользователей представлен на рисунке 12.

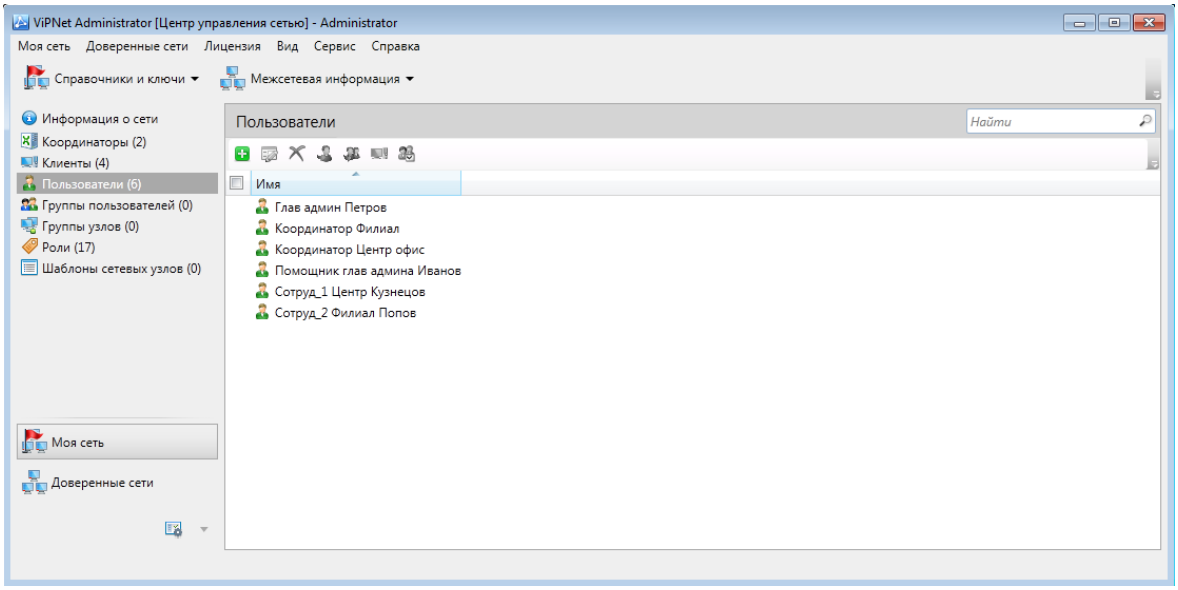


Рисунок 12 – Результат добавления пользователей

2.3. Создание межсервных каналов и связей.

Межсерверный канал связывает двух координаторов и позволяет им выполнять функцию сервера-маршрутизатора — обмениваться управляющими и прикладными транспортными конвертами. Необходимо, чтобы все координаторы были связаны между собой напрямую или через других координаторов.

Для построения межсерверного канала между Координатор Центр офис и Координатор Филиал необходимо:

1. Зайти в свойства СУ Координатор Центр офис.
2. Нажать на кнопку Добавить.
3. В открывшемся окне выбрать сетевой узел Координатор Филиал и нажать на кнопку Добавить.
4. Добавить связи между пользователями в соответствии с таблицей 2.
5. Проверить конфигурацию сети, выбрав в меню Моя сеть пункт Проверить конфигурацию сети... В случае, если сеть сконфигурирована верно, на экран выведется сообщение, аналогичное рис. 13.

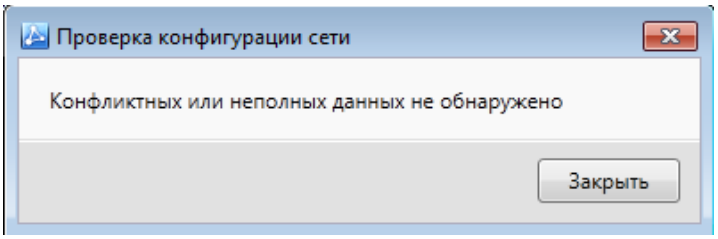


Рисунок 13 – Результат добавления пользователей

6. Следует подготовить данные для создания дистрибутивов в УКЦ. Для этого необходимо сформировать справочники, выбрав в меню Моя сеть пункт Создать справочники. Создать их надо для всего списка.

2.4. Первый запуск программы VipNet УКЦ.

1. При первом запуске программы VipNet УКЦ необходимо выбрать пункт Настройка новой базы Данных в окне Начало работы с программой Удостоверяющий и ключевой центр.
2. На странице Подключение к базе Данных VipNet Administrator указать сетевой адрес экземпляра SQL-сервера и имя базы данных.
3. На следующей странице выбрать тип проверки По имени и паролю пользователя SQL- сервера (рис. 14).

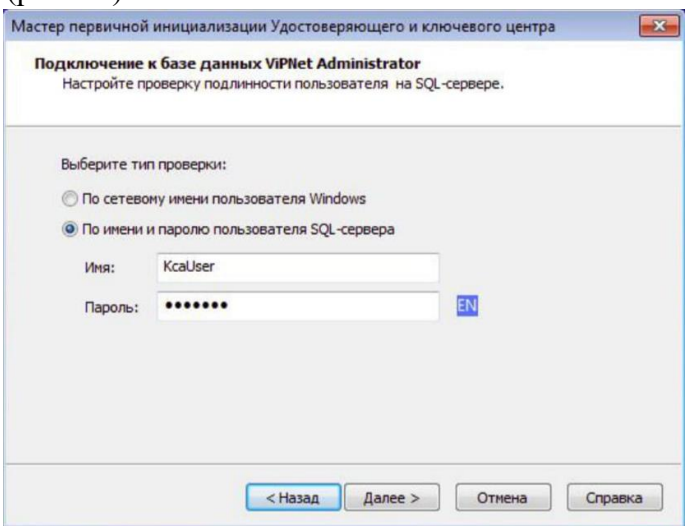


Рисунок 14 – Начало работы с программой Удостоверяющий и ключевой центр

4. В следующем окне указать имя главного администратора VipNet компании — Владимир (рис. 15).

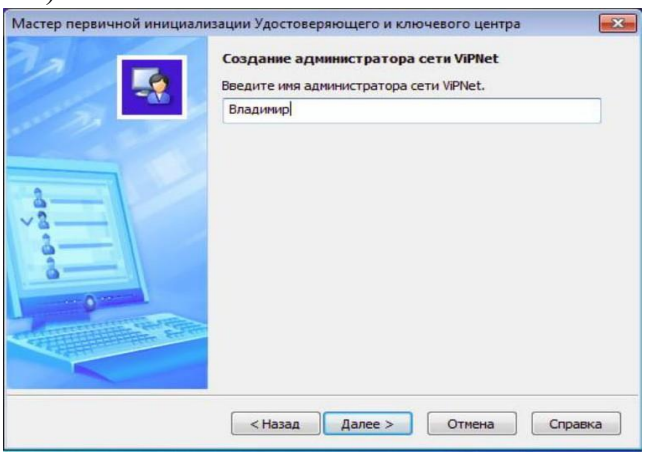


Рисунок 15 – Имя главного администратора сети

5. На следующих страницах необходимо ввести информацию о владельце сертификата, параметры ключа электронной подписи (по умолчанию), срок действия сертификата (192 месяца с настоящего момента).
6. На странице Место хранения контейнеров ключа подписи и ключа защиты УКЦ надо выбрать В файле.
7. На странице Настройка паролей выбрать тип — Собственный пароль, способ выдачи пароля пользователя — Сохранять пароль в XPS в папку. На появившейся страничке задать пароль администратора – 11111111.

8. После подтверждения введенных данных и прохождения Электронной рулетки инициализация будет успешно пройдена. В этом случае будет:

- создана учетная запись администратора УКЦ;
- создан ключ электронной подписи и издан сертификат администратора УКЦ;
- созданы мастер-ключи;
- установлено соединение с базой данных SQL и произведено ее заполнение данными.

В случае корректной инициализации появится главное окно программы (рис. 16).

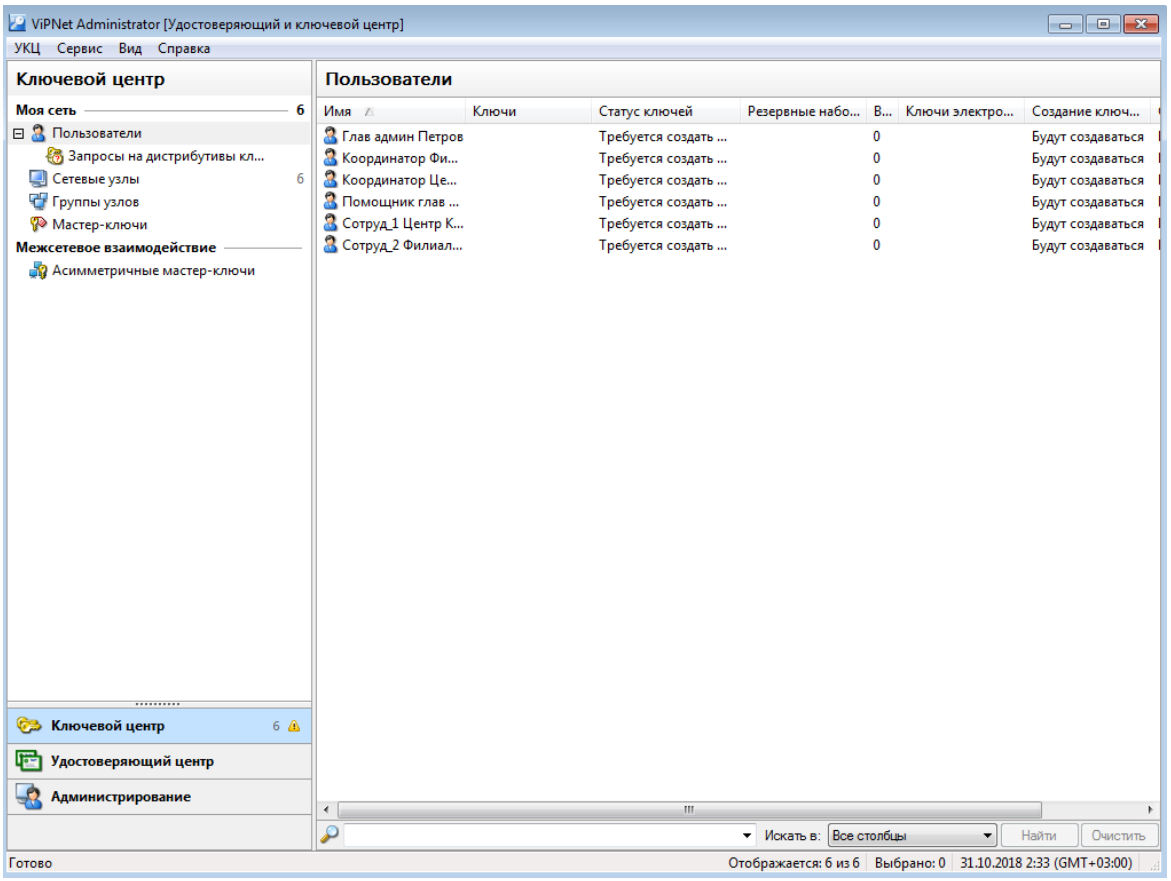


Рисунок 16 - Главное окно УКЦ

Перед началом работы в УКЦ необходимо проверить первоначальные настройки. В меню Сервис выбрать пункт Настройка. В открывшемся окне в разделе Пароли установить тип пароля — Собственный пароль, на вкладке Сертификаты снять галочку с Редактировать поля сертификатов при издании и Создавать ключи электронной подписи.

Для каждого пользователя надо снять вручную флажок Создавать ключи электронных подписей в свойствах.

2.5. Выдача дистрибутивов ключей.

Для выдачи дистрибутивов ключей необходимо:

1. В окне программы VipNet Удостоверяющий и ключевой центр на панели навигации выбрать представление Ключевой центр и перейти в раздел Моя сеть Сетевые узлы.
2. Задать пароль администратора для всех созданных сетевых узлов (пароль 11111111)

3. Выделить все сетевые узлы, в контекстном меню выбрать Выдать новый Дистрибутив ключей ...
4. Задать пароля пользователя пользователя – 11111111 по очереди для каждого пользователя (рис. 17).

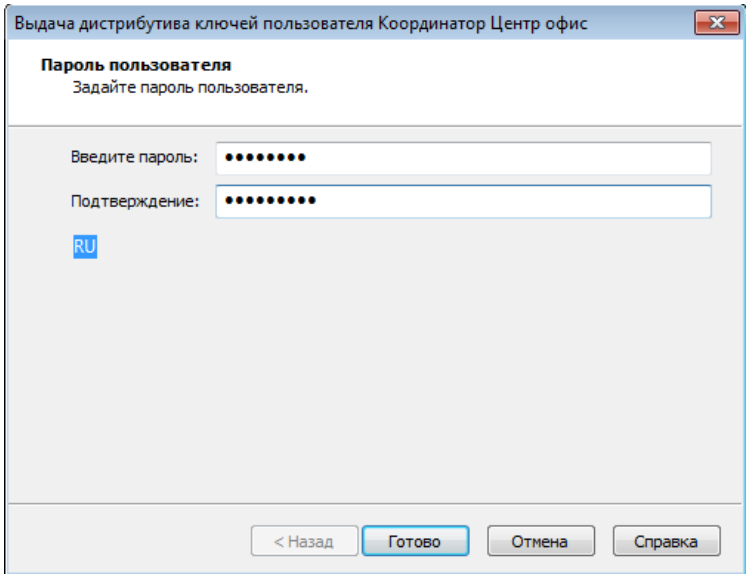


Рисунок 17 - Задание пароля для пользователя

После успешной настройки откроется папка, в которой хранятся дистрибутивы ключей. Администратор УКЦ должен доверенным путем передать пользователю следующее:

- Дистрибутив ключей
- Пароль пользователя.

3. Настройка резервного копирования и восстановления Данных в ПО VipNet Administrator.

3.1 Создание резервной копии в ручном режиме.

В состав резервной копии конфигурации сети (файл *.rp) входят следующие данные:

- копия базы данных VipNet Administrator, в которой содержится информация о структуре сети VipNet, о сертификатах и списках аннулированных сертификатов, изданных в УКЦ, и др. данные.
- Копия папки, в которой хранится служебная информация УКЦ: C: \Program Data \Infotecs \ VipNet Administratork \ *KC*
- Копии контейнеров ключей администраторов УКЦ.
- Справочники и ключи связи

Резервные копии по умолчанию помещаются в папку *C:\Program Data \Infotecs \ VipNet Administrator\KC\Restore.*

Для создания резервной копии необходимо:

1. В окне программы VipNet Удостоверяющий и ключевой центр в меню Сервис выбрать пункт Восстановление конфигурации ...
2. В появившемся окне выбрать Создать резервную копию текущей конфигурации (рис. 18).

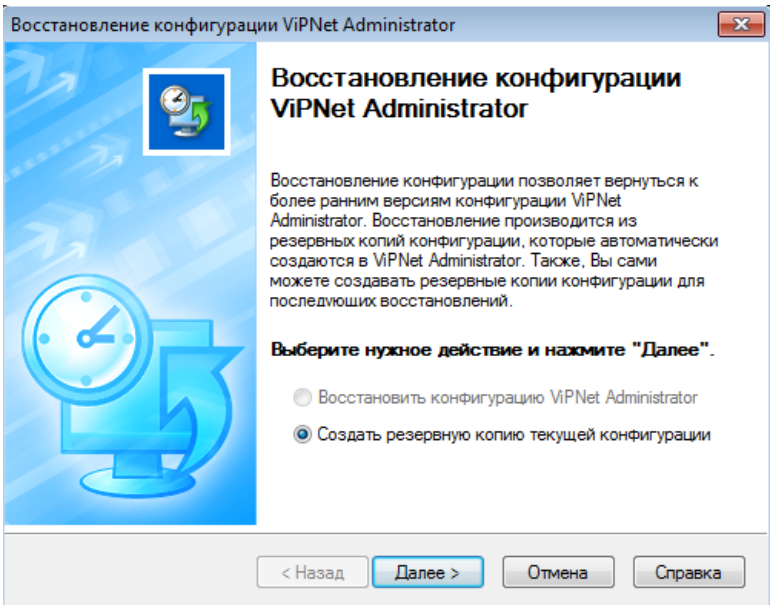


Рисунок 18 - Создание резервной копии текущей конфигурации

3. В окне Создание резервной копии ввести комментарий.

Чтобы посмотреть список резервных копий в меню Сервис необходимо выбрать пункт Восстановление конфигурации... Редактировать список резервных копий. На экран будет выведен список созданных копий (рис. 19).

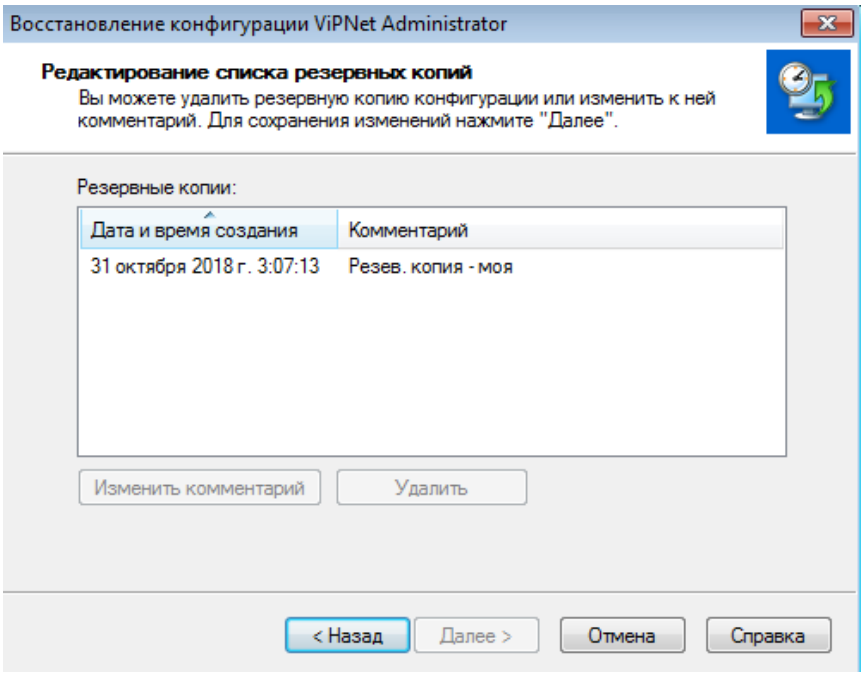


Рисунок 19 - Список созданных резервных копий

3.2 Настройка автоматического резервного копирования.

1. В меню Сервис выбрать пункт Настройки Восстановление конфигурации.
2. Проверить установлен ли флажок Автоматически создавать резервные копии каждые...
3. Указать периодичность создания резервной копии 1 день, время создания — 23:59.

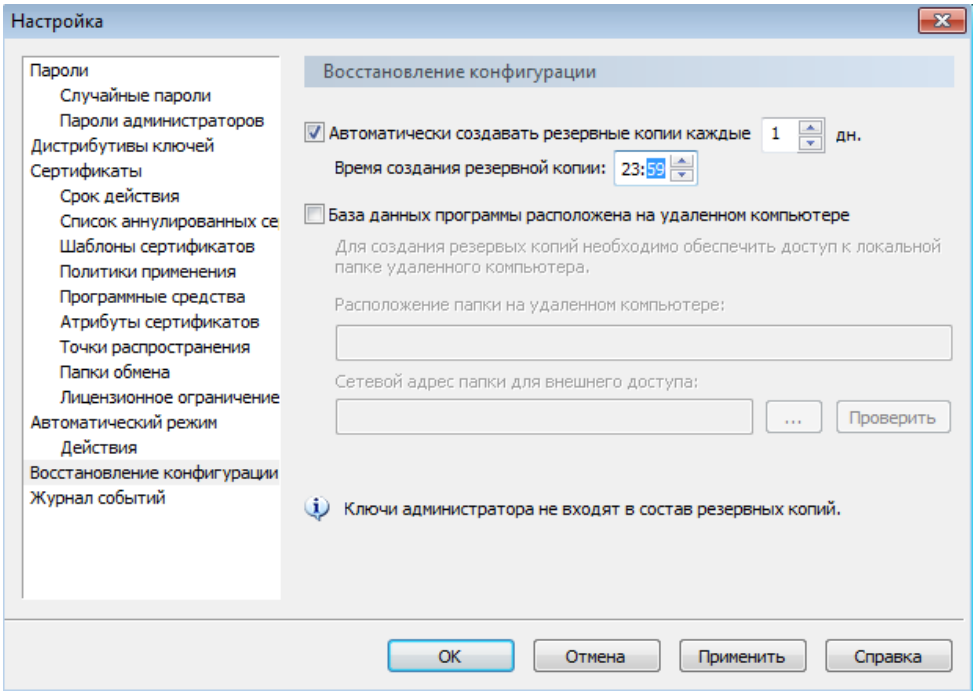


Рисунок 20 - Настройка автоматического резервного копирования

4. Развертывание рабочего места помощника главного администратора.

4.1 Установка VipNet Client.

ПО VipNet Client необходимо установить на обе виртуальные машины. Для этого:

1. На VM 1 запустить файл ../Материалы/ViPNetClient 4/1. Программное обеспечение/Client_RUS 4.3.2.46794.exe.
2. Принять условия лицензионного соглашения.
3. Дождаться установки и перезагрузки машины.
4. После перезагрузки системы на экран будет выведено диалоговое окно об отсутствии ключей. Необходимо подтвердить установку ключей и указать файл дистрибутива ключей *.dst для пользователя Глав админ Петров сетевого узла Главный администратор. Данные дистрибутивы были созданы ранее. При успешном выполнении выведется соответствующее сообщение (рис. 21).

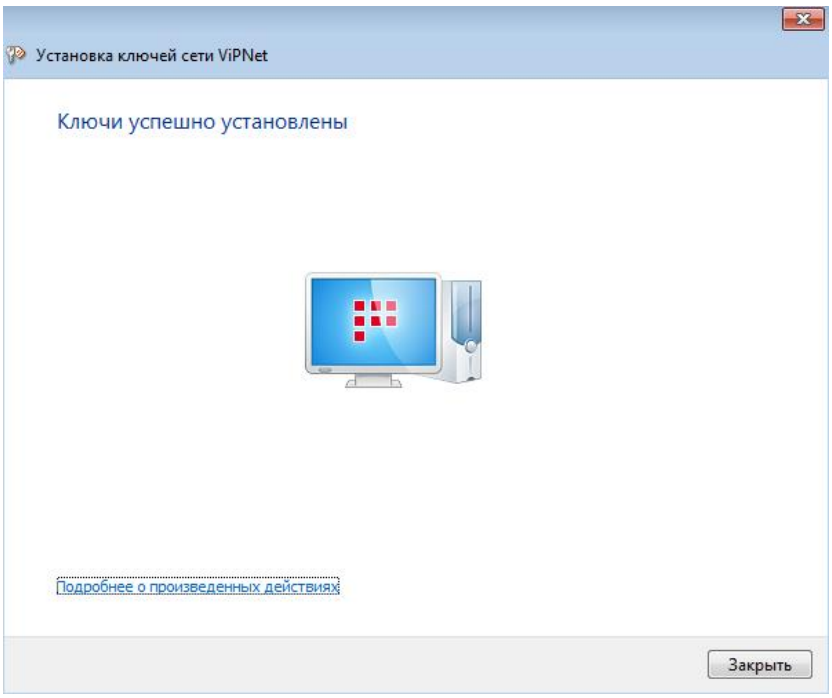


Рисунок 21 - Успешная установка ключей

5. На экране появится окно аутентификации в ПО VipNet Client. Необходимо выбрать способ — Пароль и ввести пароль, заданный при создании дистрибутивов - 11111111
6. Если пароль введен верно, то в области уведомлений н панели задач появится значок VipNet Client Монитор (рис.22).

Рисунок 22 - Значок VipNet Client Монитор

Аналогичным образом устанавливается ПО VipNet Client на рабочую машину помощника главного администратора VM 2. Чтобы удостовериться в связности узлов на машине помощника необходимо зайти в VipNet Client Монитор и в разделе Защищенная сеть выделить узел Главный администратор и нажать F5 — узел должен иметь статус Доступен.

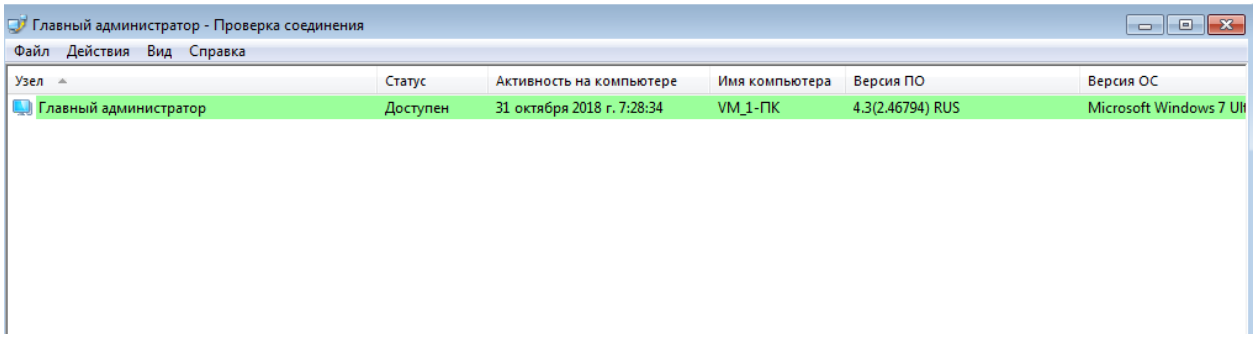


Рисунок 23 - Связанность узлов

4.2 Установка и настройка клиентского приложения ЦУС на рабочем месте помощника главного администратора сети.

Чтобы дать возможность помощника главного администратора управлять через дополнительное рабочее место ЦУС конфигурацией защищенной сети, необходимо создать учетную запись помощника главного администратора ЦУС (на VM 1) и установить клиентское приложение ЦУС на рабочем месте помощника (VM 2).

Для создания учетной записи помощника главного администратора необходимо:

1. Перейти на рабочее место Главный администратор в программе VipNet Центр управления сетью.
2. В окне программы VipNet Центр управления сетью выбрать пункт меню Вид Администрирование, раздел Учетные записи (рис. 24).

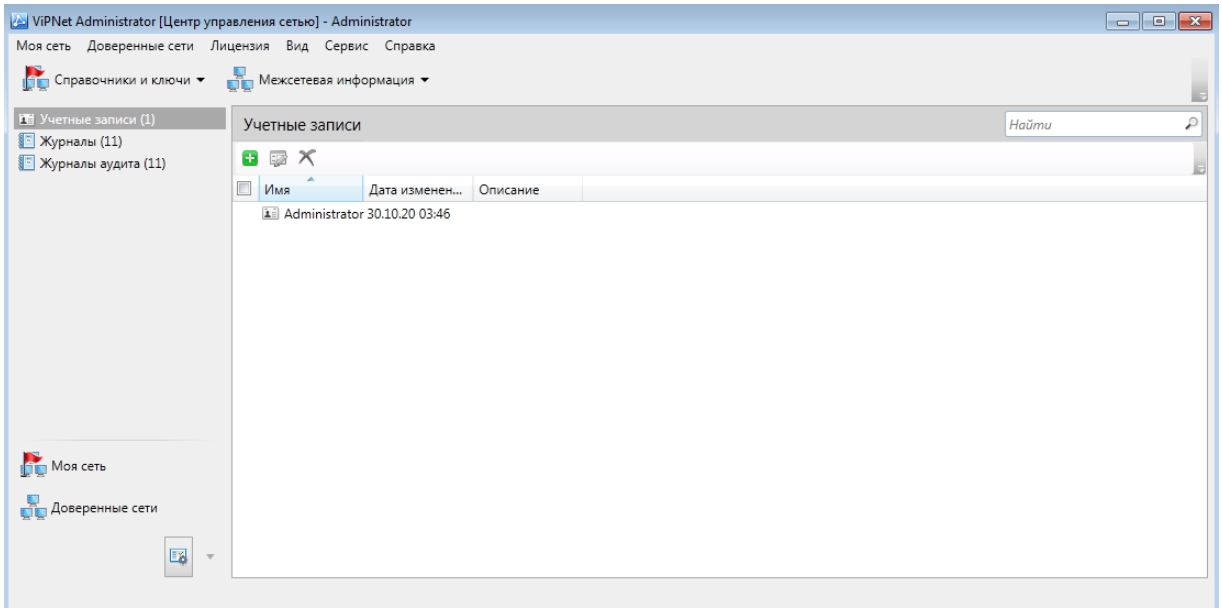


Рисунок 24 - Раздел” Администрирование”

3. В разделе Учетные записи на панели инструментов нажать кнопку Добавить.
4. В открывшемся окне указать имя Administrator2, пароль – 11111111, описание — Помощник главного администратора сети (рис. 25).

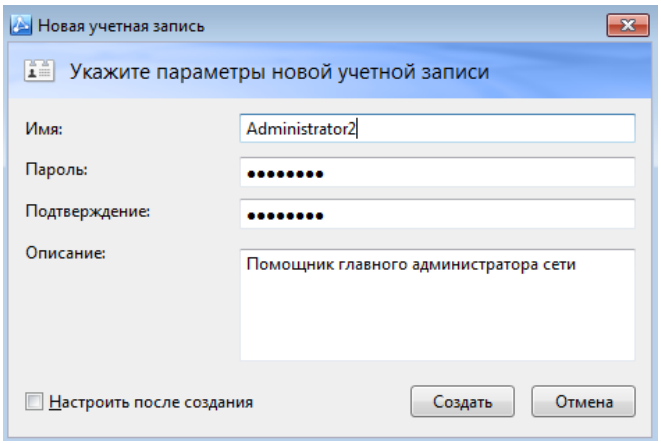


Рисунок 25 - Добавление новой учетной записи

После этого раздел Учетные записи примет вид согласно рисунку ниже (рис. 26). На вкладке Защищенная сеть необходимо посмотреть IP-адрес сетевого узла Главный администратор.

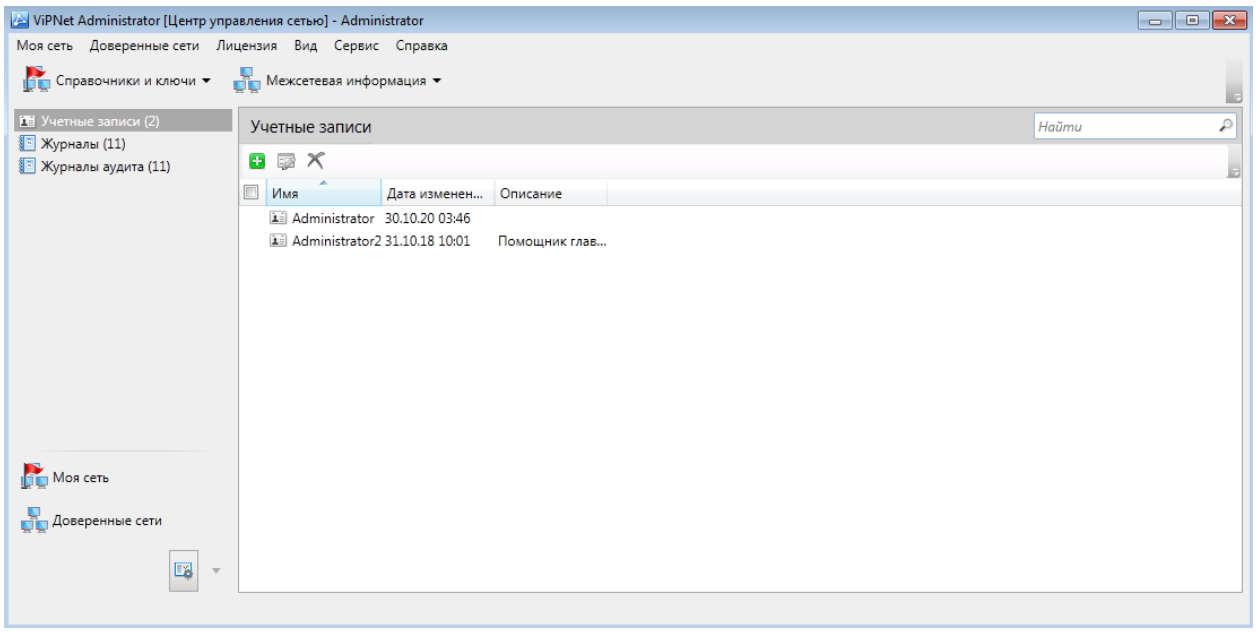


Рисунок 26 - Раздел Учетные записи

На рабочем месте помощника главного администратора (VM 2) необходимо установить клиентскую часть VipNet Administrator ЦУС аналогично тому, как это делалось ранее. После чего надо:

1. Запустить клиентскую часть VipNet Administrator ЦУС.
2. В появившемся окне ввести IP-адрес сетевого узла Главный администратор (рис. 27).

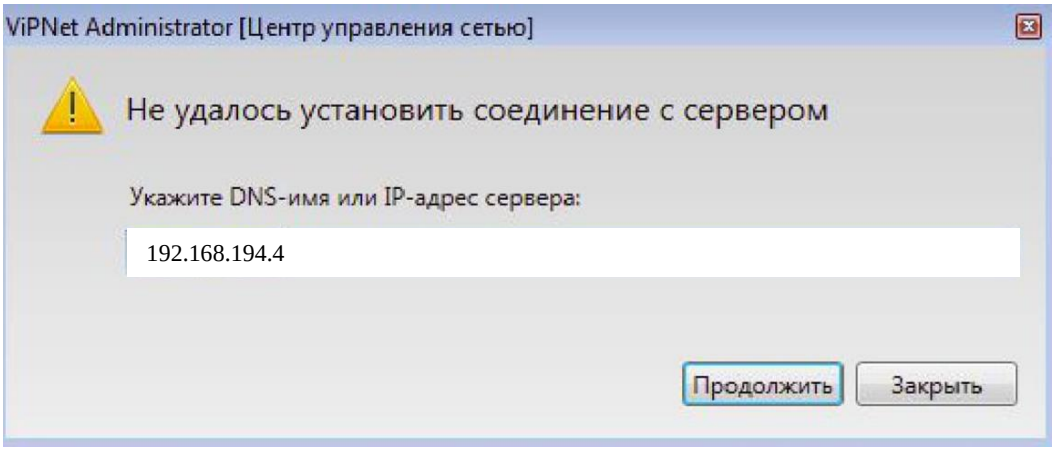


Рисунок 27 - IP-адрес сетевого узла Главный администратор

3. Если связь с сервером установилась — появится окно для ввода имени пользователя — Administrator2, пароль — 11111111
4. После подключения надо будет задать новый пароль. Старый пароль – 11111111, новый 11111111.

Теперь можно управлять защищенной сетью VipNet с двух рабочих мест.

4. Выводы

В данной лабораторной работе была создана и сконфигурирована защищенная VipNet сеть, для этого:

1. Созданы пользователи и сетевые узлы, настроены связи между ними.
2. Создано автоматическое резервное копирование.