Задание № 1.2. Создание структуры защищенной сети

Формулировка задания

Создать структуру защищенной сети в соответствии с заданной схемой, настроить связи пользователей (в соответствии с матрицей связей) в ЦУС и сформировать дистрибутивы ключей для сетевых узлов в УКЦ.

В ЦУС предусмотрено автоматическое создание связей без возможности их удаления между некоторыми сетевыми узлами (в списке связей помечаются серым цветом, *ЦУС→Свойства узла*):

- Связь узла с Центром управления сетью.
- Связи между координатором и зарегистрированными на нем клиентами.
- Связи между координатором и клиентами, для которых данный координатор назначен сервером IP-адресов.
- Связь между сетевым узлом и координатором, выбранным для организации соединений с внешними узлами.
- Связи между координаторами, которые образуют межсерверный канал.
- Связь между узлом с программой *ViPNet Policy Manager* и подчиненными ему сетевыми узлами *(см. Практическое занятие № 2)*.
- Связи шлюзовых координаторов своей сети со шлюзовыми координаторами доверенных сетей *(см. Практическое занятие № 3)*.
- Связи Центра управления сетью с Центрами управления сетью доверенных сетей.

Связь узла с *Центром управления сетью* является технологической и используется только для обеспечения возможности рассылки справочников, ключей и обновлений ПО.

Таблица 1 – Пользователи и сетевые узлы (клиенты)

№	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 2 – Матрица связей пользователей

Матрица связей пользователей	*Координатор Центр офис*	*Глав админ Петров*	*Помощник глав админа Иванов*	*Сотруд_1 Центр Кузнецов*	*Координатор Филиал*	*Сотруд_2 Филиал Попов*
Координатор Центр офис		+	+	+	+	
Глав админ Петров	+		+			
Помощник глав админа Иванов	+	+				
Сотруд_1 Центр Кузнецов	+					+
Координатор Филиал	+					+
Сотруд_2 Филиал Попов				+	+	

Примечание 1. Рекомендуется устанавливать в первую очередь связи пользователей, так как в данном случае связи узлов будут установлены автоматически.
На каждом защищенном узле в программе ViPNet Монитор в разделе «Защищенная сеть» отображается список сетевых узлов, с которыми связан данный узел. Однако для отображения в программе ViPNet Монитор узла с программой ViPNet Центр управления сетью необходимо **дополнительно** создать связь между пользователями сетевого узла и Центра управления сетью. Если связь с Центром управления сетью должна оставаться скрытой, не следует создавать связи между пользователями сетевых узлов и пользователем Центра управления сетью.
Примечание 2. Для удобства администрирования сети ViPNet рекомендуется выработать правила формирования имен узлов и пользователей, чтобы было понятно, какой пользователь за каким узлом находится (пример: Глав админ Петров, состоит из сокращенного названия узла и ФИО пользователя). Если по архитектуре сети не критично наличие в названии узла ФИО пользователя, можно установить в настройках ЦУС автоматическое создание одноименного пользователя для создаваемого узла.

Первый запуск ViPNet Центр управления сетью

Внимание. Если при первом же запуске возникли проблемы, а именно не удается запустить или подключиться к Центру управления сетью, рекомендуем обратиться к подразделу Возможные неполадки и способы их устранения раздела Справочная информация **(**см. стр. 180**)** или одноименному разделу в технической документации.

1. Чтобы начать работу с программой ViPNet Центр управления сетью, выполните запуск программы с ярлыка на Рабочем столе или через меню Пуск (Пуск > Все программы > ViPNet > ViPNet Administrator > Центр управления сетью).
2. В появившемся окне введите имя *Administrator* и пароль *Administrator*, нажмите кнопку *Продолжить (Рисунок 12)*.

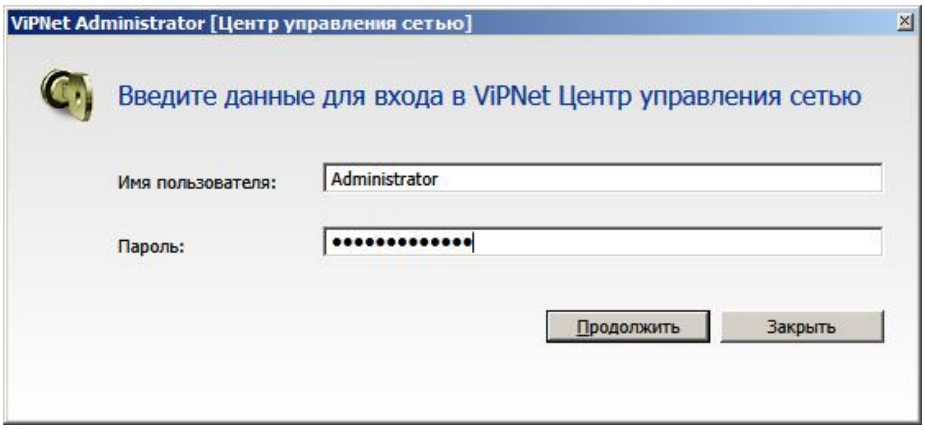

Рисунок 1 – Ввод имени пользователя и пароля

3. После загрузки программы будет предложено сменить пароль. Чтобы сменить пароль, введите текущий пароль (*Administrator*), новый пароль, а затем нажмите кнопку *Продолжить*. В рамках практического занятия, новый пароль - *11111111*.

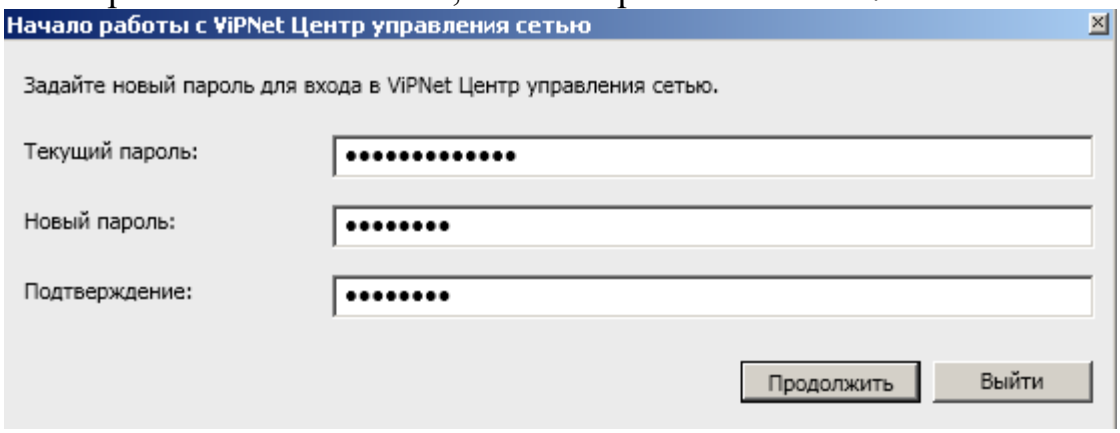

Рисунок 2 – Смена пароля

4. В окне *Начало работы с ViPNet Центр управления сетью* с помощью кнопки *Обзор* укажите путь к файлу лицензии на сеть ViPNet (**.itcslic* или *infotecs.reg*) и нажмите кнопку *Продолжить (Рисунок 14)*.

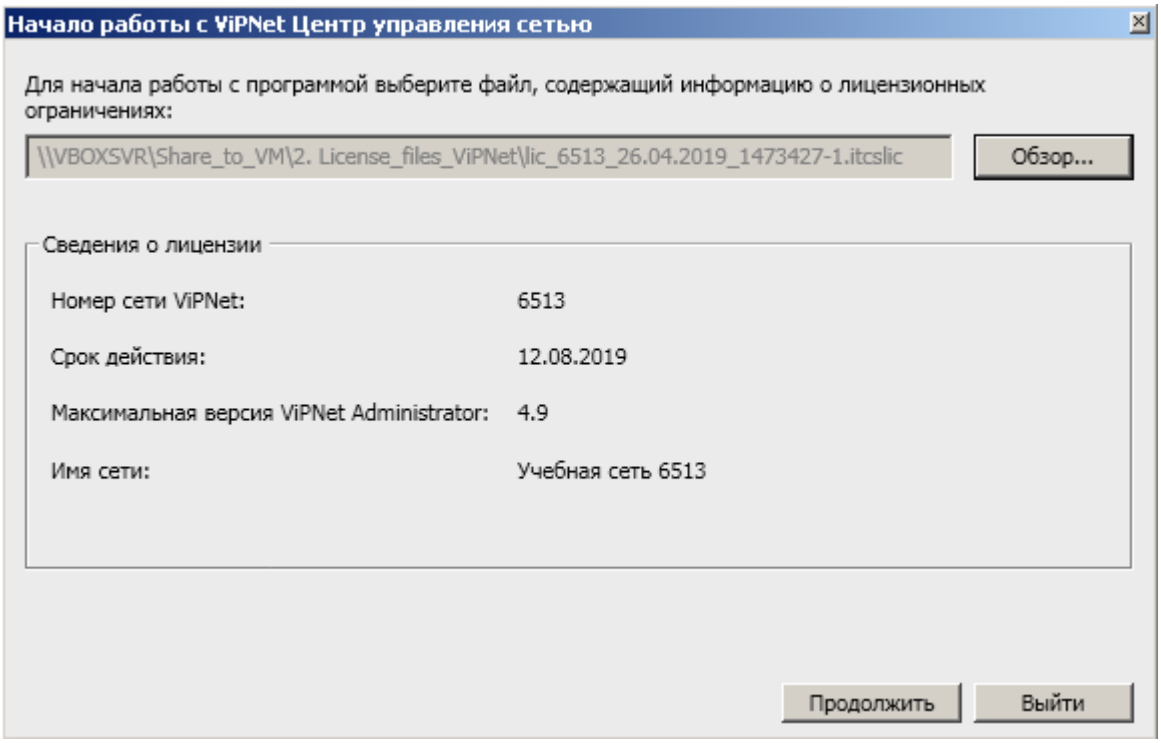

Рисунок 3 – Выбор файла лицензии

5. В появившемся окне с выбором возможных сценариев работы нажмите *Настроить структуру защищенной сети самостоятельно (Рисунок 15)*.

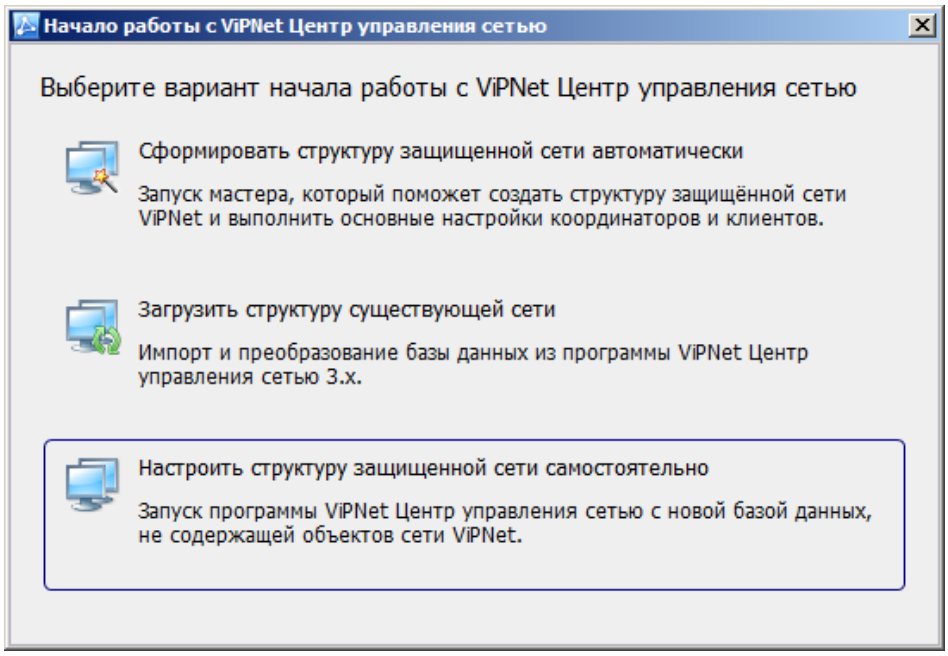

Рисунок 4 – Выбор варианта начала работы с ЦУС

6. Откроется главное окно программы *(Рисунок 16)*.

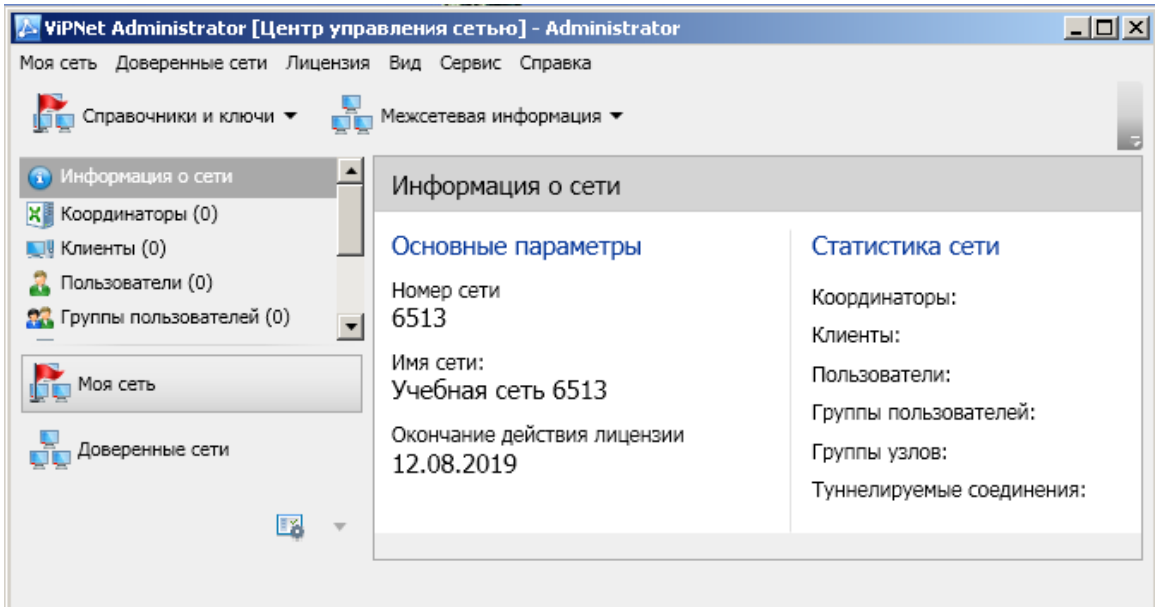

Рисунок 5 – Вид главного окна ЦУС

7. Проверьте первоначальные настройки программы *ViPNet Центр управления сетью*. Для этого выполните следующие действия:

В меню *Сервис* выберите пункт *Параметры* и в открывшемся окне перейдите в раздел *Роли*, затем, если обнаружите различия, задайте значения параметров в соответствии с *Рисунком 17*.

В реальной сети рекомендуется задавать средний или минимальный уровень полномочий. Полномочия задаются при нажатии на подчеркнутые мелким пунктиром, расположенные в скобочках параметры.

Теперь можно приступить к созданию структуры защищенной сети.

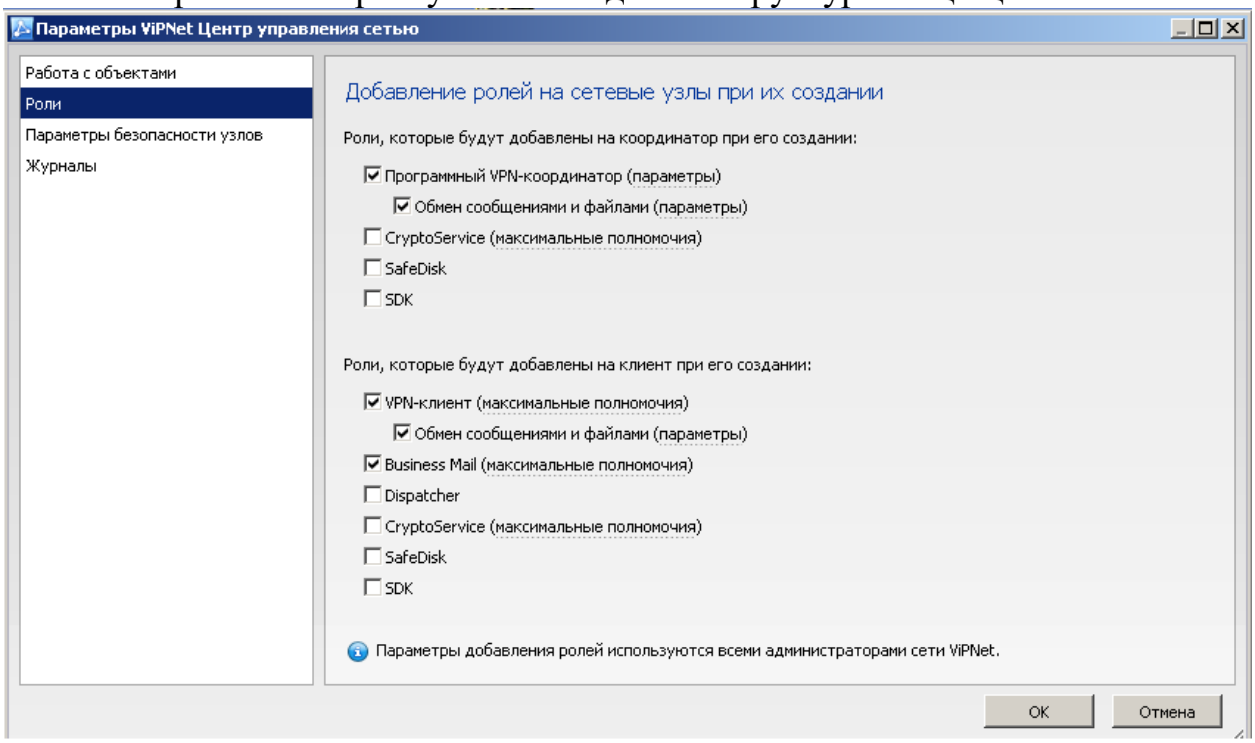

Рисунок 6 – Окно *Параметры* программы *ViPNet Центр управления сетью*

1.2.1. Создание координаторов

В соответствии со схемой развертывания ViPNet в локальной сети компании необходимо создать сетевые узлы: *Координатор Центр офис* и *Координатор Филиал.*

Чтобы добавить в сеть ViPNet новый координатор, выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел *Координаторы*.
3. В разделе *Координаторы* на панели инструментов нажмите кнопку *Создать*.
4. В появившемся окне задайте имя *Координатор Центр офис*, оставьте флажок *Создать одноименного пользователя* и нажмите кнопку *Создать*. В данном случае нам не требуется снимать флажок, так как имя узла и имя пользователя координатора, будут совпадать, таким образом не придется совершать лишних действий (это ускорит процесс создания структуры сети). Режим работы также следует оставить по умолчанию.

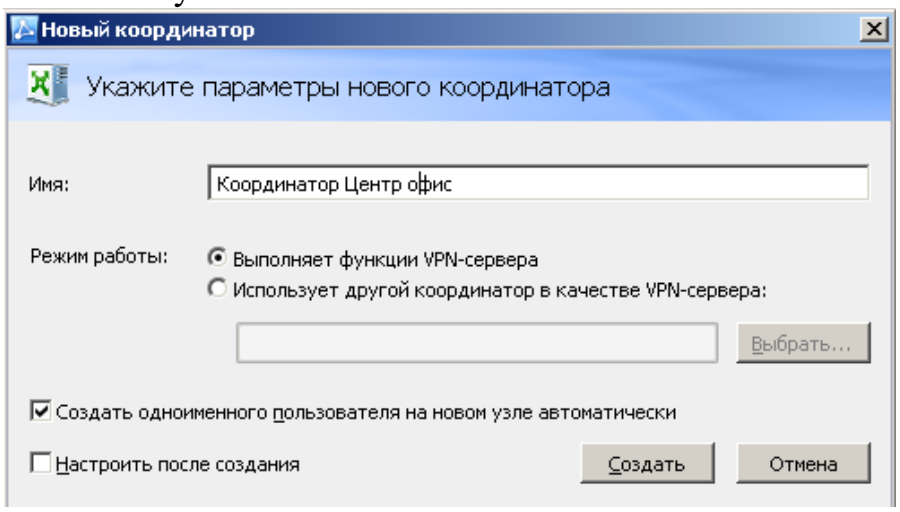

Рисунок 7 – Параметры нового координатора

Аналогичным образом создается сетевой узел *Координатор Филиал*.

После создания раздел *Координаторы* окна *ViPNet Центр управления сетью* представления *Моя сеть* будет иметь следующий вид *(Рисунок 19)*.

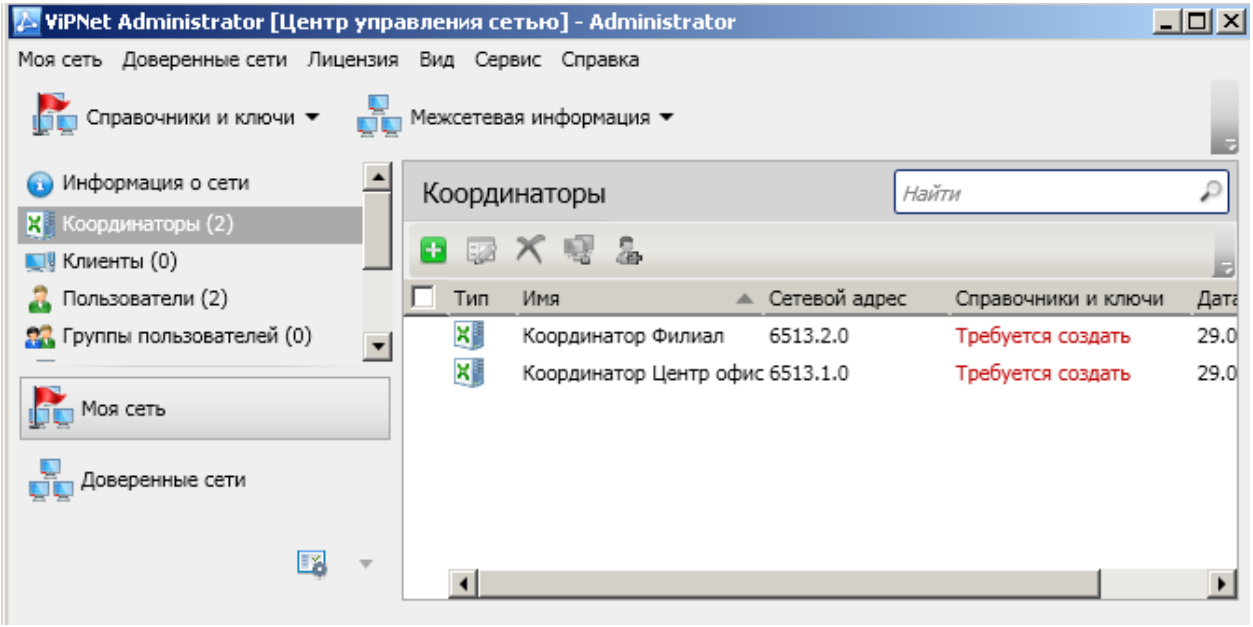

Рисунок 8 – Раздел *Координаторы* представления *Моя сеть*

Созданным координаторам автоматически назначаются роли *Программный VPN-координатор* и *Обмен сообщениями и файлами*. Чтобы убедиться в этом, зайдите в свойства координатора (двойной щелчок по выбранному координатору), вкладка *Роли узла (Рисунок 20)*.

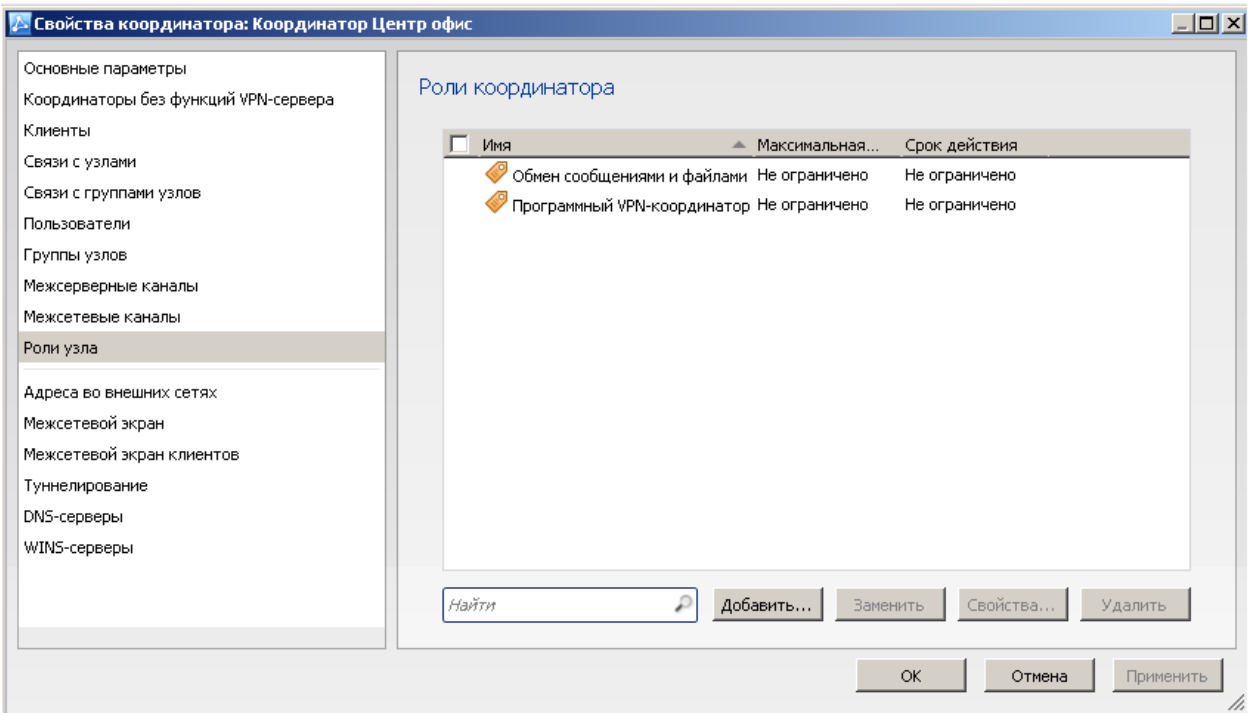

Рисунок 9 – Роли координатора

1.2.2. Создание клиентов

В соответствии со схемой развертывания ViPNet в сети компании необходимо создать клиенты: *Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис, Сотрудник_2 Филиал.*

Каждый клиент должен быть зарегистрирован на одном из координаторов. На сетевом узле *Координатор Центр офис* необходимо зарегистрировать следующие клиенты – *Главный администратор, Помощник глав админа, Сотрудник_1 Центр офис,* а на сетевом узле *Координатор Филиал - Сотрудник_2 Филиал.*

Чтобы добавить в сеть ViPNet нового клиента, выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел *Клиенты*.
3. В разделе *Клиенты* на панели инструментов нажмите кнопку *Создать*.
4. В появившемся окне задайте имя *Главный администратор*, выберите координатор *Координатор Центр офис* для регистрации на нем создаваемого клиента, уберите флажок *Создать одноименного пользователя* и нажмите кнопку *Создать (Рисунок 21)*. В данном случае снимать флажок требуется ввиду того, что как правило в компании требуется точно знать за каким узлом находится конкретный пользователь, тем более если на одном узле их несколько.

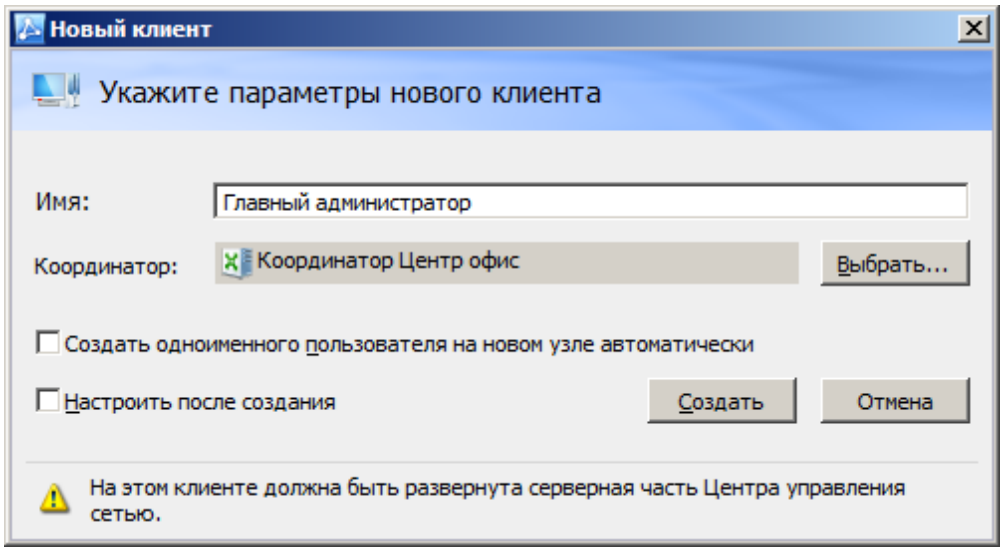

Рисунок 10 – Параметры нового клиента

Аналогичным образом создаются остальные клиенты.

После создания клиентов раздел *Клиенты* окна *ViPNet Центр управления сетью* представления *Моя сеть* будет иметь следующий вид *(Рисунок 22)*.

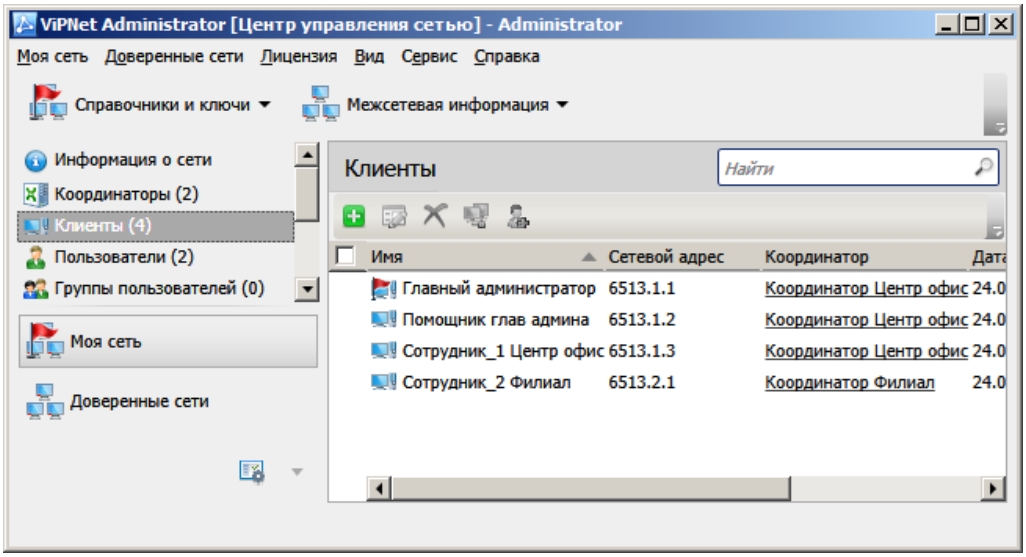

Рисунок 11 – Раздел *Клиенты* представления *Моя сеть*

Созданным клиентам автоматически назначаются роли *Business Mail*, *VPN-клиент* и *Обмен сообщениями и файлами*, а для первого созданного клиента, дополнительно, системные роли *Network Control Center* и *Policy Manager*. Чтобы убедиться в этом, зайдите в свойства клиента (двойной щелчок по выбранному узлу), вкладка *Роли узла*.

Теперь необходимо создать пользователей и зарегистрировать их на клиентах в соответствии с таблицей 3. Для этого выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите представление Моя сеть.
2. На панели навигации выберите раздел *Пользователи*.
3. В разделе *Пользователи* на панели инструментов нажмите кнопку *Создать*.
4. В появившемся окне задайте имя пользователя *Глав admin Петров*, выберите сетевой узел *Главный администратор* и нажмите кнопку *Создать (Рисунок 23)*.

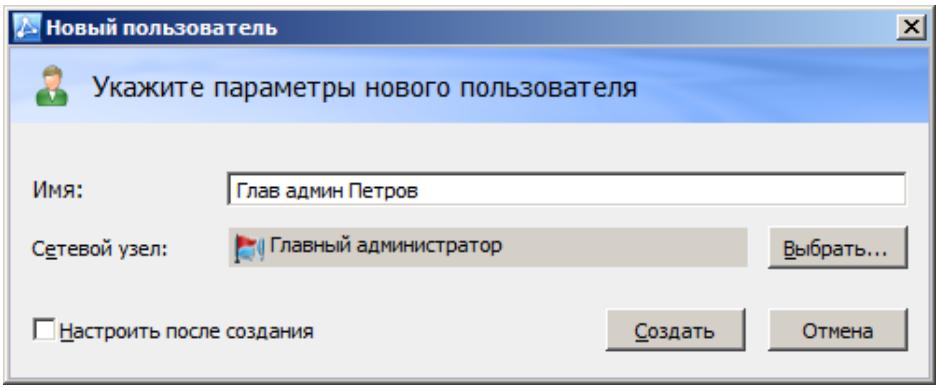

Рисунок 12 – Параметры пользователя

Аналогичным образом создаются пользователи для остальных узлов.

После создания пользователей и регистрации их на координаторах и клиентах раздел *Пользователи* окна *ViPNet Центр управления сетью* представления *Моя сеть* будет иметь следующий вид *(Рисунок 24)*.

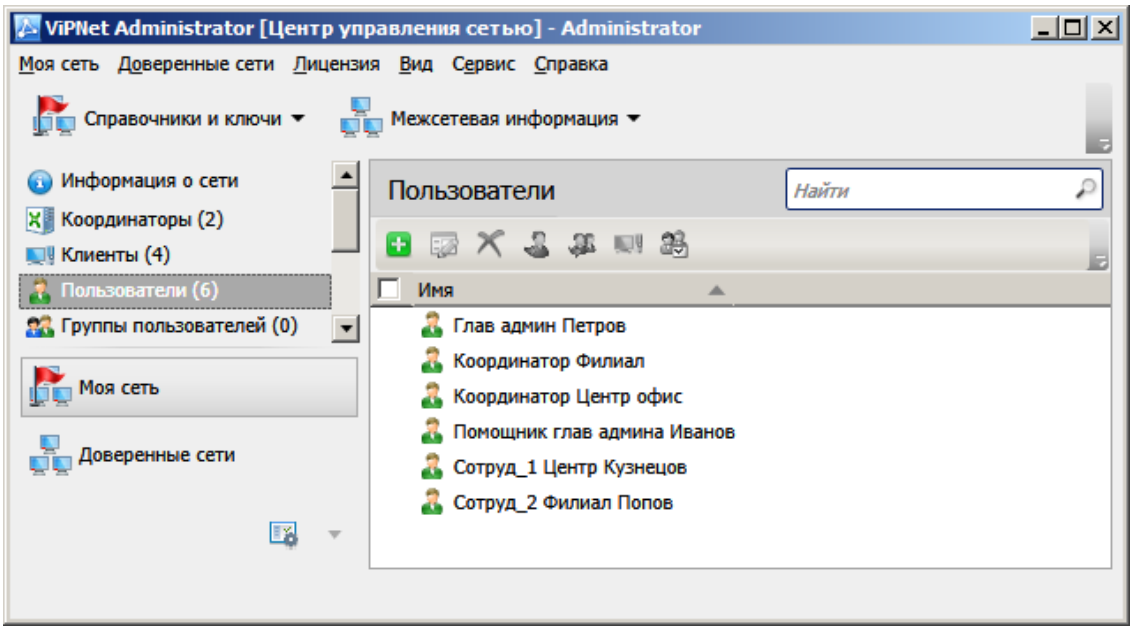

Рисунок 13 – Раздел *Пользователи* представления *Моя сеть*

1.2.3. Создание межсерверных каналов и связей

Межсерверный канал связывает два координатора и позволяет им выполнять функцию сервера-маршрутизатора – обмениваться управляющими и прикладными транспортными конвертами. Необходимо, чтобы все координаторы были связаны между собой напрямую или через другие координаторы, то есть должен существовать хотя бы один путь передачи служебной информации между двумя любыми координаторами. Можно связать все координаторы с одним центральным координатором (схема «звезда»), все координаторы между собой или использовать другие схемы.

Построим межсерверный канал между координаторами *Координатор Центр офис* и *Координатор Филиал*. Для этого выполните следующие действия:

1. Перейдите в свойства сетевого узла *Координатор Центр офис* (двойной щелчок по выбранному узлу).
2. На вкладке *Межсерверные каналы* нажмите кнопку *Добавить*.
3. В открывшемся окне выберите сетевой узел *Координатор Филиал* и нажмите кнопку *Добавить*. Вкладка *Межсерверные каналы* примет следующий вид *(Рисунок 25)*.

Теперь необходимо создать связи между пользователями в соответствии с матрицей связей пользователей защищенной сети (см. Таблицу 4).

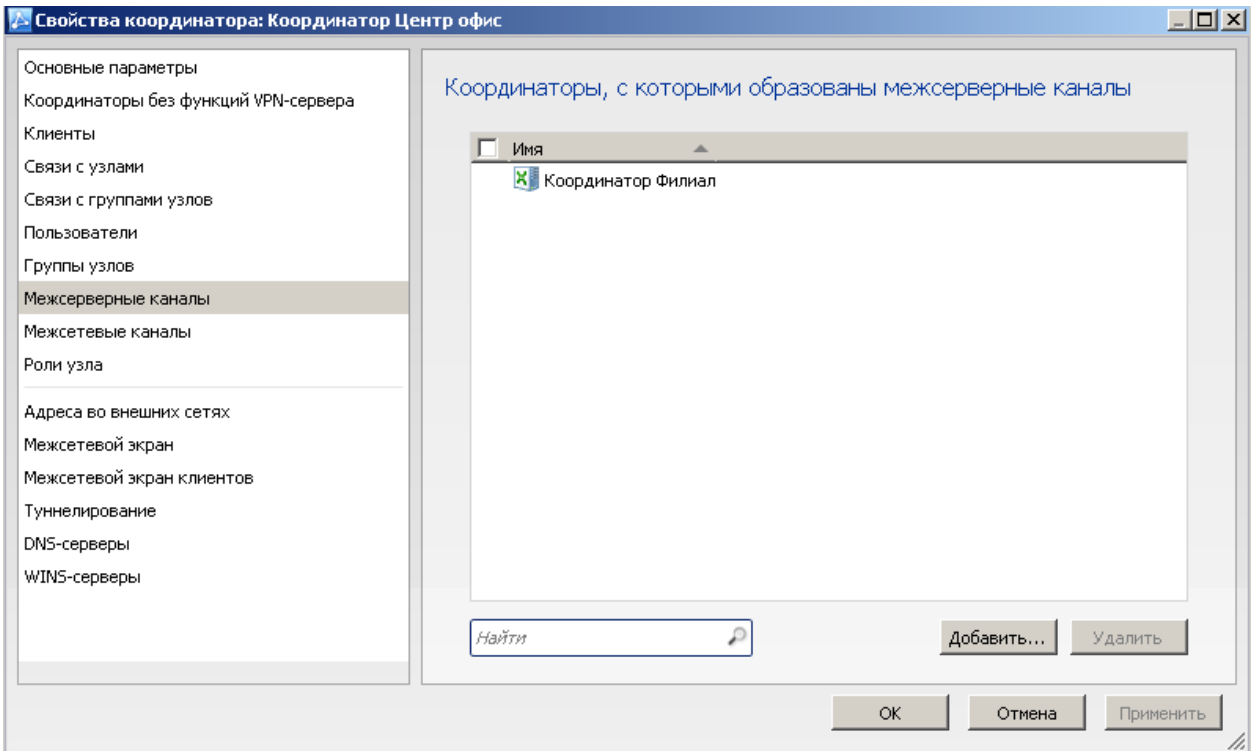

Рисунок 14 – Вкладка *Межсерверные каналы*

4. Перейдите в свойства пользователя *Координатор Центр офис* (двойной щелчок по выбранному узлу). Вкладка *Связи с пользователями* имеет следующий вид (на первоначальном этапе данный раздел пуст – *Рисунок 26*).

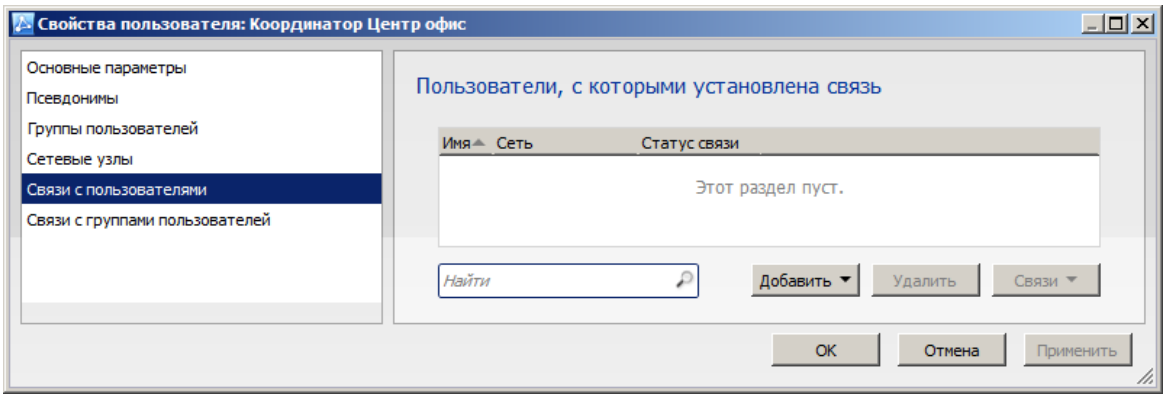

Рисунок 15 – Вкладка *Связи с пользователями*

5. Добавьте связь пользователя *Координатор Центр офис* с пользователем *Глав admin Петров*. Для этого на вкладке *Связи с пользователями* нажмите кнопку *Добавить* и выберите из списка пользователя *Глав admin Петров,* а также других в соответствии с матрицей связей пользователей.

После связывания пользователей вкладка *Связи с пользователями* для *Координатор Центр офис* будет иметь следующий вид *(Рисунок 27)*.

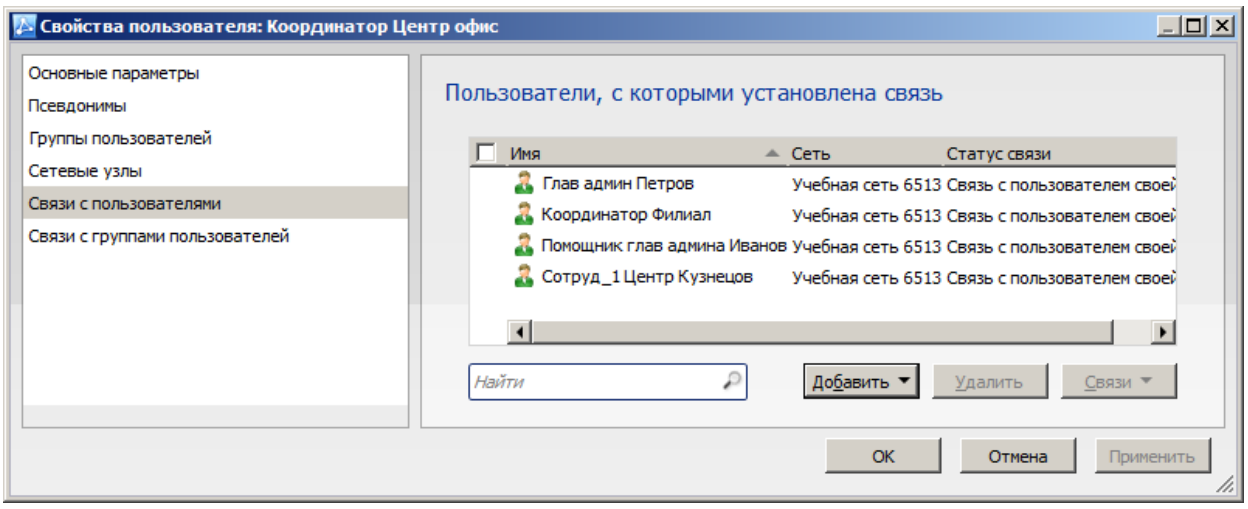

Рисунок 16 – Вкладка *Связи с пользователями* Координатора Центр офис

Аналогичным образом необходимо создать связи для других пользователей согласно матрице связей пользователей *(см. Таблицу 4)*.

После этого автоматически будут созданы связи между узлами, к которым относятся связанные пользователи. Вкладка *Связи с узлами* имеет следующий вид *(Рисунок 28)*.

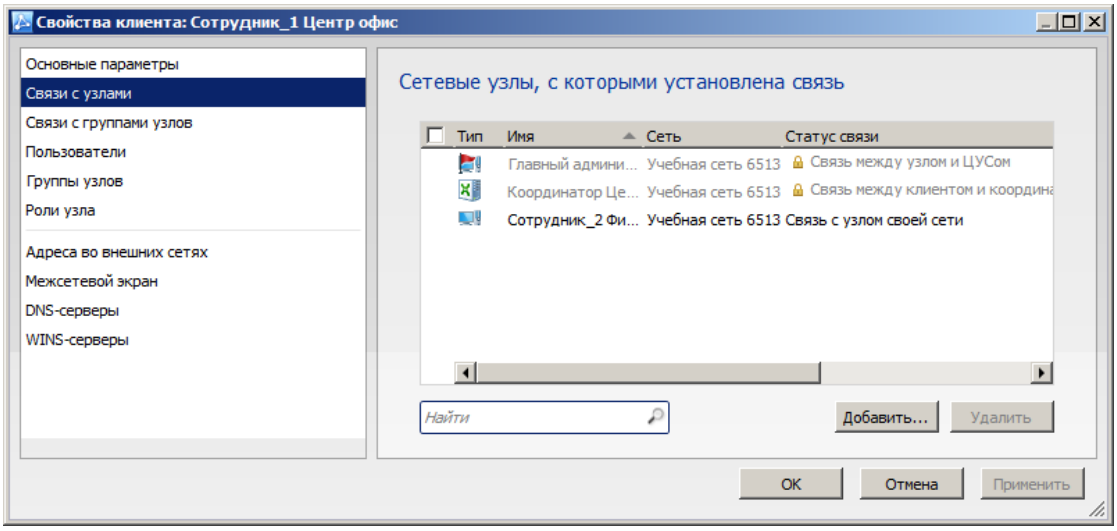

Рисунок 17 – Вкладка *Связи с узлами* клиента Сотрудник_1 Центр

	Примечание. Рекомендуется устанавливать в первую очередь связи между пользователями. Появиться возможность вести конфиденциальную переписку между конкретными пользователями, а не узлами.

6. Проверьте конфигурацию сети, выбрав в меню *Моя сеть* пункт *Проверить конфигурацию сети…* В случае, если сеть сконфигурирована верно, на экран будет выведено сообщение «Конфликтных или неполных данных не обнаружено».

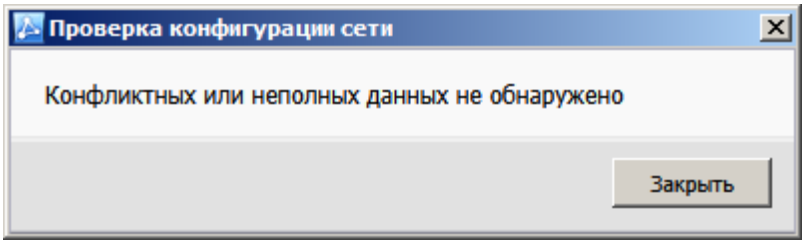

Рисунок 18 – Положительный результат проверки конфигурации сети

7. После проверки конфигурации сети необходимо подготовить данные для создания дистрибутивов в УКЦ. Для этого сформируйте справочники, выбрав в меню *Моя сеть* > *Создать справочники*. На экран будет выведено окно со списком узлов, для которых требуется создать справочники. Нажмите кнопку *Создать для всего списка*.

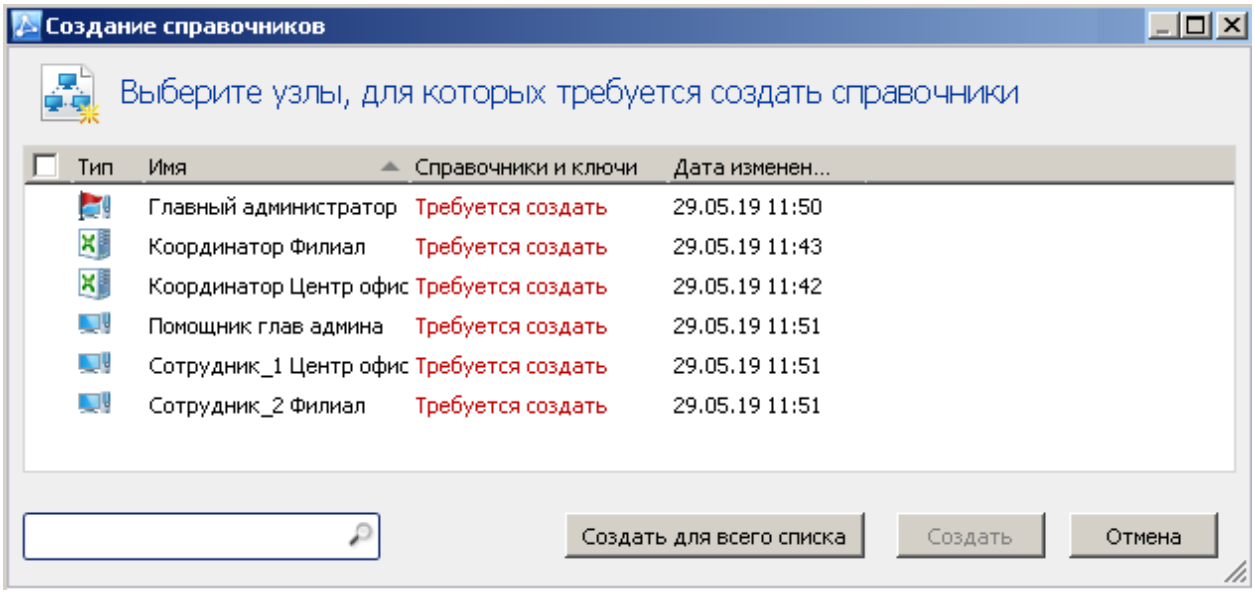

Рисунок 19 – Окно *Создание справочников*

Справочники содержат информацию о сетевых узлах, пользователях и их свойствах: идентификаторах, связях, ролях сетевых узлов, адресах и так далее.

После создания справочников можно перейти к первому запуску компонента *ViPNet Удостоверяющий и ключевой центр*.

1.2.4. Первый запуск программы ViPNet Удостоверяющий и ключевой центр

1. Чтобы начать работу с программой ViPNet Удостоверяющий и ключевой центр, выполните запуск программы с ярлыка на *Рабочем столе* или через меню *Пуск* > *Все программы* > *ViPNet* > *ViPNet Administrator* > *Удостоверяющий и ключевой центр*.
2. В окне *Начало работы с программой Удостоверяющий и ключевой центр* выберите *Настройка новой базы данных* и нажмите кнопку

Продолжить для запуска процедуры первичной инициализации (Рисунок 31).

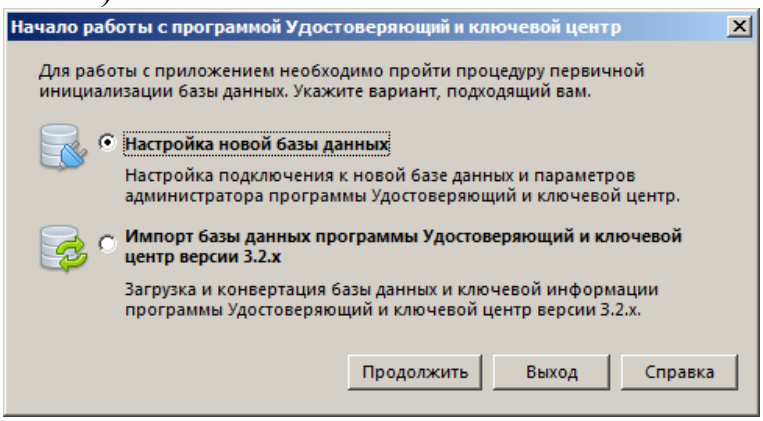

Рисунок 20 – Выбор базы данных

3. На первой странице мастера инициализации нажмите кнопку *Далее*.
4. На странице *Подключение к базе данных ViPNet Administrator* укажите сетевой адрес экземпляра SQL-сервера – *.\winnccsql* и имя базы данных – *ViPNetAdministrator* и нажмите кнопку *Далее (Рисунок 32)*.

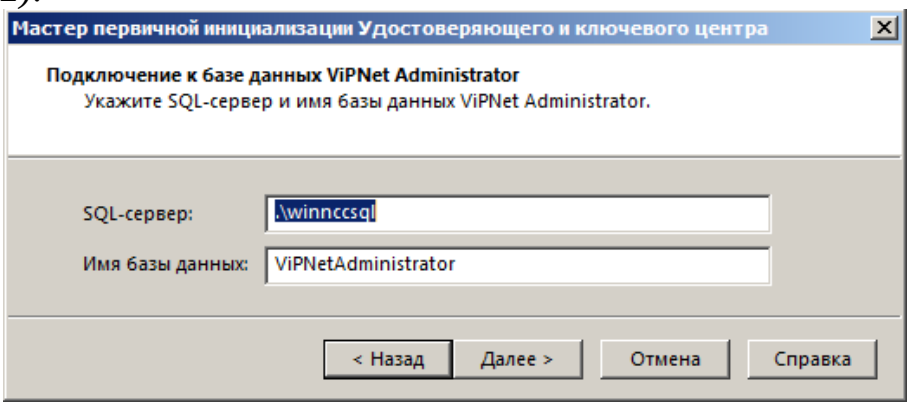

Рисунок 21 – Подключение к базе данных *ViPNet Administrator*

5. На следующей странице выберите тип проверки при подключении к SQL-серверу *По имени и паролю пользователя SQL-сервера*, укажите имя пользователя – *KcaUser*, пароль – *Number1* и нажмите кнопку *Далее (Рисунок 33)*.

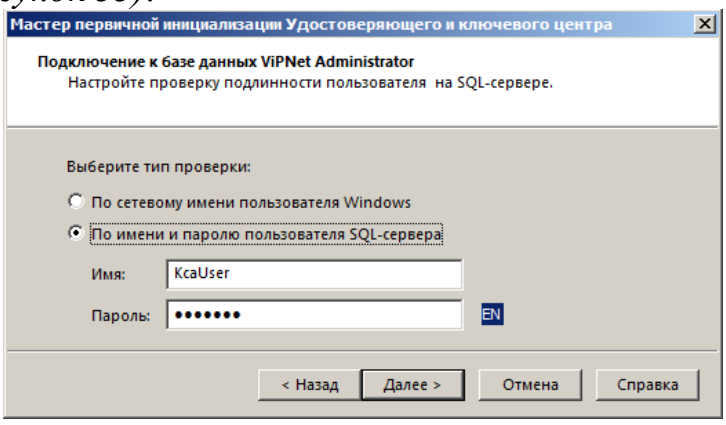

Рисунок 22 – Задание имени и пароля для подключения к SQL-серверу

6. Имя главного администратора ViPNet компании – *Владимир*. На странице *Создание администратора сети ViPNet* задайте имя учетной записи администратора УКЦ – *Владимир*, и нажмите кнопку *Далее*.

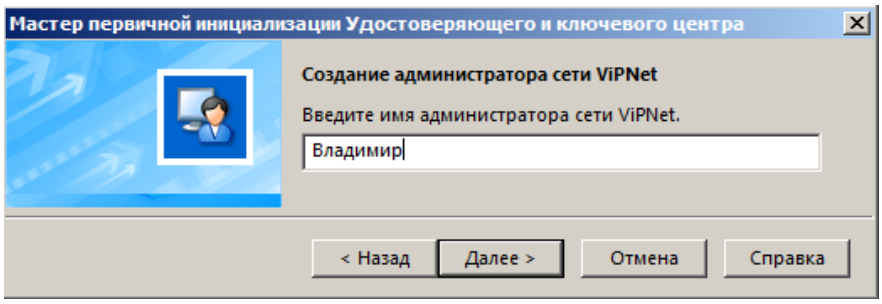

Рисунок 23 – Ввод имени администратора ViPNet

7. На страницах *Владелец сертификата* введите личные данные, которые будут указаны в сертификате ключа проверки электронной подписи главного администратора ViPNet в соответствии с рисунками ниже *(Рисунок 35,36,37)*.

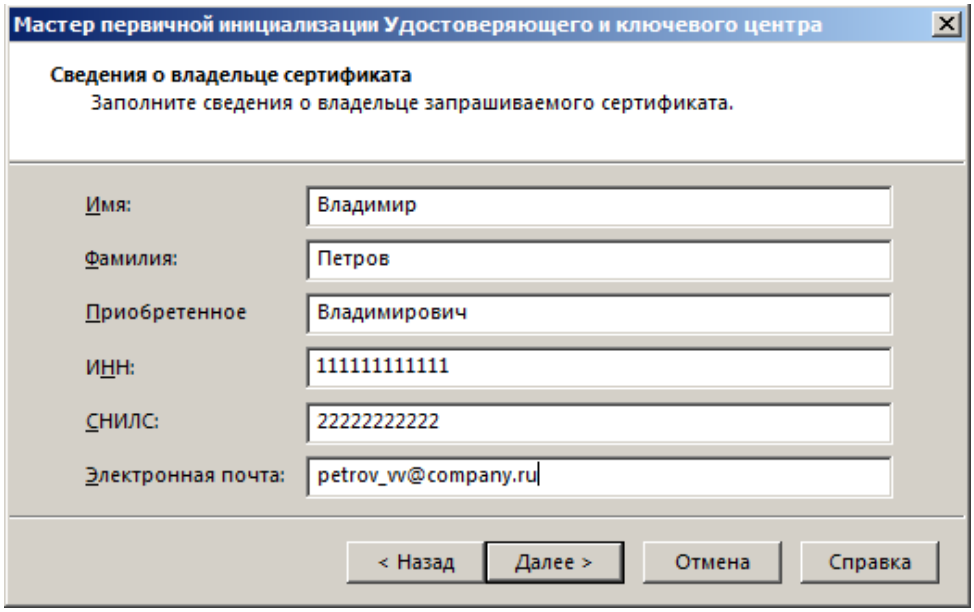

Рисунок 24 – Ввод данных для издания сертификата администратора ViPNet (часть 1)

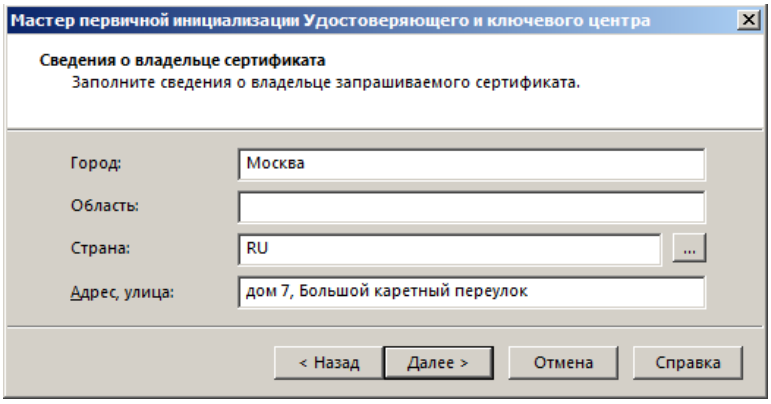

Рисунок 25 – Ввод данных для издания сертификата администратора ViPNet (часть 2)

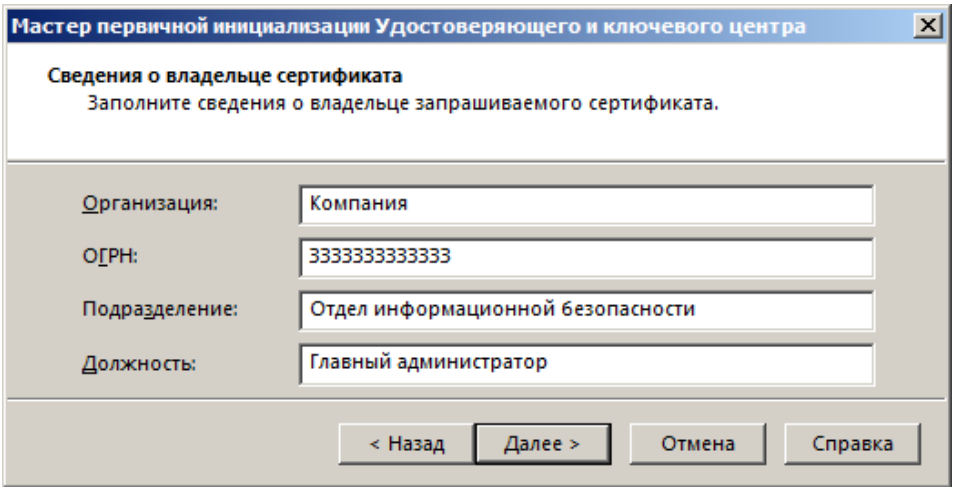

Рисунок 26 – Ввод данных для издания сертификата администратора ViPNet (часть 3)

8. На странице *Дополнительные сведения* о владельце сертификата нажмите кнопку *Далее*.
9. На странице *Параметры ключа электронной подписи* оставьте значения по умолчанию и нажмите кнопку *Далее*.

На странице *Место хранения контейнеров ключа подписи и ключа защиты УКЦ* выберите место хранения контейнера ключей администратора – *В файле*.

На странице *Срок действия сертификата* установите максимальное значение – 192 месяца с настоящего момента.

10. На странице *Программные средства*, в случае, если планируется осуществлять создание и выдачу квалифицированных сертификатов ключей проверки электронных подписей, указываются программные продукты, используемые в качестве средства электронной подписи издателя, средства электронной подписи владельцев сертификатов и средства удостоверяющего центра.

	**Внимание.** В рамках настоящего практического задания функционирование продуктов ViPNet в качестве аккредитованного удостоверяющего центра не рассматривается, поэтому флажок «Функционировать в качестве аккредитованного удостоверяющего центра» устанавливать не нужно.

11. На странице *Автоматический режим работы* нажмите кнопку *Далее*.

В зависимости от выбранного места хранения будет определен срок действия ключа электронной подписи. При хранении ключа электронной подписи в файле на компьютере либо на внешнем устройстве, которое не поддерживает алгоритм ГОСТ 34.10-2001, срок действия ключа ограничивается одним годом. Если ключ электронной подписи хранится на устройстве с поддержкой ГОСТ 34.10-2001 (был непосредственно сформирован на нем), то его срок действия составляет 3 года. Под сроком действия понимается срок использования ключа электронной подписи для

подписи издаваемых сертификатов пользователей. При этом список аннулированных сертификатов может быть подписан и по истечении срока действия ключа электронной подписи.

12. На странице *Настройка паролей* выберите тип создаваемого пароля – *Собственный пароль*, способ выдачи пароля пользователя – *Сохранять пароль в файл XPS в папку* (рекомендуется запомнить путь к данной папке или заменить на собственный, в дальнейшем его можно будет изменить на вкладке *Сервис→Настройка…→Пароли*), нажмите кнопку *Далее*. На появившейся странице задайте пароль администратора сети ViPNet – 11111111 (восемь единиц) *(Рисунок 38)*.

	Примечание 1. В реальной ситуации, при настройке и формировании сети рекомендуется руководствоваться существующими правилами парольной безопасности или применять сгенерированные встроенными средствами ViPNet пароли достаточной сложности. **Примечание 2.** При выполнении практических занятий рекомендуется использовать простые запоминающиеся пароли во всех программах (например, 11111111 (восемь единиц))

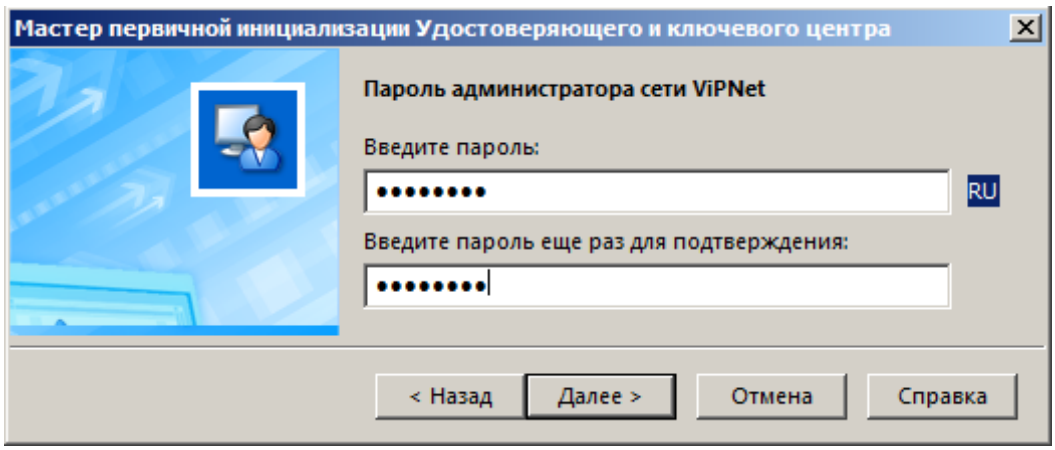

Рисунок 27 – Задание пароля администратора

13. На странице готовности к завершению первичной инициализации убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки *Назад*.
14. Для продолжения работы нажмите кнопку *Далее*. Поводите указателем в пределах окна *Электронная рулетка (Рисунок 39)* и после успешного завершения инициализации нажмите кнопку *Закрыть*.

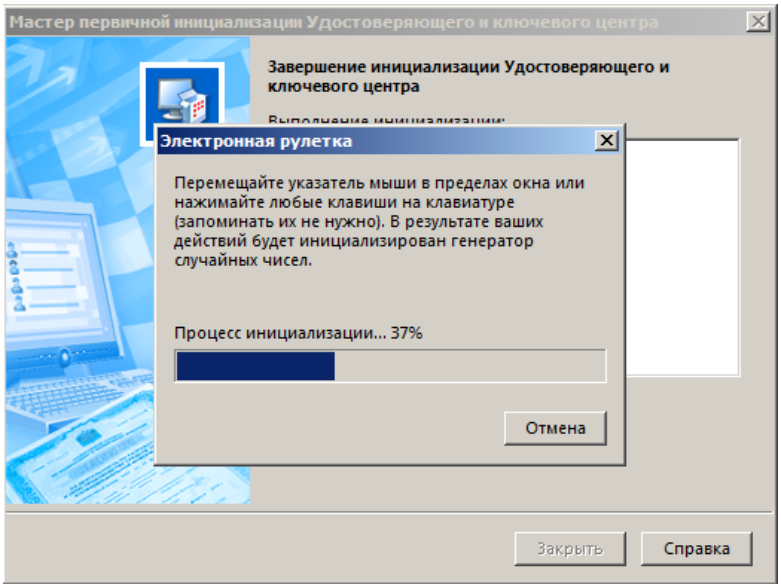

Рисунок 28 – Окно *Электронная рулетка*

При успешном проведении первичной инициализации будут выполнены следующие операции:

- 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 (*Рисунок 40)*.

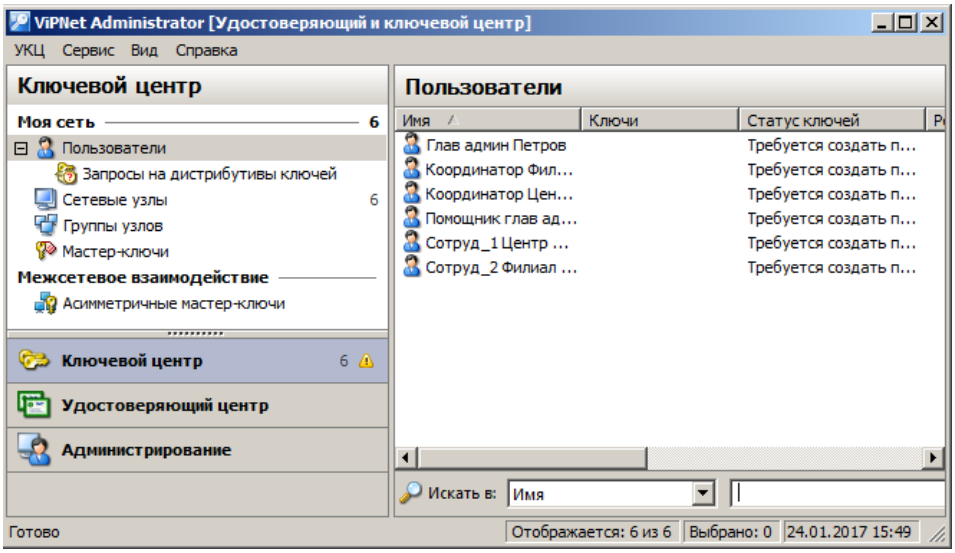

Рисунок 29 – Главное окно УКЦ

Перед началом работы в УКЦ проверьте первоначальные настройки программы. В меню *Сервис* выберите пункт *Настройка*. В открывшемся окне в разделе *Пароли* установите тип пароля, который будет использоваться при создании новых паролей, – *Собственный пароль*, а на вкладке *Сертификаты*

снимите флажки *Редактировать поля сертификатов при издании* и *Создавать ключи электронной подписи*.

После проверки первоначальных настроек необходимо снять вручную флажок *Создавать ключи электронной подписи* в свойствах пользователей (*УКЦ>Моя сеть>Пользователи*, кликнуть правой кнопкой мыши на пользователя и выбрать пункт *Ключи пользователя>Создавать ключи электронной подписи*).

Теперь можно приступить к созданию дистрибутивов ключей.

	**Примечание.** В разделе Сервис → Настройка…→ Сертификаты, стоит обратить внимание на второй пункт: *Создавать ключи электронной подписи*. В случае, если в вашей сети для большинства узлов (клиентов) требуется выпуск электронной подписи и сертификата проверки электронной подписи (например, для обеспечения юридически значимого электронного документооборота), то рекомендуется оставить данный флажок включенным. Но главное не забывать снимать вручную данный флажок в свойствах конкретного пользователя, которому не нужно выпускать электронную подпись (*УКЦ→Моя сеть→Пользователи*, кликнуть правой кнопкой мыши на пользователя которому не нужно формировать ЭП выбрать пункт *Ключи пользователя→Создавать ключи электронной подписи*). В ином случае, рекомендуется снять галочку в настройках УКЦ, тогда ключи электронной подписи не будут формироваться для всех новых узлов, добавляемых в сеть. Также стоит учесть тот факт, что для координаторов нет необходимости создавать ЭП, поэтому сразу же рекомендуется снять данную галочку для всех координаторов в сети. В противном случае при каждом обновлении ключей будет создаваться новая ЭП и сертификат проверки ЭП.

1.2.5. Выдача дистрибутивов ключей

	**Примечание.** В процессе создания структуры сети для сетевых узлов необходимо задавать не только пароли пользователя, но и пароли администратора сетевых узлов, так как это необходимо на случай, если нужно будет разграничить доступ лиц, осуществляющих настройку на конкретном сетевом узле (локальный администратор информационной безопасности). Также есть возможность разграничить доступ на уровне групп узлов, в данном случае все узлы, входящие в конкретную группу, могут запускаться в режиме администратора с использованием пароля администратора данной группы. При создании сети ViPNet в ЦУСе автоматически создается группа «Вся сеть», в которую входят все узлы данной сети ViPNet. При первом запуске УКЦ в обязательном порядке задается пароль администратора сетевых узлов группы «Вся сеть». Данную группу нельзя удалить, а пароль, присвоенный данной группе, может быть использован для запуска ПО ViPNet на любом узле в режиме администратора.
	**Внимание!** Пароли администратора (группы или узла) нельзя передавать или каким-либо образом сообщать пользователю узла. Данный тип паролей предназначен исключительно для администрирования конкретного узла или группы узлов и может быть сообщен только лицу, ответственному за настройку и контроль работоспособности средств криптографической защиты информации

	(например, локальному администратору по информационной безопасности, назначенному внутренним приказом по организации).

Дистрибутивы ключей необходимы для активации программных продуктов ViPNet (ViPNet Client, ViPNet Coordinator, ViPNet Policy Manager и т.д.) на сетевых узлах защищенной сети.

Если на сетевом узле зарегистрировано несколько пользователей, то для каждого пользователя узла будет сформирован свой дистрибутив.

Для выдачи дистрибутивов ключей выполните следующие действия:

1. В окне программы *ViPNet Удостоверяющий и ключевой центр* на панели навигации выберите представление *Ключевой центр* и перейдите в раздел *Моя сеть* > *Сетевые узлы*.
2. Задайте пароль администратора для всех созданных сетевых узлов. Для этого двойным щелчком откройте *Свойства сетевого узла*, перейдите на вкладку *Пароль администратора*, нажмите кнопку *Создать пароль…>Тип пароля: Собственный> Пароль: 11111111* (при создании паролей администраторов в реальной сети следует руководствоваться парольными политиками компании, а также делать его отличным от пароля пользователя).
3. Выделите все сетевые узлы. В контекстном меню выберите пункт *Выдать новый дистрибутив ключей…(Рисунок 41).*

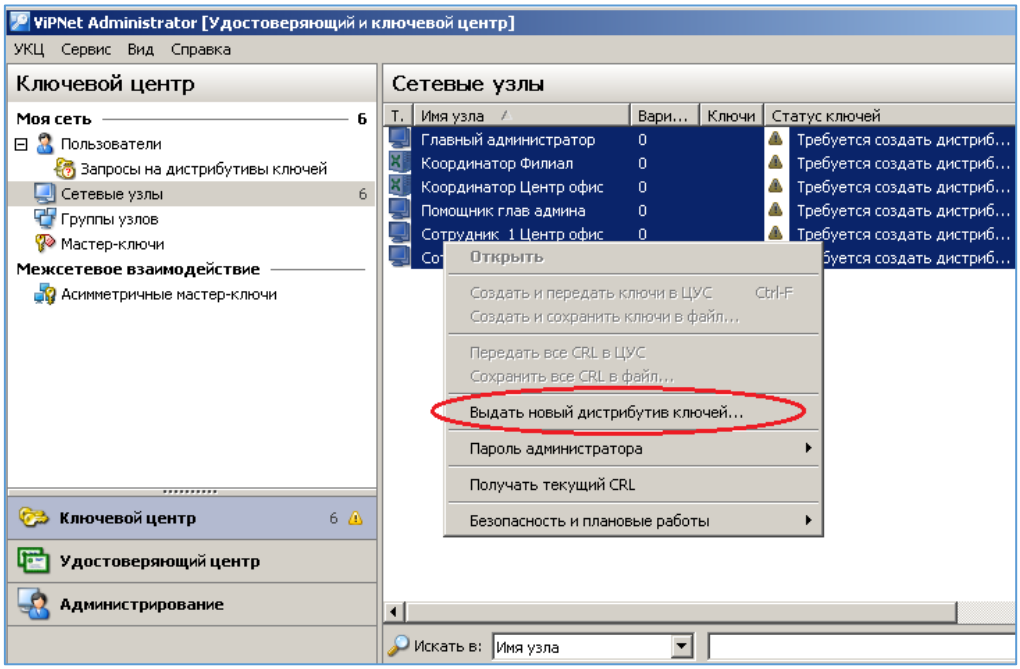

Рисунок 30 – Выдача дистрибутивов ключей

4. Задайте пароль пользователя – *11111111* по очереди для каждого пользователя защищенной сети *(Рисунок 42)*.

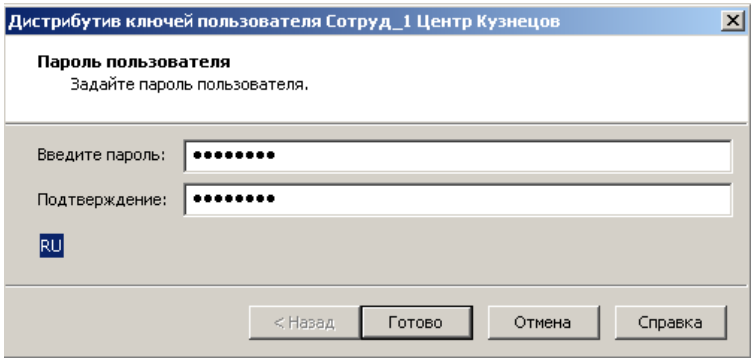

Рисунок 31 – Задание пароля пользователя

После окончания выдачи дистрибутива откроется окно проводника с папкой, содержащей подпапки сетевых узлов с готовыми дистрибутивами *(Рисунок 43)*. Запомните путь до этой папки или измените папку, используемую по умолчанию для сохранения дистрибутивов на собственную (*Сервис→Настройка…→Дистрибутивы ключей*). Путь до папки с дистрибутивами ключей понадобиться в дальнейшем для установки и активации ПО ViPNet.

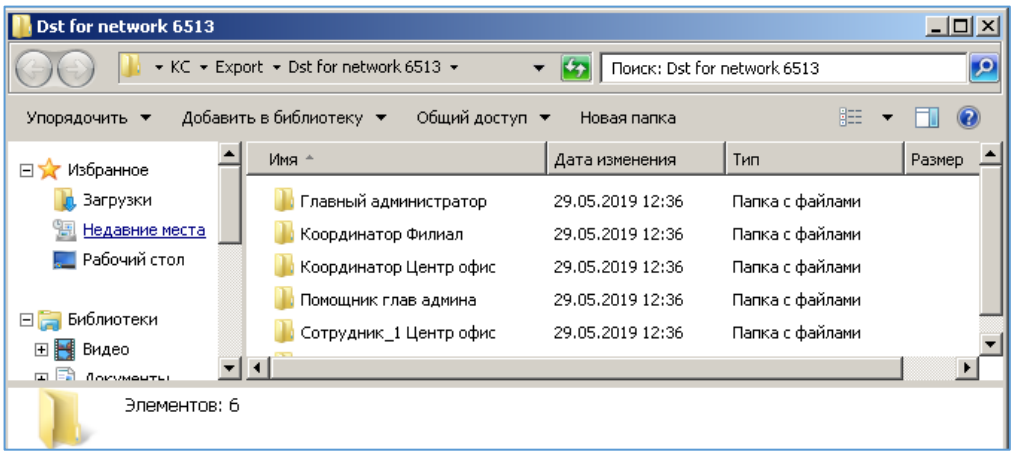

Рисунок 32 – Папка с дистрибутивами ключей

Администратор УКЦ должен доверенным путем (например, с помощью спец- или фельдъегерской связи, отправки на существующий сетевой узел с помощью программы ViPNet Client или лично в руки по доверенности) передать пользователю следующее:

- Дистрибутив ключей (*dst*-файл).
- Пароль пользователя.