

Практическое занятие 1. Развертывание защищенной сети ViPNet

СОДЕРЖАНИЕ ПРАКТИЧЕСКОГО ЗАНЯТИЯ

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

Для выполнения первого практического задания нам понадобятся две виртуальные машины VM_1 и VM_2 (рис. 4). На каждой из виртуальных машин должно быть поднято по 1-му сетевому адаптеру, находящимся в одной подсети.

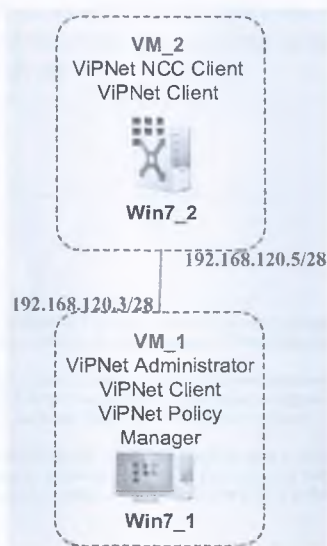


Рис. 4. Схема стенда для Практического занятия 1

Задание 1.1. Установка ПК ViPNet Administrator 4

Формулировка задания. Установить все компоненты ViPNet Administrator 4 на одно рабочее место VM_1.



Примечание. Перед установкой компонентов ViPNet необходимо убедиться в соответствии узла (персонального компьютера/сервера/виртуальной машины) системным требованиям.

В случае если узел, на котором запланирована установка компонентов ViPNet, не соответствует системным требованиям, его необходимо переконфигурировать. В противном случае корректная работа и правильность выполнения практических заданий не гарантирована. С системными требованиями для каждого из компонентов можно ознакомиться в разделе Справочная информации или в технической документации (портал документации ViPNet – <http://docs.infotecs.ru>)

1.1.1. Установка серверного приложения ViPNet Центр управления сетью

1. Для установки серверного приложения ViPNet Центр управления сетью откройте файл *Setup.exe* из каталога серверного приложения ViPNet Administrator.

2. В окне *Установка ViPNet Administrator Центр управления сетью* будет предложено установить дополнительное программное обеспечение. Список необходимого дополнительного программного обеспечения зависит от ранее установленных на компьютер программ. Чтобы начать установку, нажмите кнопку *Продолжить* (рис. 5).

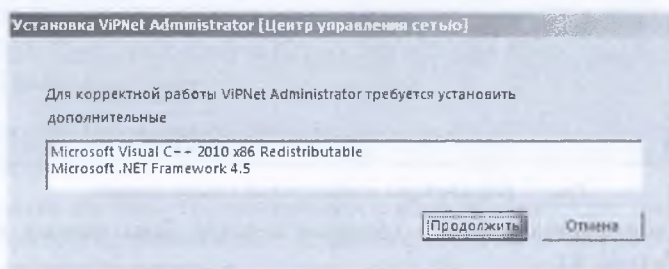


Рис. 5. Установка дополнительного программного обеспечения

3. В появившемся окне выберите язык для программы ViPNet Центр управления сетью и нажмите *Продолжить* (рис. 6).

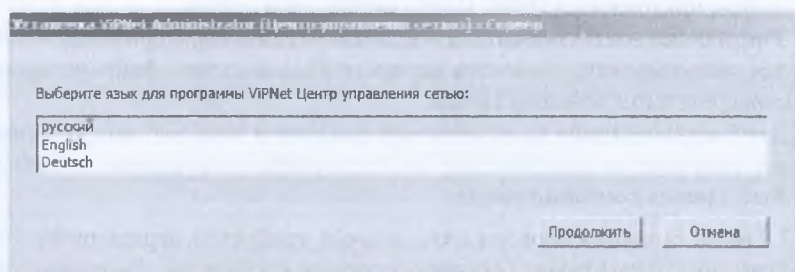


Рис. 6. Выбор языка программы

4. На странице *Лицензионное соглашение* ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку *Продолжить*.

5. На странице *Установка продукта* задайте параметры подключения к базе данных. Если вы не укажете имя существующего SQL-сервера, то на компьютере будет установлен SQL-сервер из комплекта поставки и создан именованный экземпляр с именем *WINNCCSQL*. При необходимости вы можете задать другое имя экземпляра. В рамках выполнения практического задания изменять параметры подключения не требуется. Нажмите кнопку *Продолжить* (рис. 7) и, в следующем окне, *Установить сейчас*.

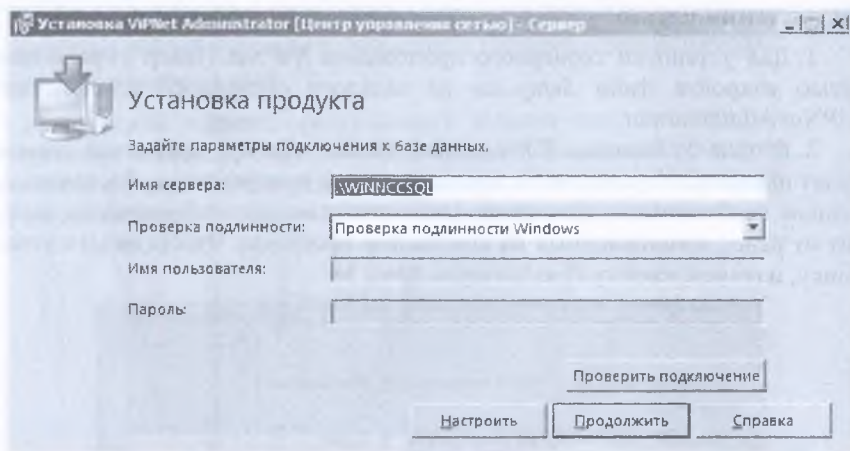


Рис. 7. Параметры подключения к базе данных

6. В появившемся окне о создании сервера базы данных нажмите кнопку *Да* (рис. 8).

При этом на SQL-сервере будут созданы:

- База данных с именем *ViPNetAdministrator*.
- База данных с именем *ViPNetJournals*, в которой хранятся журналы аудита программы *ViPNet Центр управления сетью*.
- Учетная запись пользователя с правами администратора базы данных для пользователя, от имени которого был запущен файл установки серверного приложения ЦУСа.
- Две учетные записи пользователей *KcaUser* и *NccUser*, под которыми осуществляется подключение УКЦ и серверного приложения ЦУСа к базе данных соответственно.

7. После создания сервера базы данных требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку. После перезагрузки установка серверного приложения ЦУСа будет продолжена автоматически. Если после перезагрузки установка серверного приложения не продолжилась автоматически, необходимо самостоятельно запустить *Setup.exe* из каталога серверного приложения

ViPNet Administrator (это необходимо для завершения установки серверного приложения, так как до перезагрузки были установлены только дополнительные компоненты и SQL-сервер).

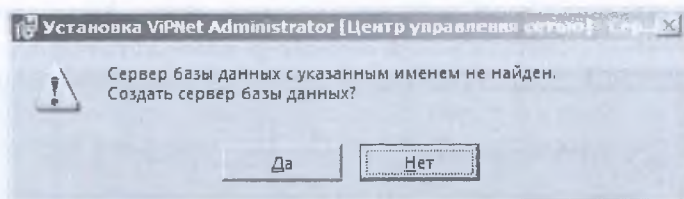


Рис. 8. Создание сервера базы данных

8. В появившемся окне выберите язык для программы ViPNet Центр управления сетью и нажмите *Продолжить*.

9. На странице *Установка продукта* нажмите кнопку *Продолжить*.

10. В появившемся окне проверьте выбранные параметры установки. Чтобы начать установку, нажмите кнопку *Установить сейчас*.

11. По завершении установки нажмите кнопку *Закреть*.

В результате серверное приложение ЦУСа будет установлено на компьютер. Далее можно приступить к установке клиентского приложения ЦУСа.

1.1.2. Установка клиентского приложения ViPNet Центр управления сетью

В рамках настоящего практического задания клиентское приложение ViPNet Центр управления сетью устанавливается на то же рабочее место, что и серверное приложение.

1. Для установки клиентского приложения ViPNet Центр управления сетью откройте файл *Setup.exe* из каталога клиентского приложения ViPNet Administrator.

2. В появившемся окне выберите язык для клиентского приложения ViPNet Центр управления сетью и нажмите *Продолжить* (рис. 9).

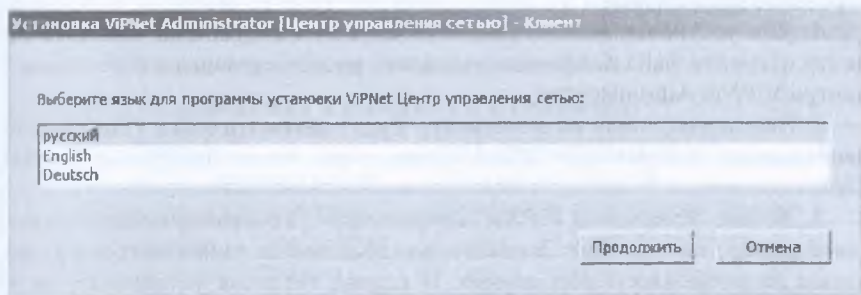


Рис. 9. Выбор языка программы

3. На странице *Лицензионное соглашение* ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку *Продолжить*.

4. На странице *Способ установки* нажмите кнопку *Установить сейчас* (рис. 10).

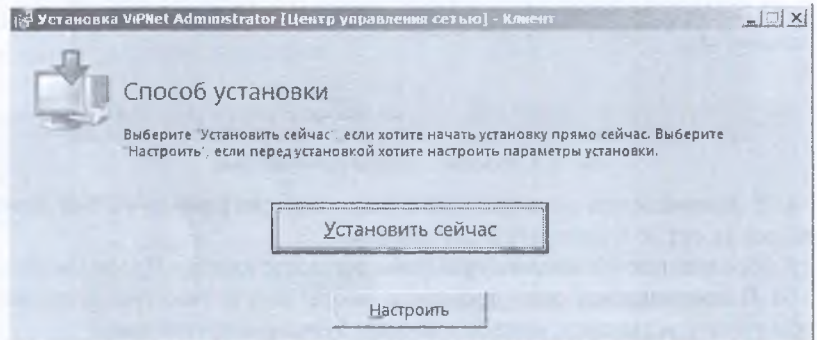


Рис. 10. Способ установки

Если требуется настроить параметры установки, то нажмите кнопку *Настроить* на странице *Способ установки* и укажите:

- путь к папке установки программы на компьютере;
- имя пользователя и название организации;
- название папки программы и ее расположение в меню *Пуск*.

5. По завершении установки нажмите кнопку *Закреть*.

В результате клиентское приложение ЦУСа будет установлено на компьютер. Далее можно приступить к установке ViPNet Удостоверяющий и ключевой центр.

1.1.3. Установка ViPNet Удостоверяющий и ключевой центр

В рамках настоящего практического задания ViPNet Удостоверяющий и ключевой центр устанавливается на то же рабочее место, что и серверное приложение.

1. Для установки компонента ViPNet Удостоверяющий и ключевой центр откройте файл *Setup.exe* из каталога удостоверяющего и ключевое центра ViPNet Administrator.

2. Подождите, пока на компьютер будет автоматически установлено необходимое программное обеспечение, в том числе программа ViPNet CSP.

3. В окне *Установка ViPNet Administrator [Удостоверяющий и ключевой центр]* на странице *Лицензионное соглашение* ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку *Продолжить*.

4. На странице *Способ установки* нажмите кнопку *Установить сейчас*.

5. Если потребуется настроить параметры установки, то нажмите кнопку *Настроить* (рис. 11) на странице *Способ установки* и укажите:

- путь к папке установки программы на компьютере;
- имя пользователя и название организации;
- название папки программы и ее расположение в меню *Пуск*.

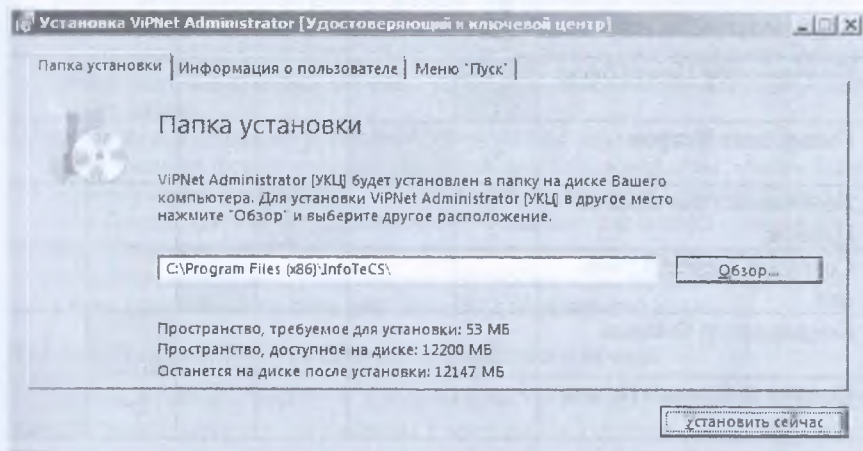


Рис. 11. Настройка установки

6. По окончании установки нажмите кнопку *Заккрыть*.

После установки УКЦ потребуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Выполните перезагрузку.

Теперь можно начинать работу с ПО ViPNet Administrator 4.

Задание 1.2. Создание структуры защищенной сети

Формулировка задания. Создать структуру защищенной сети в соответствии с заданной схемой (см. рис. 2, табл. 3), настроить связи пользователей (в соответствии с матрицей связей, табл. 4) в ЦУС и сформировать дистрибутивы ключей для сетевых узлов в УКЦ.

Таблица 3. 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 4. 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 Кузне- цов	+					+
Координатор Филиал	+					+
Сотруд_2 Филиал Попов				+	+	

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.

Примечания:

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.
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

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* (рис. 12).

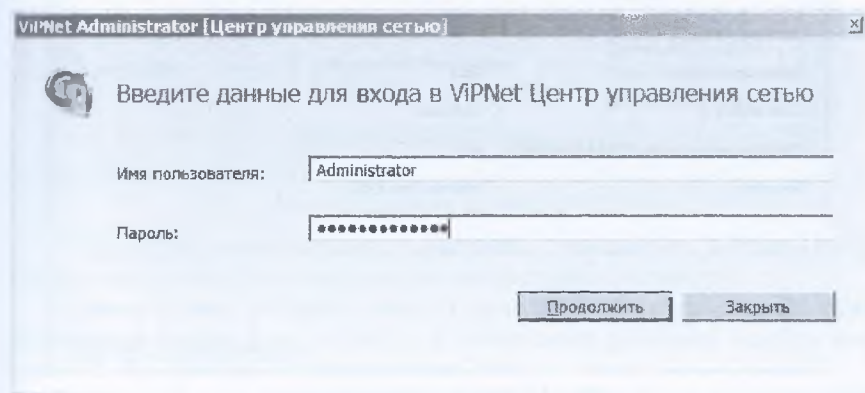


Рис. 12. Ввод имени пользователя и пароля

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 спо-

собы их устранения раздела Справочная информация или одноименному разделу в технической документации.

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 (рис. 13).

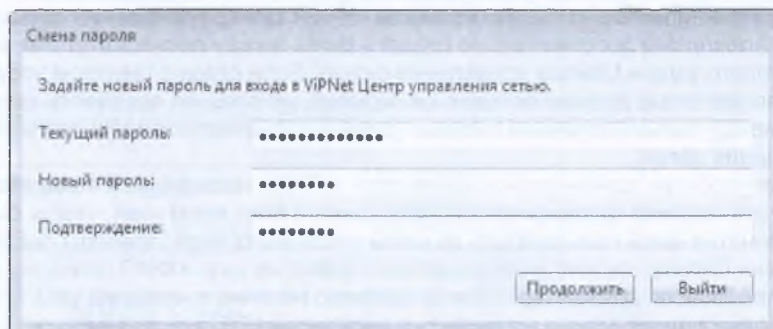


Рис. 13. Смена пароля

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* (рис. 14).

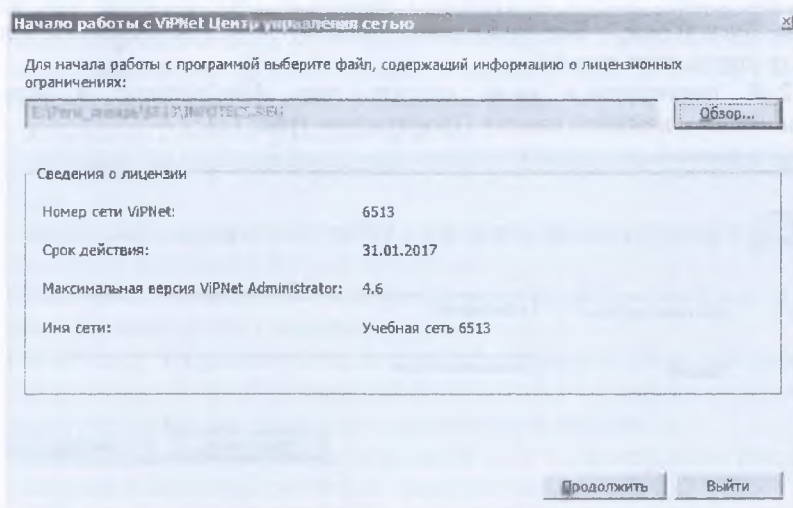


Рис. 14. Выбор файла лицензии

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

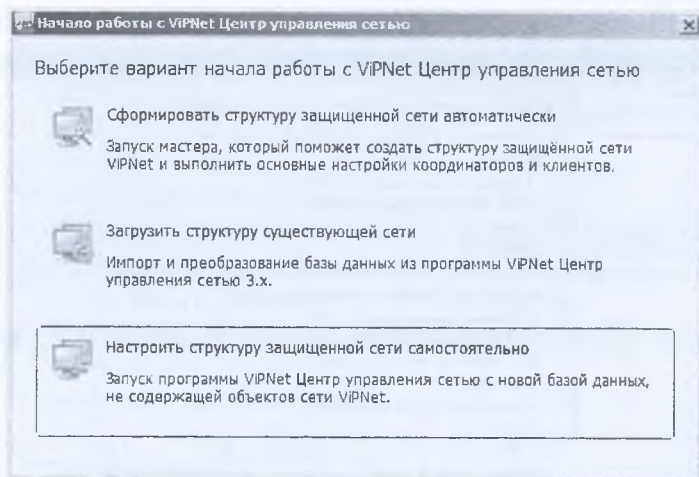


Рис. 15. Выбор варианта начала работы с ЦУС

6. Откроется главное окно программы (рис. 16).

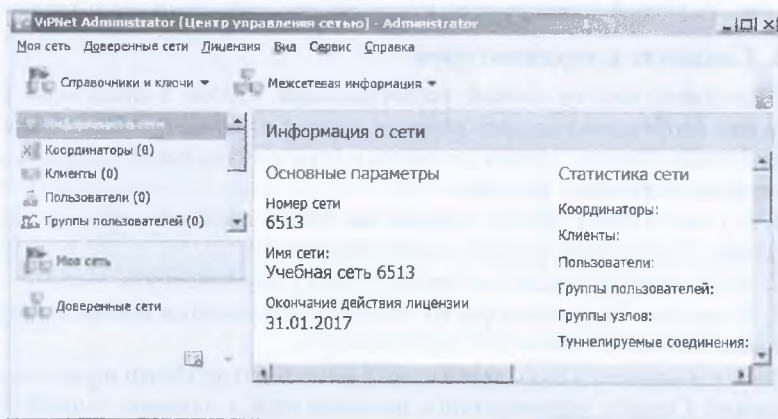


Рис. 16. Вид главного окна ЦУС

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 рис. 17.

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

Теперь можно приступить к созданию структуры защищенной сети.

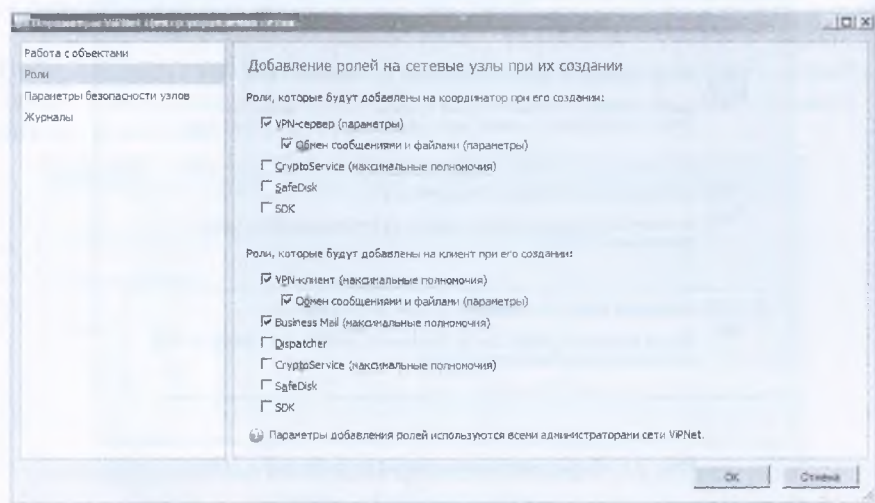


Рис. 17. Окно Параметры программы ViPNet Центр управления сетью

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).

Аналогичным образом создается сетевой узел *Координатор Филиал*.

После создания раздел *Координаторы* окна ViPNet Центр управления сетью представления *Моя сеть* будет иметь вид рис. 19.

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

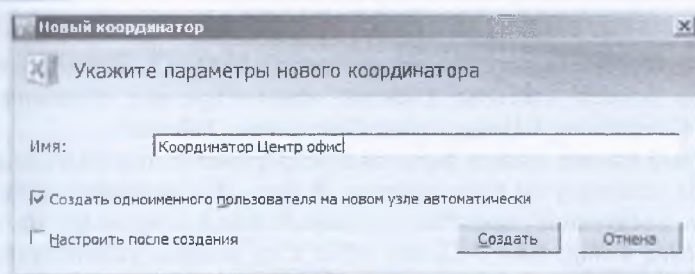


Рис. 18. Параметры нового координатора

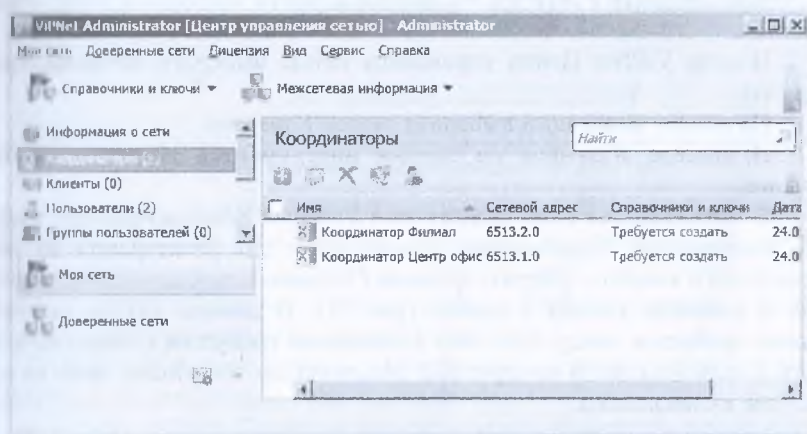


Рис. 19. Раздел Координаторы представления Моя сеть

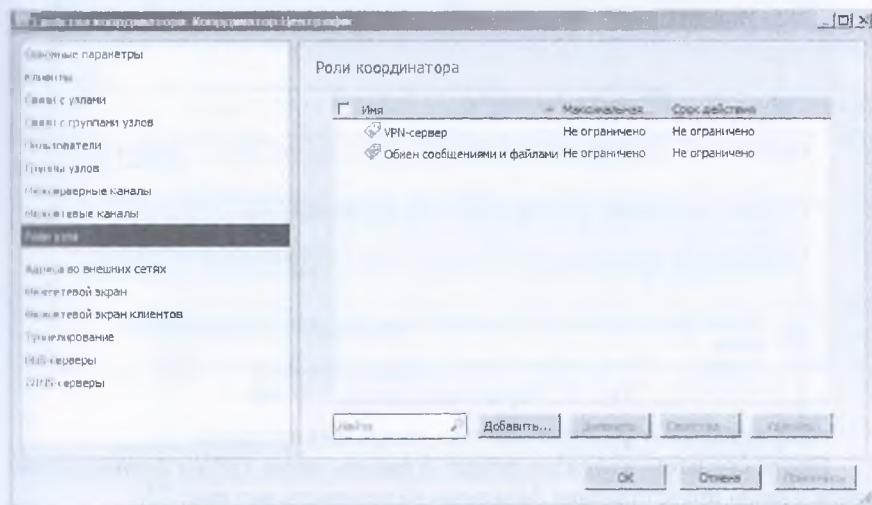


Рис. 20. Роли координатора

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* (рис. 21). В данном случае снимать флажок требуется ввиду того, что в компании требуется точно знать, за каким узлом находится конкретный пользователь, тем более, если на одном узле их несколько.

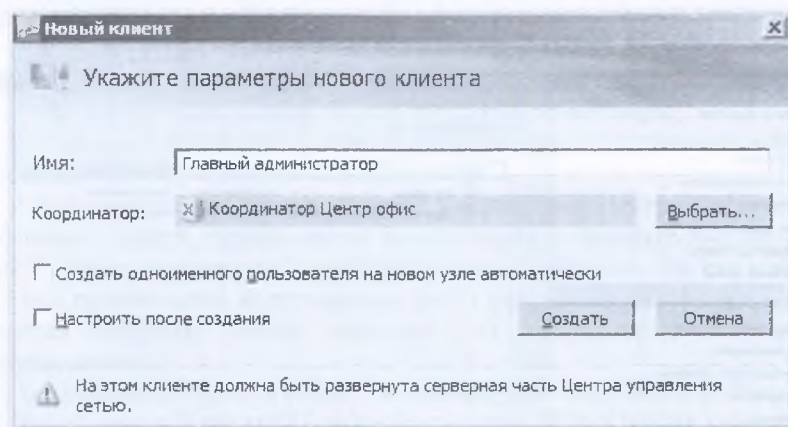


Рис. 21. Параметры нового клиента

Аналогичным образом создаются остальные клиенты.

После создания клиентов раздел *Клиенты* окна *ViPNet Центр управления сетью* представления *Моя сеть* будет иметь вид рис. 22.

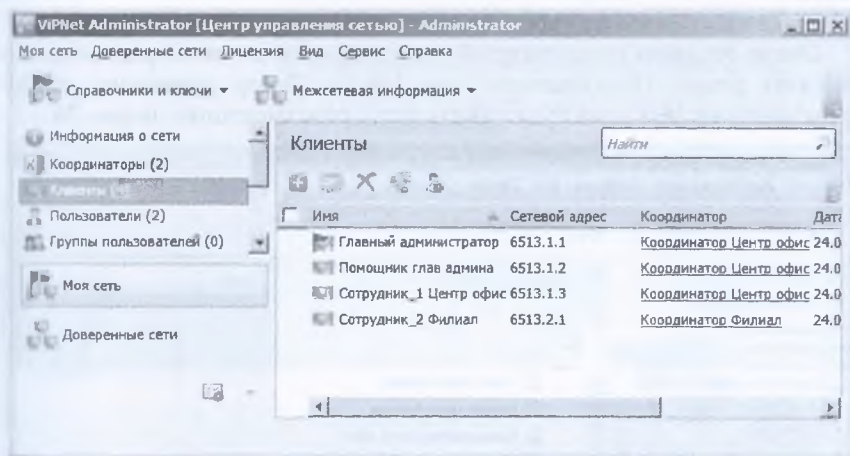


Рис. 22. Раздел Клиенты представления Моя сеть

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 табл. 3. Для этого:

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 админ Петров*, выберите сетевой узел *Главный администратор* и нажмите кнопку *Создать* (рис. 23).

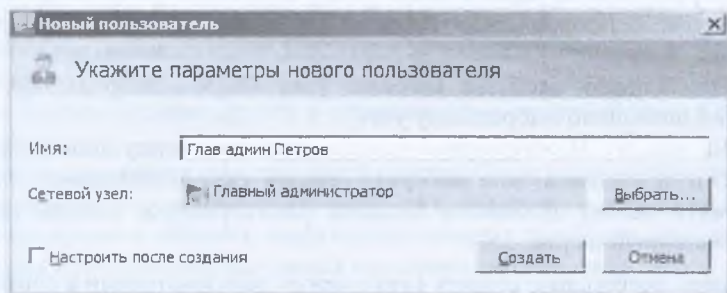


Рис. 23. Параметры пользователя

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 вид, представленный на рис. 24.

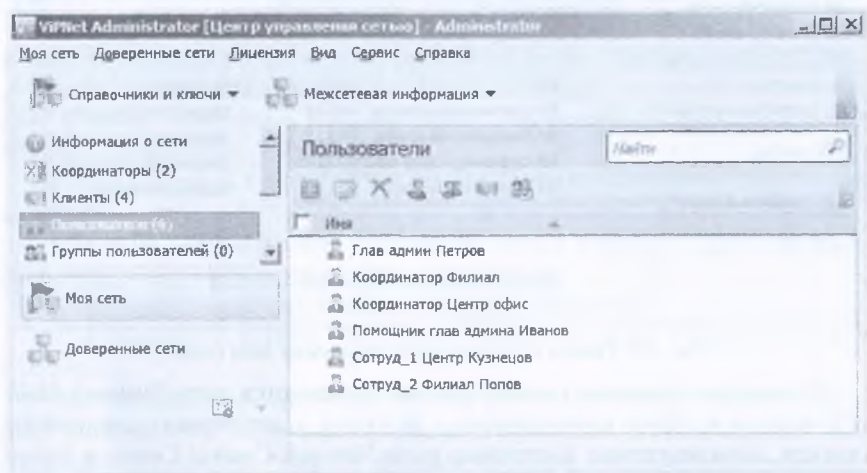


Рис. 24. Раздел *Пользователи* представления *Моя сеть*

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 вид, показанный на рис. 25.

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

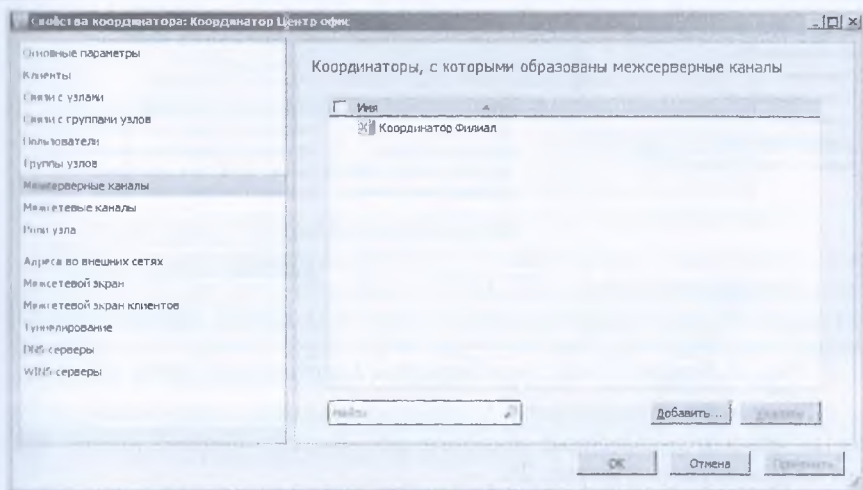


Рис. 25. Вкладка Межсерверные каналы

4. Перейдите в свойства пользователя *Координатор Центр офис* (двойной щелчок по выбранному узлу). Вкладка *Связи с пользователями* на первоначальном этапе пуста (рис. 26).

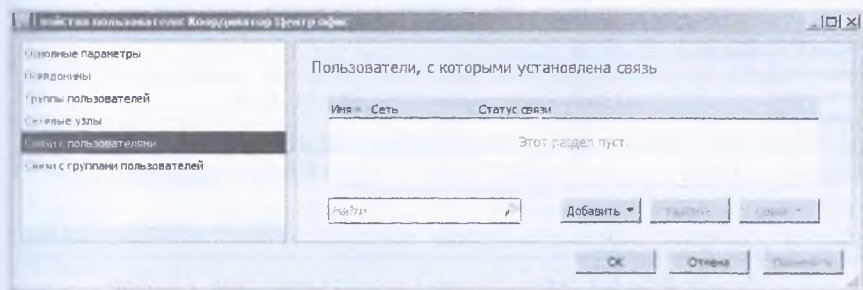


Рис. 26. Вкладка Связи с пользователями

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

После связывания пользователей вкладка *Связи с пользователями* для *Координатор Центр офис* будет иметь вид, представленный на рис. 27.

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

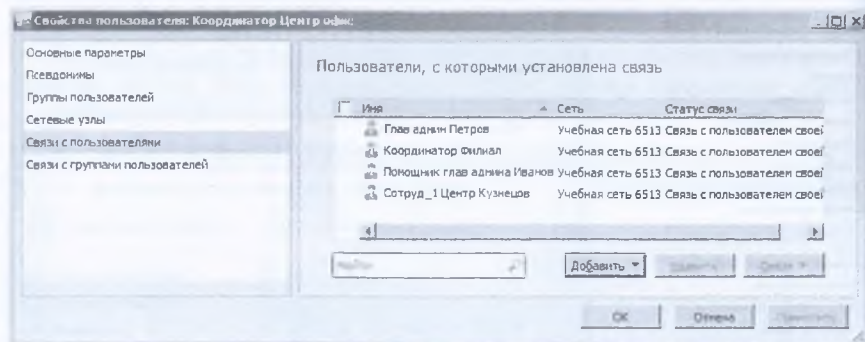


Рис. 27. Вкладка Связи с пользователями Координатора Центр офис

После этого автоматически будут созданы связи между узлами, к которым относятся связанные пользователи. Вкладка *Связи с узлами* примет вид, показанный на рис. 28.

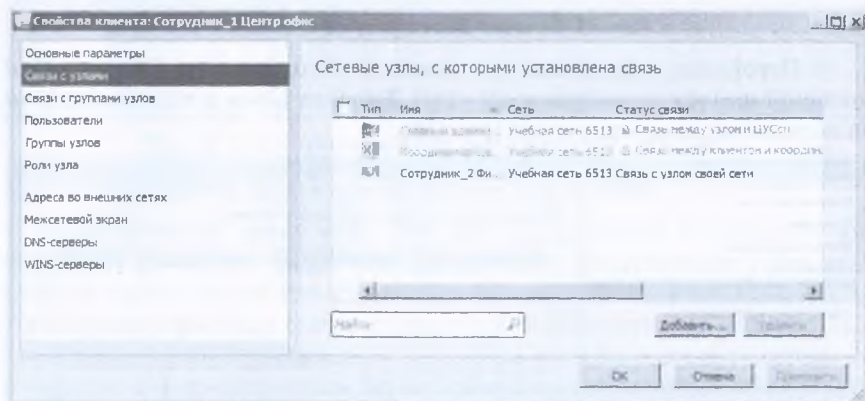


Рис. 28. Вкладка Связи с узлами клиента Сотрудник_1 Центр

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» (рис. 29).

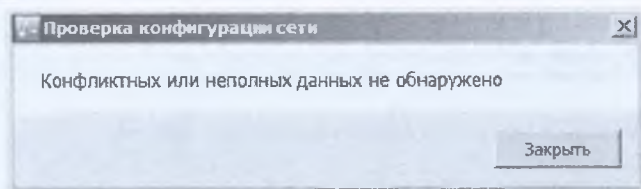


Рис. 29. Положительный результат проверки конфигурации сети

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* (рис. 30).

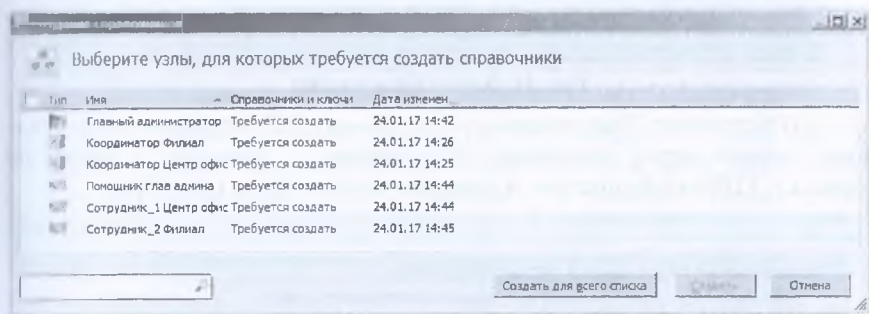


Рис. 30. Окно Создание справочников

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 (рис. 31).

3. На первой странице мастера инициализации нажмите кнопку *Далее*.

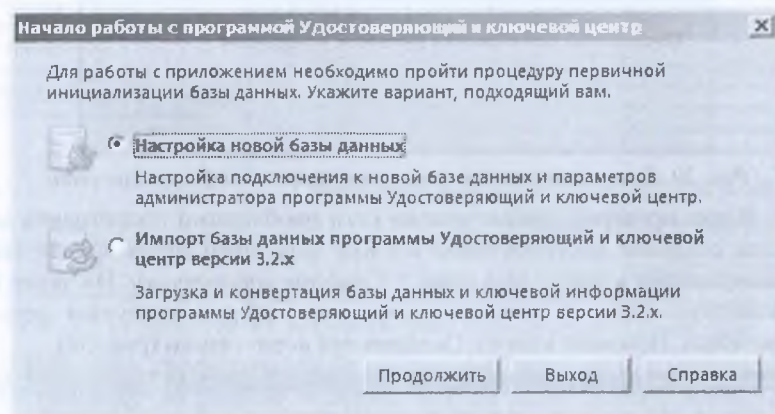


Рис. 31. Выбор базы данных

4. На странице *Подключение к базе данных ViPNet Administrator* укажите сетевой адрес экземпляра SQL-сервера – *.\winccsql* и имя базы данных – *ViPNetAdministrator* и нажмите кнопку *Далее* (рис. 32).

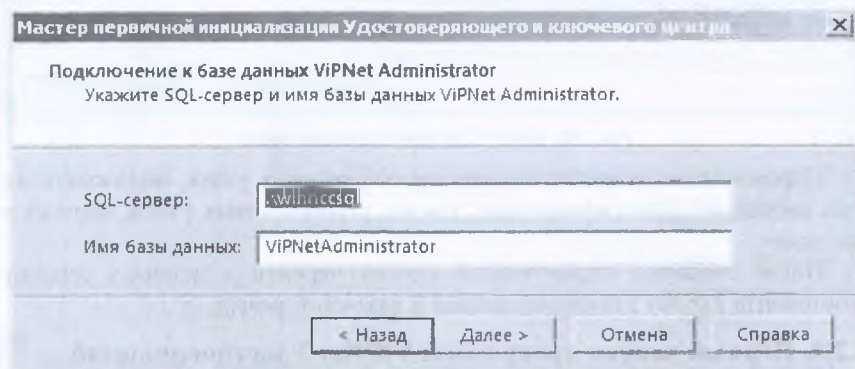


Рис. 32. Подключение к базе данных ViPNet Administrator

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* (рис. 33).

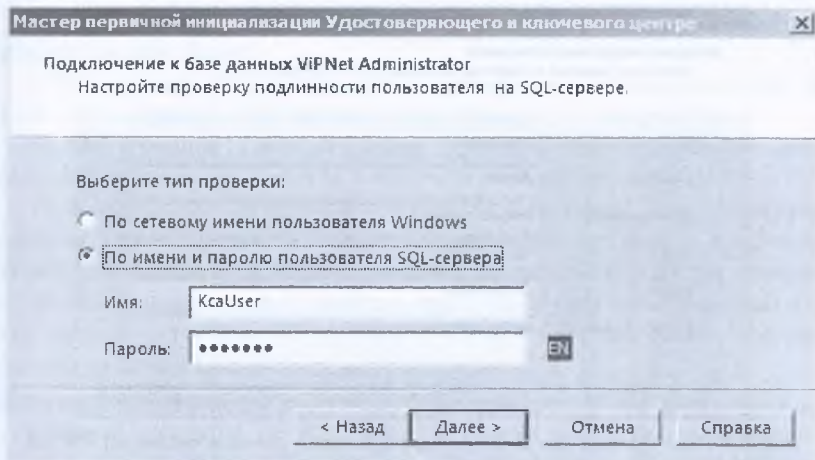


Рис. 33. Задание имени и пароля для подключения к SQL-серверу

6. Имя главного администратора ViPNet компании – *Владимир*. На странице *Создание администратора сети ViPNet* задайте имя учетной записи администратора УКЦ – *Владимир*, и нажмите кнопку *Далее* (рис. 34).

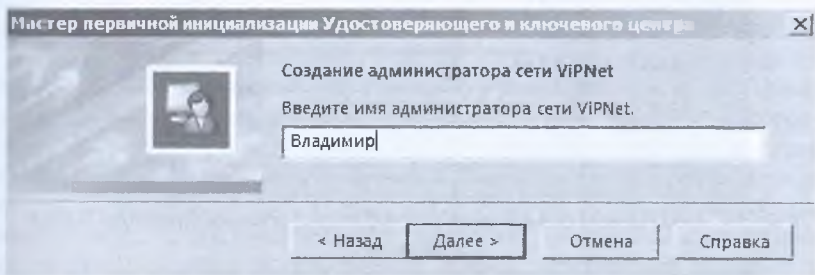


Рис. 34. Ввод имени администратора ViPNet

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 (рис. 35–37).

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Имя: Владимир

Фамилия: Петров

Приобретенное: Владимирович

ИНН: 1111111111

СНИЛС: 2222222222

Электронная почта: petrov_vv@company.ru

< Назад Далее > Отмена Справка

Рис. 35. Ввод данных для издания сертификата администратора ViPNet (часть 1)

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Город: Москва

Область:

Страна: RU

Адрес, улица: дом 7, Большой каретный переулок

< Назад Далее > Отмена Справка

Рис. 36. Ввод данных для издания сертификата администратора ViPNet (часть 2)

Мастер первичной инициализации Удостоверяющего и ключевого центра

Сведения о владельце сертификата
Заполните сведения о владельце запрашиваемого сертификата.

Организация: Компания

OGRN: 333333333333

Подразделение: Отдел информационной безопасности

Должность: Главный администратор

< Назад Далее > Отмена Справка


Рис. 37. 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*.

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

11. 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 издания, 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.

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

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

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.

14. 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 длинной 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) (рис. 38).

Примечания:

1. В реальной ситуации, при настройке и формировании сети рекомендуется руководствоваться существующими правилами парольной безо-

пасности или применять сгенерированные встроенными средствами ViPNet пароли, достаточной сложности.

2. При выполнении практических занятий рекомендуется использовать, простые запоминающиеся пароли во всех программах (например, 11111111 (восемь единиц))

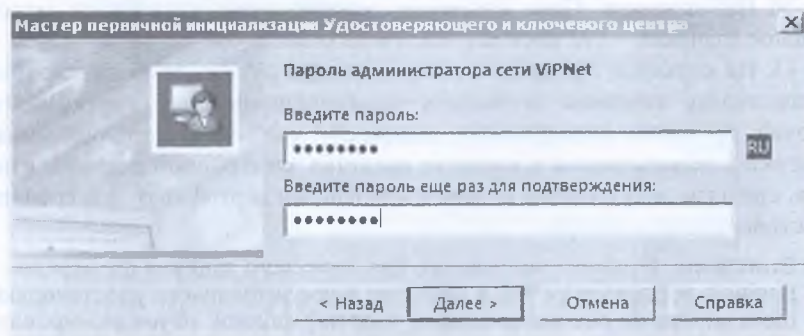


Рис. 38. Задание пароля администратора

15. 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*.

16. Для продолжения работы нажмите кнопку *Далее*. Поводите указателем в пределах окна *Электронная рулетка* (рис. 39) и после успешного завершения инициализации нажмите кнопку *Заккрыть*.

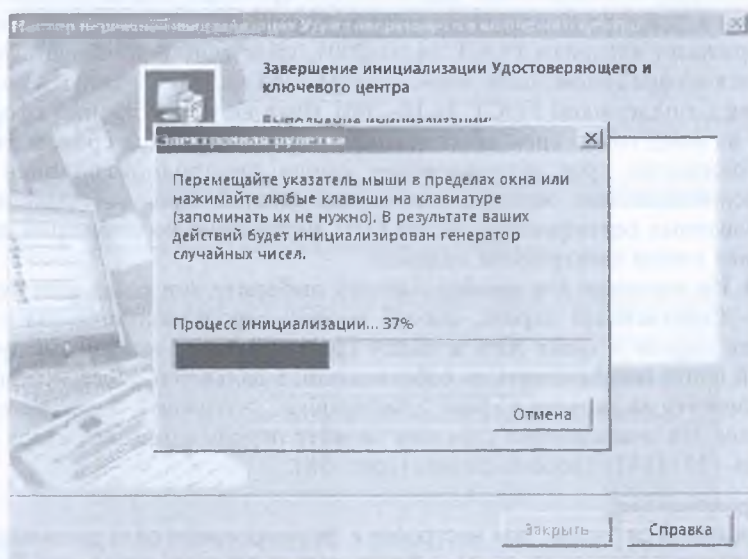


Рис. 39. Окно Электронная рулетка

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 (рис. 40).

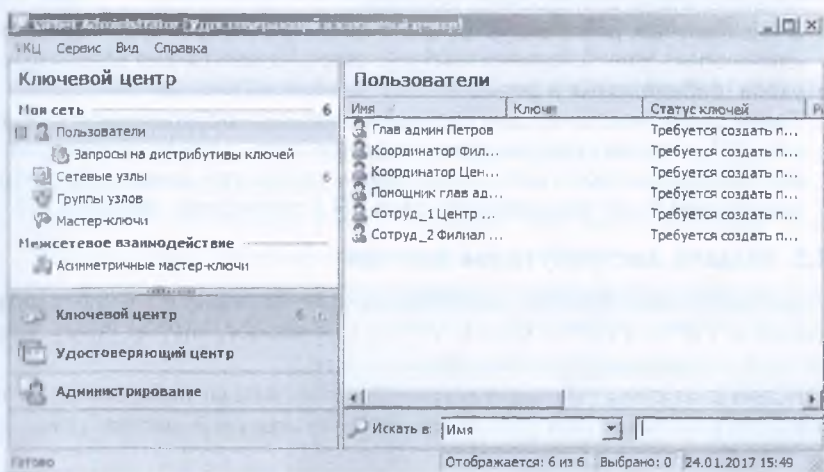


Рис. 40. Главное окно УКЦ

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 ручную 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*. Если же 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, 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

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.



Примечание. В процессе создания структуры сети для сетевых узлов необходимо задавать не только пароли пользователя, но и пароли администратора сетевых узлов при необходимости разграничить доступ лиц, осуществляющих настройку на конкретном сетевом узле (локальный администратор информационной безопасности).

Также есть возможность разграничивать 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 ей 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 (локальному администратору по информационной безопасности, назначенному внутренним приказом по организации).

Для выдачи дистрибутивов ключей выполните следующие действия:

- В окне программы ViPNet Удостоверяющий и ключевой центр на панели навигации выберите представление *Ключевой центр* и перейдите в раздел *Моя сеть* > *Сетевые узлы*.
- 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).
- Выделите все сетевые узлы. В контекстном меню выберите пункт *Выдать новый дистрибутив ключей...*(рис. 41).

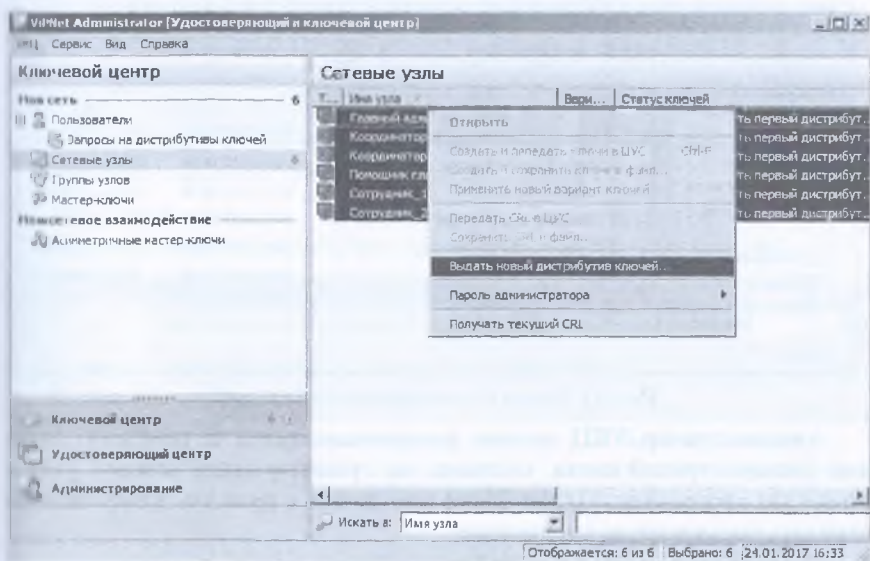


Рис. 41. Выдача дистрибутивов ключей

Задайте пароль пользователя 11111111 по очереди для каждого пользователя защищенной сети (рис. 42).

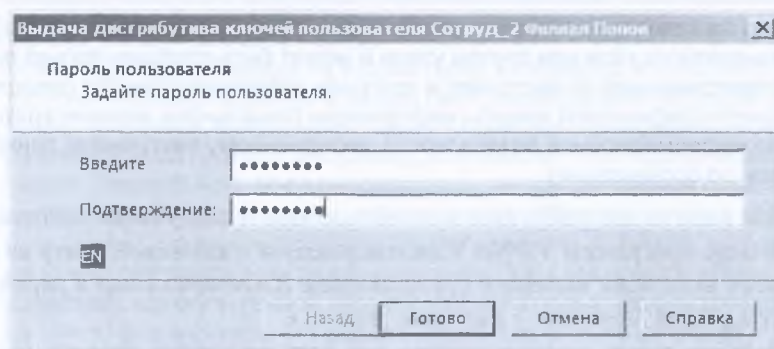


Рис. 42. Задание пароля пользователя

После окончания выдачи дистрибутива откроется окно проводника с папкой, содержащей подпапки сетевых узлов с готовыми дистрибутивами (рис. 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 понадобится в дальнейшем для установки и активации ПО ViPNet.

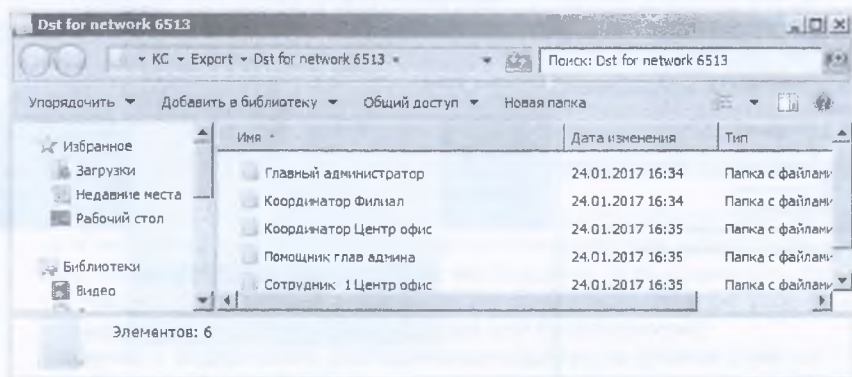


Рис. 43. Папка с дистрибутивами ключей

Администратор УКЦ должен доверенным путем (с помощью специализированной 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.

Задание 1.3. Настройка резервного копирования данных и восстановление данных в ПО ViPNet Administrator

Формулировка задания:

1. Создать резервную копию в ручном режиме.
2. Настроить ежедневное автоматическое резервное копирование данных ПО ViPNet Administrator в 23.59.

1.3.1. Создание резервной копии в ручном режиме

В программе ViPNet Удостоверяющий и ключевой центр существует возможность создания резервных копий конфигурации сети, позволяющих при необходимости осуществлять возврат к более ранним конфигурациям.

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

- Копия базы данных ViPNet Administrator, в которой содержится информация о структуре сети ViPNet, сведения о сертификатах и списках аннулированных сертификатов, изданных в УКЦ, и другие данные.
- Копия папки, в которой хранится служебная информация УКЦ: *C:\ProgramData\Infotecs\ViPNet Administrator\KC*.

В резервную копию конфигурации сети не включаются:

- Копии контейнеров ключей администраторов УКЦ. Резервные копии контейнеров ключей требуется создавать отдельно.
- Справочники и ключи узлов. При необходимости они могут быть созданы после восстановления конфигурации сети.

Резервные копии автоматически перемещаются в папку *C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore* (рис. 44).

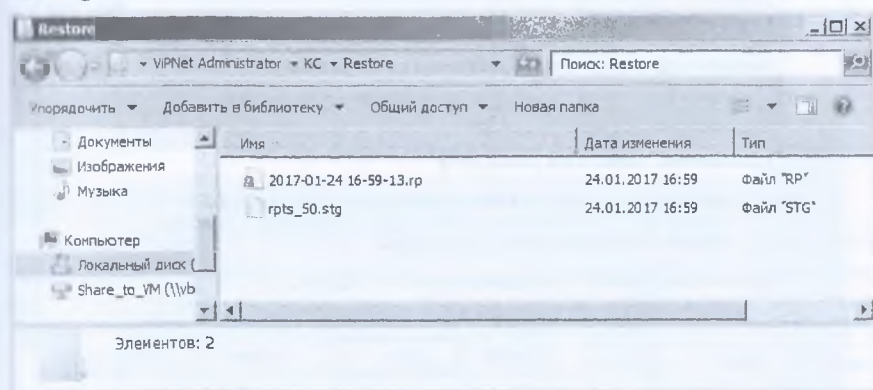


Рис. 44. Содержание каталога Restore

Для создания резервной копии выполните следующие действия:

1. В программе ViPNet Удостоверяющий и ключевой центр в меню *Сервис* выберите пункт *Восстановление конфигурации...*

2. В появившемся окне выберите *Создать резервную копию текущей конфигурации* и нажмите кнопку *Далее* (рис. 45).

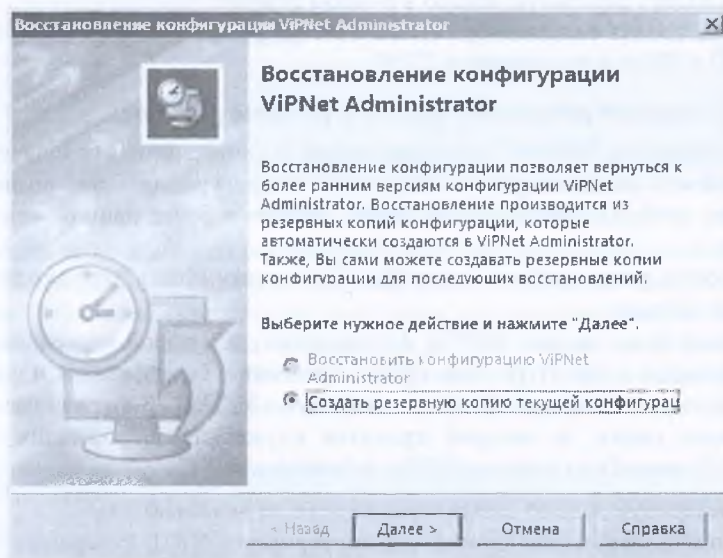


Рис. 45. Окно Восстановление конфигурации ViPNet Administrator

3. В окне *Создание резервной копии* введите комментарий и нажмите кнопку *Далее* (рис. 46).

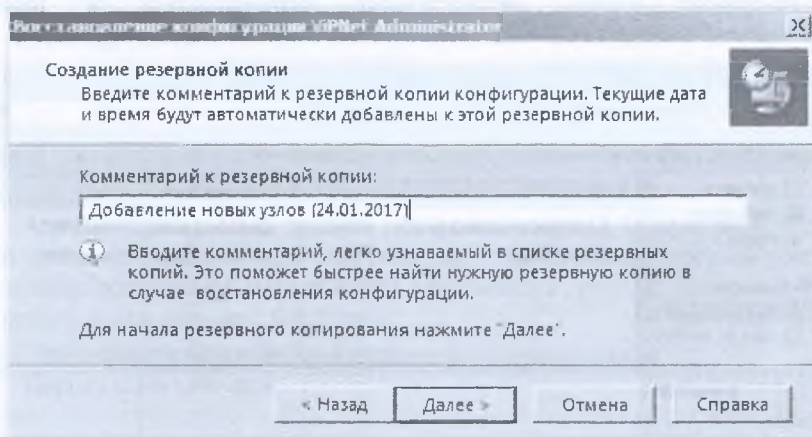


Рис. 46. Окно Создание резервной копии

4. По завершении операции нажмите кнопку *Готово*.

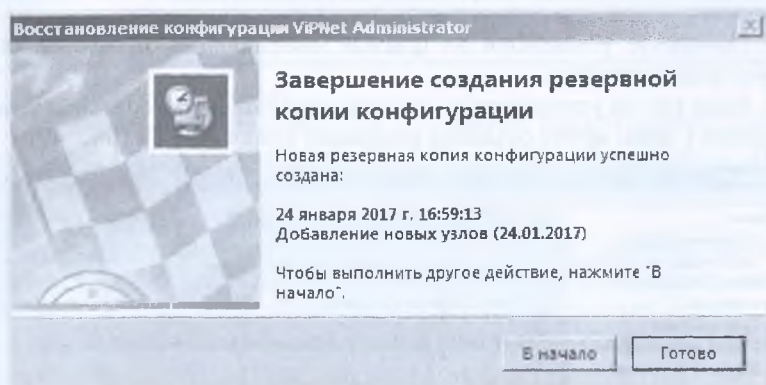


Рис. 47. Окно *Завершение создания резервной конфигурации*

Чтобы просмотреть список резервных копий, в меню *Сервис* выберите пункт *Восстановление конфигурации...* выберите *Редактировать список резервных копий* и нажмите кнопку *Далее*. На экран будет выведено окно с перечнем созданных резервных копий (рис. 48).

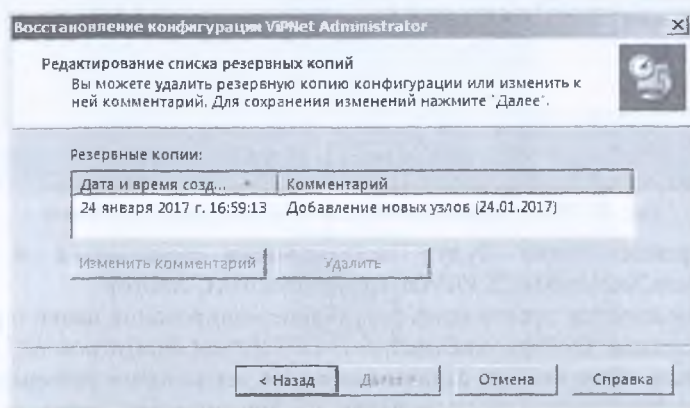


Рис. 48. Окно *Список резервных копий*

1.3.2. Настройка автоматического резервного копирования

В программе ViPNet Удостоверяющий и ключевой центр существует возможность настройки автоматического создания резервных копий конфигурации с определенной периодичностью в заданное время (по умолчанию резервная копия создается каждый день в 02:00).

Зададим настройки таким образом, чтобы резервные копии создавались ежедневно в 23:59 часа. Для этого выполните следующие действия:

1. В меню *Сервис* выберите пункт *Настройки > Восстановление конфигурации*.

2. Проверьте установлен ли флажок *Автоматически создавать резервные копии каждые...*

3. Если нет то установите и укажите периодичность создания резервной копии 1 день, время создания резервной копии – 23:59 (рис. 49).

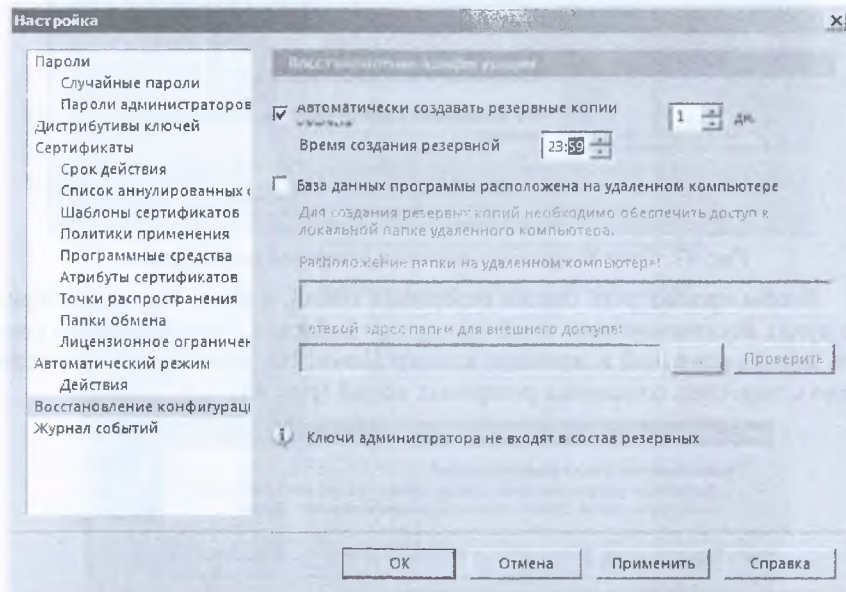


Рис. 49. Настройка параметров создания резервной копии

Резервные копии будут автоматически помещаться в папку *C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore*.

Рекомендуется производить регулярное копирование папки с резервными копиями *C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore* на носитель информации, отличный от того, на котором развернуто ПО ViPNet Administrator (сетевую папку на другом компьютере, съемный жесткий диск).

Для обеспечения возможности полноценного восстановления работоспособности ПО ViPNet Administrator требуется вручную создавать резервные копии контейнеров ключей администратора УКЦ. Каталог с контейнерами ключей администратора УКЦ расположен по следующему пути: *C:\Users\<имя учетной записи локального администратора Windows, от лица которого была произведена установка УКЦ>\AppData\Roaming\Infotecs\ViPNet Administrator*.

Задание 1.4. Развертывание рабочего места помощника главного администратора

Формулировка задания:

1. На виртуальной машине (VM_1 – рабочее место главного администратора сети), где уже установлен ЦУС и УКЦ, доустановить ViPNet Client и активировать его с помощью *dst*-файла, выпущенного для сетевого узла *Главный администратор*.

2. Развернуть на виртуальной машине (VM_2 – рабочее место помощника главного администратора) программное обеспечение клиентской части ViPNet Administrator [Центр управления сетью] и ViPNet Client, который необходимо активировать с помощью *dst*-файла, выпущенного для сетевого узла *Помощник глав админа*.

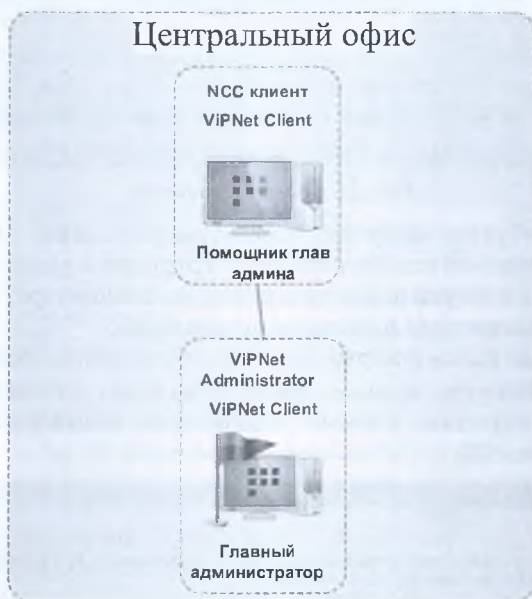


Рис. 50. Схема стэнда для задания 1.4

1.4.1. Установка ViPNet Client

Программное обеспечение ViPNet Client необходимо установить на VM_1 и VM_2. Для этого выполните следующие действия:

- На рабочем месте главного администратора сети (VM_1) запустите установочный файл *<имя файла>.exe*. Дождитесь завершения подготовки к установке ViPNet Client.

- Ознакомьтесь с условиями лицензионного соглашения, установите флажок подтверждения вашего согласия и нажмите кнопку *Продолжить*.
- На странице *Способ установки* установите флажок, чтобы после завершения установки компьютер был перезагружен автоматически, и нажмите кнопку *Установить сейчас* (рис. 51).

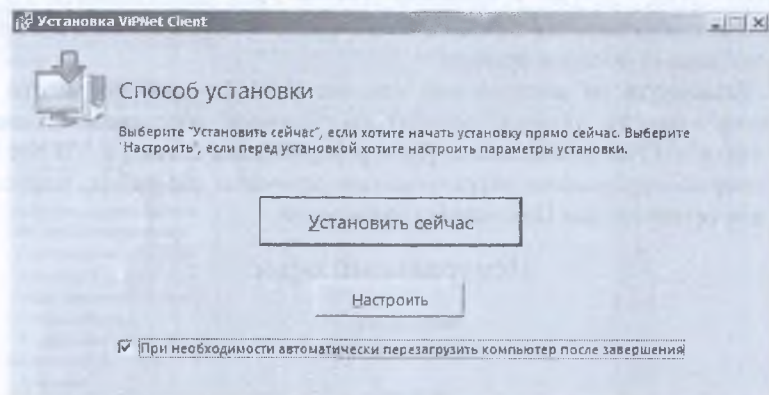


Рис. 51. Способ установки

- Если потребуется настроить параметры установки, то на странице *Способ установки* нажмите кнопку *Настроить* и укажите:
 - путь к папке установки программы на компьютере;
 - имя пользователя и название организации;
 - название папки программы и ее расположение в меню *Пуск*.
- После перезагрузки компьютера на экран будет выведено диалоговое окно об отсутствии ключей. Необходимо подтвердить установку ключей (рис. 52).

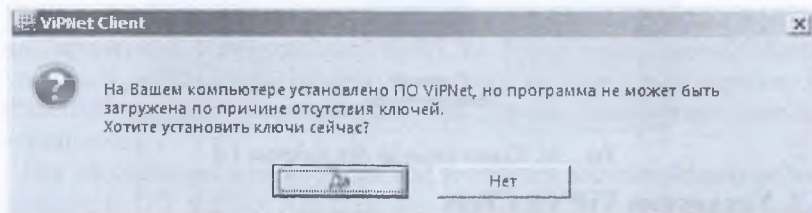


Рис. 52. Диалоговое окно с вопросом об установке ключей

- На странице *Установка ключей сети ViPNet* укажите файл дистрибутива ключей **.dst* для пользователя *Глав админ Петров* сетевого узла *Главный администратор* и нажмите кнопку *Установить ключи* (рис. 53). Дистрибутивы ключей были созданы при выполнении задания 1.2.5.

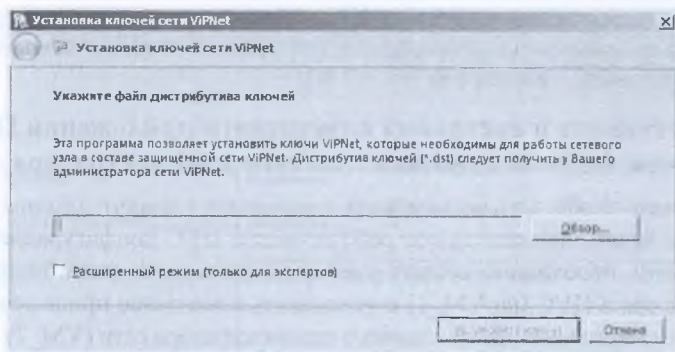


Рис. 53. Выбор дистрибутива ключей

- По завершении процедуры установки ключей нажмите кнопку *Закрыть*.
- На экране появится окно аутентификации в ПО ViPNet Client. Выберите способ аутентификации *Пароль* и введите пароль, заданный при создании дистрибутивов, – 11111111 (рис. 54).

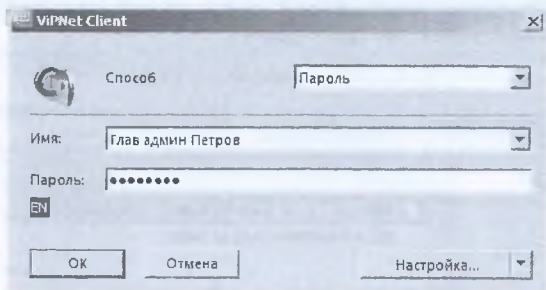


Рис. 54. Окно аутентификации ViPNet Client

Если пароль введен правильно, то в области уведомлений на панели задач отобразится значок *ViPNet Client Монитор*.

Аналогичным образом установите ПО ViPNet Client на рабочем месте помощника главного администратора (VM_2). При этом необходимо установить ключи пользователя *Помощник глав админа Иванов* сетевого узла *Помощник глав админа*.

Проверьте связанность узлов для этого на рабочем месте помощника главного администратора (VM_2) необходимо войти в ViPNet Client Монитор и в разделе защищенная сеть выделить узел *Главный администратор* и нажать F5, узел должен иметь статус *Доступен*.



Примечание. После установки и успешной аутентификации в ViPNet Client, появится диалоговое окно *Установка корневого сертификата*. Это связано с тем, что при формировании *dst*-файла для данного

пользователя была создана ЭП, так как в настройках для созданных узлов по умолчанию устанавливается флажок *Создавать ключи электронной подписи* (см. пп. 1.2.4.).

1.4.2. Установка и настройка клиентского приложения ЦУСа на рабочем месте помощника главного администратора сети

Для того, чтобы дать возможность помощнику главного администратора управлять через дополнительное рабочее место ЦУС конфигурацией защищенной сети, необходимо создать учетную запись помощника главного администратора в ЦУС (на VM_1) и установить клиентское приложение ЦУС на рабочем месте помощника главного администратора сети (VM_2).

Для создания учетной записи помощника главного администратора, выполните следующие действия:

1. Перейдите на рабочее место *Главный администратор* в программе *ViPNet Центр управления сетью*.

2. В окне программы *ViPNet Центр управления сетью* выберите пункт меню *Вид > Администрирование*, раздел *Учетные записи* (рис. 55).

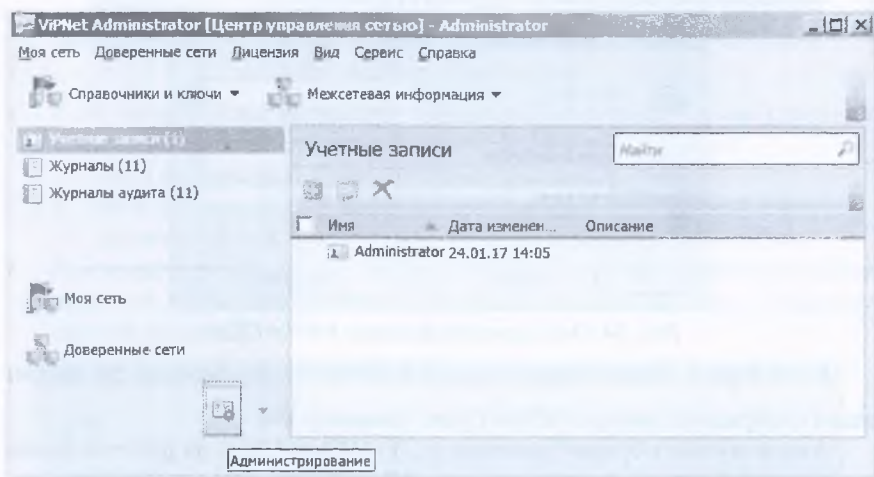


Рис. 55. Раздел *Администрирование*

3. В разделе *Учетные записи* на панели инструментов нажмите кнопку *Добавить*.

4. Откроется окно *Новая учетная запись*. В поле *Имя* укажите *Administrator2*, пароль – 11111111, описание – *Помощник главного администратора сети* (рис. 56). После создания помощника главного администратора раздел *Учетные записи* примет вид, показанный на рис. 57.

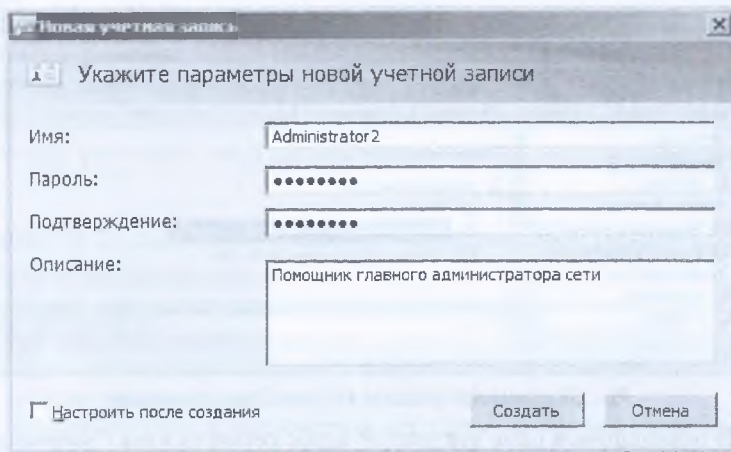


Рис. 56. Создание второго администратора ЦУС

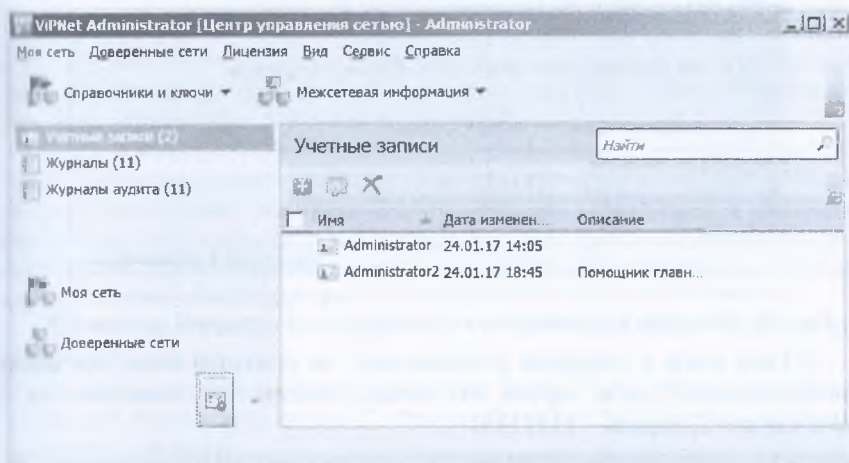


Рис. 57. Раздел Учетные записи ЦУС

В окне программы ViPNet Client Монитор на рабочем месте помощника главного администратора (VM_2) перейдите на вкладку *Защищенная сеть*, посмотрите и запомните IP-адрес сетевого узла *Главный администратор* (рис. 58).

На рабочем месте помощника главного администратора (VM_2) установите клиентскую часть ViPNet Administrator [Центр управления сетью] аналогично тому, как это выполнялось в задании 1.1.2. После установки выполните следующие действия:

1. Запустите клиентскую часть ViPNet Administrator [Центр управления сетью].

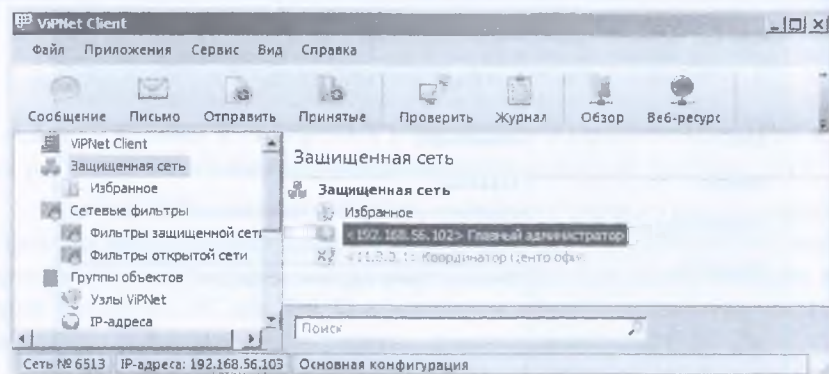


Рис. 58. Окно программы ViPNet Client Монитор

2. В появившемся окне введите IP-адрес сетевого узла *Главный администратор* (может отличаться от приведенного на рис. 59).

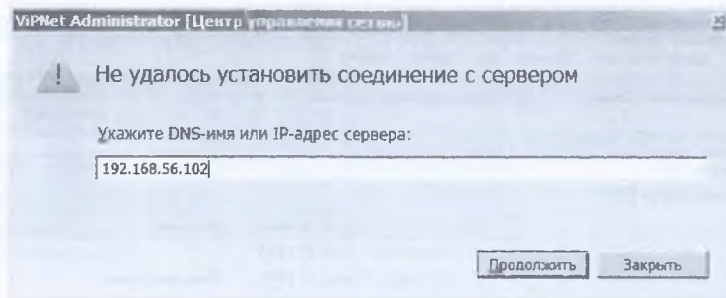


Рис. 59. Ввод адреса сетевого узла с установленной серверной частью ЦУС

3. Если связь с сервером установилась, то появится окно для ввода имени пользователя и пароля для входа. Введите имя пользователя *Administrator2*, пароль – 11111111.

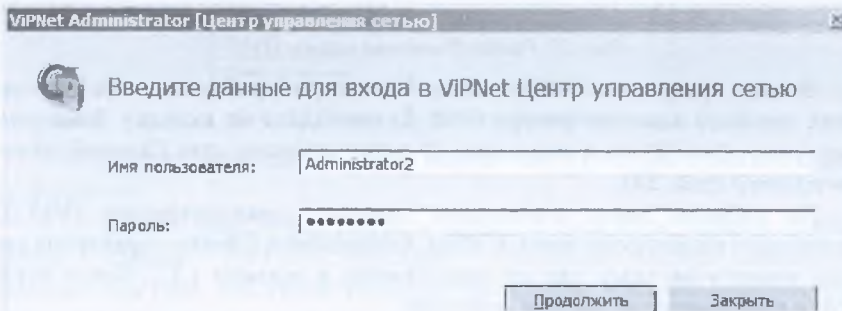


Рис. 60. Окно аутентификации клиентской части ЦУС

4. После успешного подключения клиентской части ЦУС, расположенной на рабочем месте помощника главного администратора будет выведено диалоговое окно, в котором необходимо задать новый пароль. Введите старый пароль 11111111, новый пароль – 11111111.

Теперь управлять защищенной сетью ViPNet можно с двух рабочих мест.

Задание 1.5. Дополнительное задание. Миграция ПО ViPNet Administrator

Формулировка задания:

1. Выполните миграцию компонентов ViPNet Administrator.
2. Сохраните отчет о структуре сети ViPNet в файл.
3. Настройте роли и полномочия для узла *Помощник глав админа* так, чтобы ограничить обмен файлами и чатом.

Возможны следующие сценарии миграции ПО ViPNet Administrator:

1. Компоненты ViPNet Administrator установлены на одном компьютере и требуется их перенос также на один компьютер (может понадобиться при смене операционной системы или самого компьютера, на котором функционирует ViPNet Administrator).

2. Компоненты ViPNet Administrator установлены на одном компьютере и требуется разнести их на разные компьютеры (может потребоваться при ужесточении политики безопасности по отношению к рабочему месту администратора сети, например, когда по требованиям безопасности база данных ViPNet Administrator должна быть размещена на отдельном защищенном компьютере).

Для осуществления миграции ПО ViPNet Administrator необходимы следующие данные:

- Резервная копия конфигурации сети (файл *.rp). Файлы резервных копий находятся в папке *C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore*.
- Копия архива, содержащего список всех резервных копий, которые создавались при эксплуатации сети (файл *rpts_50.stg*). Файл архива находится в папке *C:\ProgramData\InfoTeCS\ViPNet Administrator\KC\Restore*.
- Копия лицензионного файла (*infotecs.reg*).
- Копия папки с контейнерами ключей администратора УКЦ: *C:\Users\<имя учетной записи локального администратора Windows>, от лица которого была произведена установка УКЦ\>\AppData\Roaming\Infotecs\ViPNet Administrator*.

В рамках настоящего практического задания необходимо отработать первый сценарий. Отработка сценария будет проводиться на одной вир-

туальной машине (VM_1), фактически переноса на другую машину происходить не будет. Для этого выполните следующие действия:

Примечание. В процессе выполнения задания по миграции не забывайте удалять пользовательскую информацию. Так как если не удалить всю пользовательскую информацию, а только ПО ViPNet Administrator, то потенциально возникает угроза утечки информации о структуре сети. Поэтому в процессе удаления ПО не забудьте проставить галочки *Удалить пользовательские данные* (рис. 61, 62). Не забудьте сделать snapshot виртуальной машины VM_1, на которой развернут ПО ViPNet Administrator перед выполнением практического задания на случай если после выполнения практического задания и входе его выполнения возникнут проблемы которые могут повлиять на дальнейшую работоспособность ПО.

1. Создайте папку *Migration* на *Рабочем столе* и скопируйте в нее каталог с контейнерами ключей администратора УКЦ (KeysManager_1): *C:\Users\<имя учетной записи локального администратора Windows>*, от лица которого была произведена установка *УКЦ > \AppData\Roaming\Infotecs\ViPNet Administrator* и каталог с резервными копиями *C:\ProgramData\InfoTeCS\ViPNetAdministrator\KC\Restore*.

2. Завершите работу компонентов ViPNet Administrator [Центр управления сетью] и ViPNet Administrator [Удостоверяющий и ключевой центр].

3. Удалите все компоненты ViPNet Administrator (ЦУС и УКЦ) штатными средствами операционной системы (*Пуск > Панель управления > Удаление программы*).

4. При удалении ViPNet Administrator [Центр управления сетью] – Сервер подтвердите удаление пользовательских данных и базы данных Центра управления сетью (рис. 61).

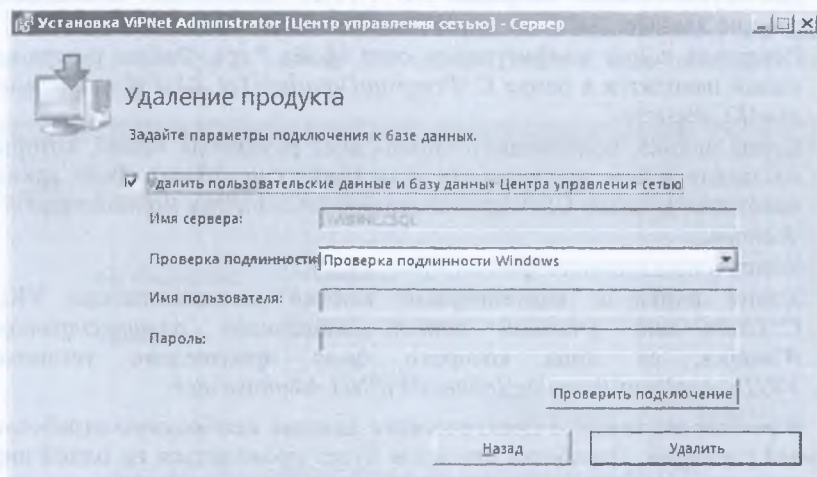


Рис. 61. Удаление ЦУС сервер

5. При удалении ViPNet Administrator [Центр управления сетью] – Клиент также подтвердите удаление пользовательских данных (рис. 62).

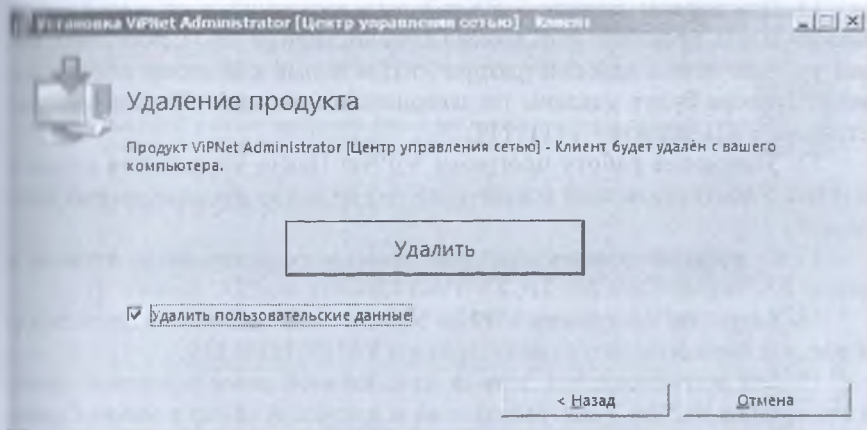


Рис. 62. Удаление ЦУС клиент

6. Удалите ViPNet Administrator [Удостоверяющий и ключевой центр].

7. Перезагрузите компьютер.

8. После перезагрузки компьютера проверьте были ли удалены следующие каталоги *C:\Users\<имя учетной записи локального администратора Windows, от лица которого была произведена установка УКЦ>\AppData\Roaming\Infotecs\ViPNetAdministrator* и *C:\ProgramFiles (x86)\InfoTeCS\ViPNetAdministrator*. Если данные папки были удалены не полностью, удалите их вручную.

Особенности восстановления из резервной копии:

- Для восстановления конфигурации сети из резервной копии необходимо знать пароль создавшего ее администратора, актуальный на момент создания копии.
- Если резервная копия была создана в более поздней версии УКЦ, ее невозможно использовать для восстановления конфигурации сети.
- При удалении одной из учетных записей администратора рекомендуется сменить ключ защиты УКЦ и удалить те резервные копии, которые были созданы данным администратором.

9. Установите компоненты ViPNet Administrator заново на виртуальную машину (VM_1), с которой в предыдущих пунктах были удалены ЦУС и УКЦ, согласно заданию 1.1.

10. Выполните первый запуск программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр согласно зада-

нию 1.2. При первом запуске ViPNet Центр управления сетью создавать сетевые узлы не требуется.

11. При первом запуске ViPNet Удостоверяющий и ключевой центр можно задать произвольные данные администратора УКЦ, поскольку новая учетная запись администратора УКЦ и новый контейнер ключей администратора будут удалены по завершении миграции. Пароль администратора УКЦ задайте – 11111111.

12. Завершите работу программ ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр после произведенных операций.

13. Скопируйте сохраненный ранее каталог с резервными копиями в папку *C:\ProgramData\InfoTeCS\ViPNetAdministrator\KC\Restore*.

14. Запустите программу ViPNet Удостоверяющий и ключевой центр и введите пароль нового администратора УКЦ – 11111111.

15. Для восстановления данных из созданной ранее резервной копии в программе ViPNet Удостоверяющий и ключевой центр в меню *Сервис* выберите пункт *Восстановление конфигурации...* В появившемся окне выберите пункт *Восстановить конфигурацию ViPNet Administrator* и нажмите кнопку *Далее* (рис. 63).

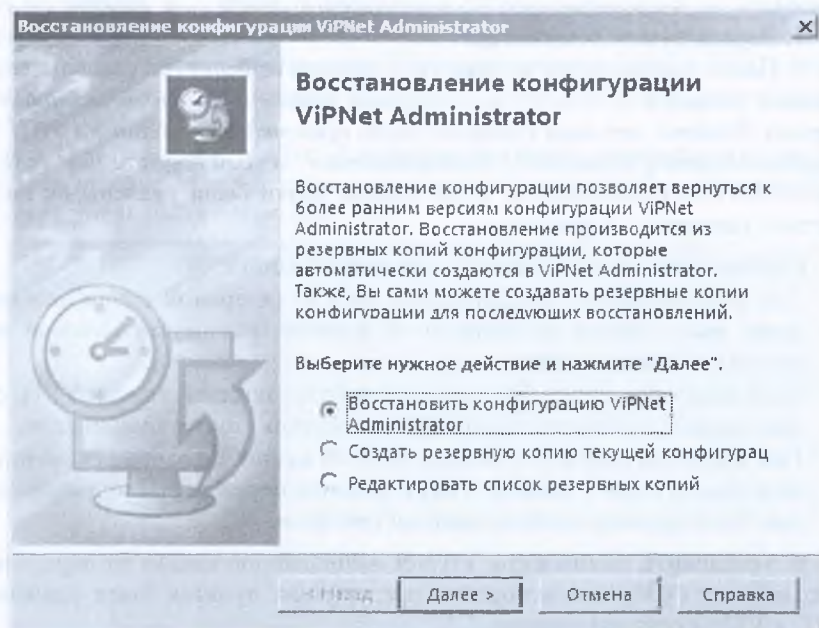


Рис. 63. Восстановление конфигурации

16. На странице выбора резервной копии отметьте резервную копию, которую создавали в ручном режиме при выполнении одного из предыдущих заданий, и нажмите кнопку *Далее* (рис. 64).

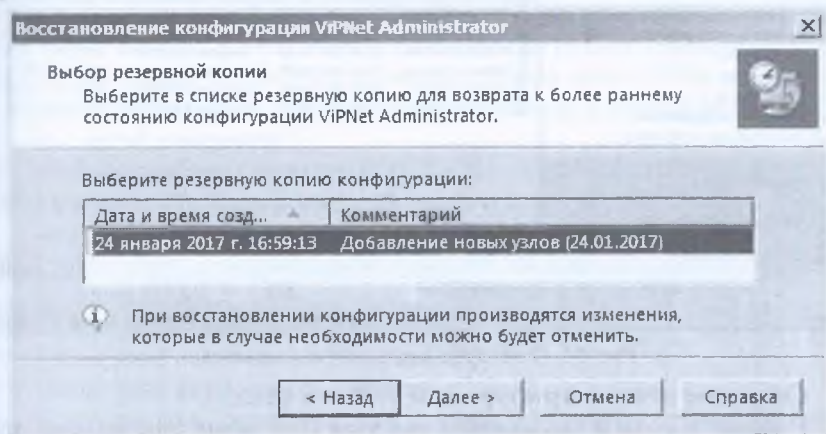


Рис. 64. Выбор резервной копии из списка

После восстановления данных программа ViPNet Удостоверяющий и ключевой центр автоматически перезапустится. На экран будет выведено диалоговое окно для входа и указаны учетные данные администратора, созданного при выполнении задания 1.2.

17. Скопируйте каталог с контейнерами ключей администратора УКЦ обратно в папку *C:\Users\<имя учетной записи локального администратора Windows>\AppData\Roaming\Infotecs\ViPNet Administrator* и после этого введите пароль 11111111 (рис. 65).

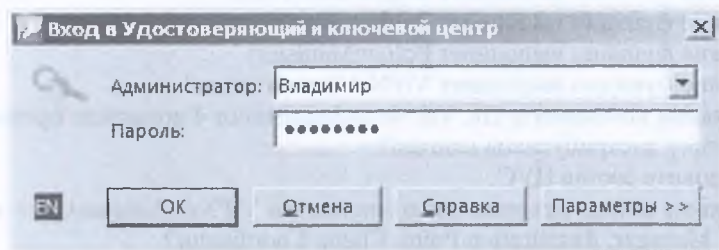


Рис. 65. Окно входа в УКЦ

Если все сделано правильно, то в появившемся окне программы ViPNet Удостоверяющий и ключевой центр будут отображены созданные ранее пользователи и сетевые узлы (рис. 66).

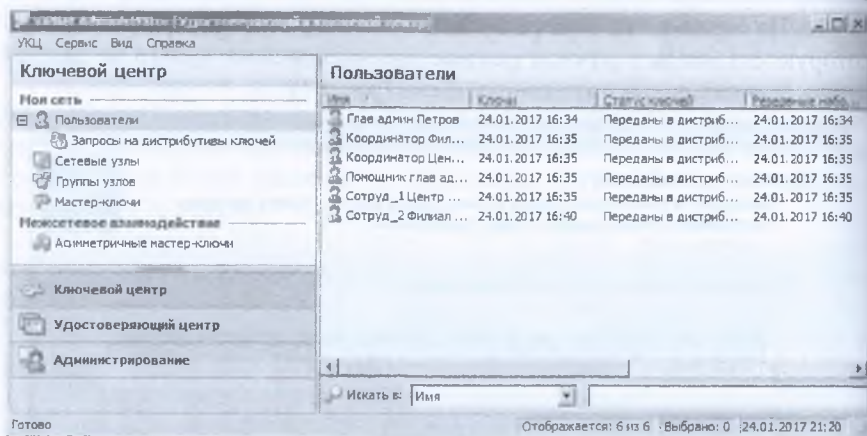


Рис. 66. Окно УКЦ после восстановления

Сохраните отчет о структуре сети ViPNet в файл.

Настройте роли и полномочия для узла *Помощник глав админа*, так чтобы ограничить обмен файлами и чат.

Контрольные вопросы

1. Из каких компонентов состоит программный комплекс ViPNet Administrator 4?
2. Какие функции выполняет ЦУС?
3. Какие функции выполняет УКЦ?
4. Какие функции выполняет ViPNet Coordinator?
5. Какие функции выполняет ViPNet Client?
6. Какие функции выполняет Registration Point?
7. Какие функции выполняет Publication Service?
8. Какие функции выполняет Policy Manager?
9. Какие функции выполняет ViPNet StateWatcher?
10. В каком компоненте ПК ViPNet Administrator 4 возможно произвести выдачу дистрибутивов ключей?
11. Назовите состав ЦУС.
12. Каковы схемы размещения компонентов ViPNet Administrator 4, Policy Manager, Registration Point, Client, Coordinator?
13. Для чего предназначена программа «Контроль приложений»?
14. Что такое полномочия? Где задаются полномочия?
15. Для каких программ задаются полномочия? Для каких ролей?
16. Что такое псевдонимы пользователей и как они задаются?
17. Что содержится в базе данных ViPNet Administrator 4?
18. Где находится папка с контейнерами ключей администратора УКЦ?
19. Какие способы создания структуры сети есть в ЦУС?

10. Что содержится в файле *.gr?
11. В какой каталог перемещаются файлы резервных копий конфигурации сети?
12. Что содержится в файле rpts_50.stg?
13. Могут ли ЦУС и УКЦ быть установлены на разные компьютеры?
14. Какие данные потребуются администратору сети ViPNet для осуществления миграции программного комплекса ViPNet Administrator 4 на другой компьютер?
15. Назовите рабочие каталоги ЦУС/УКЦ.
16. Какими свойствами должен обладать сетевой узел для того, чтобы на нем можно было установить ViPNet Policy Manager?
17. С помощью какой программы можно сохранять структуру сети в формате HTML?
18. Каково назначение ПАК IDS?
19. Какие роли назначаются Координатору?
20. Какие роли назначаются Клиенту?
21. Что такое роль, сетевая группа, служебный конверт, сетевой фильтр?
22. Каковы функции ViPNet-драйвера?
23. Что такое Администратор сетевого узла? Где задается пароль Администратора сетевого узла? Какие возможности, по сравнению с обычным пользователем у Администратора?
24. Что отображается в окне Защищенная сеть ViPNet Monitor?
25. Где можно посмотреть максимальную допустимую версию ПО, которую вы можете установить?