Практическое занятие 2. Модификация защищенной сети и настройка политик безопасности на узлах

Содержание практического занятия:

1. Модификация защищенной сети.
2. Компрометация узла и пользователя.
3. Настройка политик безопасности в ViPNet Policy Manager.
4. Дополнительное задание.

Для выполнения второго практического задания нам потребуется две виртуальные машины VM_1 (*Главный администратор*) и VM_2 (*Помощник главного администратора*). В практическом занятии 1 они были уже настроены, но лучше еще раз убедитесь в корректности сетевых настроек, а также ПО ViPNet (рис. 67).

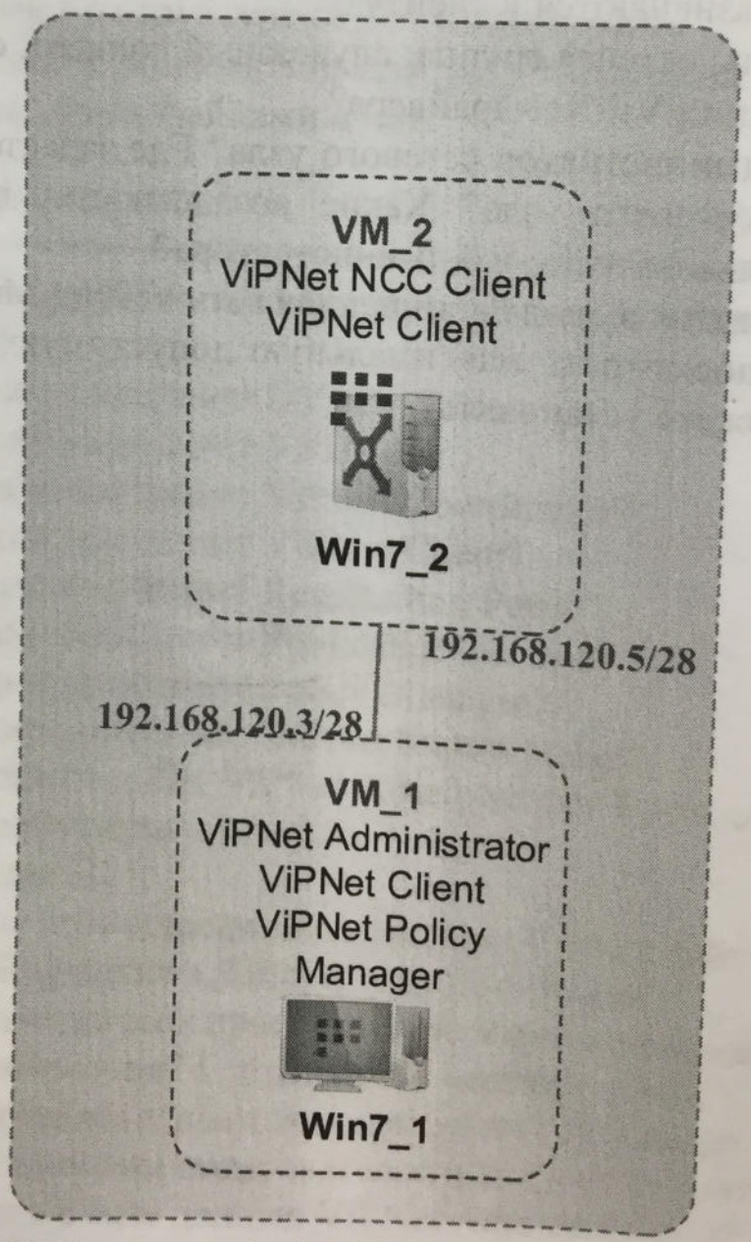

Рис. 67.Схема стенда для Практического занятия 2

Задание 2.1. Модификация защищенной сети.

Формулировка задания. На первом практическом занятии создана защищенная сеть ViPNet (рис. 68).

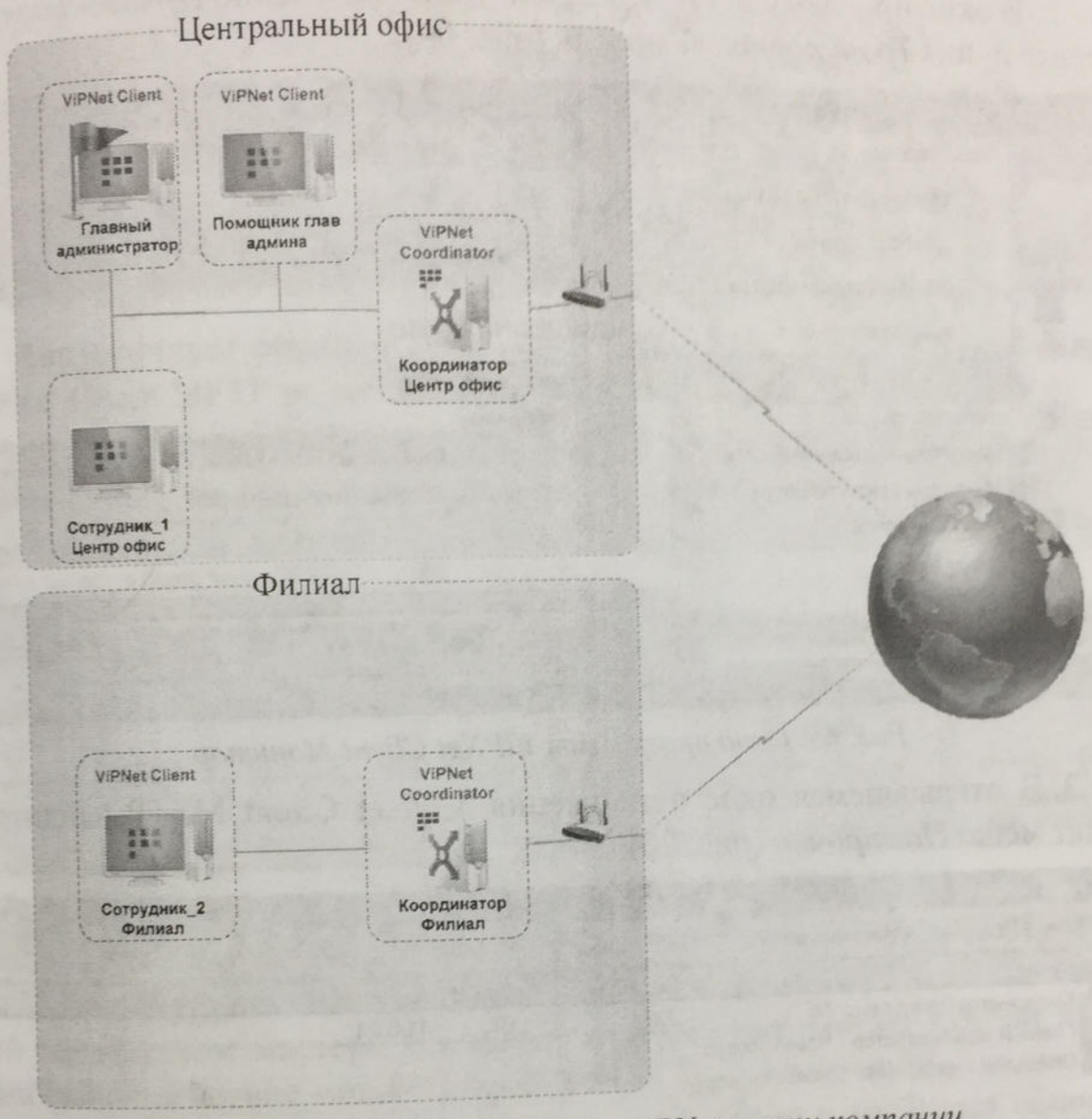

Рис. 68. Схема развертывания ViPNet в сети компании

Теперь в топологию данной защищенной сети ViPNet необходимо внести изменения.

Настройка программного обеспечения ViPNet

Для обеспечения более быстрого прохождения обновлений на клиентах при выполнении настоящего практического задания необходимо настроить *Транспортный модуль*, обеспечивающий обмен служебными конвертами. Так как на данном этапе в сети нет развернутого координатора, а рассылка обновлений по умолчанию в ViPNet Client осуществляется через координатор (в настройках транспортного модуля выставлен тип канала *Через сервер*), поэтому необходимо сменить тип канала на *MFTP*. Для этого выполните следующие действия:

1. На рабочем месте *Главного администратора (VM_1)* откройте программу ViPNet Client Монитор (*Пуск > Все программы > ViPNet > ViPNet Client > Монитор*) и введите пароль пользователя *Глав админ Петров*, заданный на первом практическом занятии – 11111111.

2. В окне программы ViPNet Client Монитор в меню *Приложения* выберите пункт *Транспортный модуль* (рис. 69).

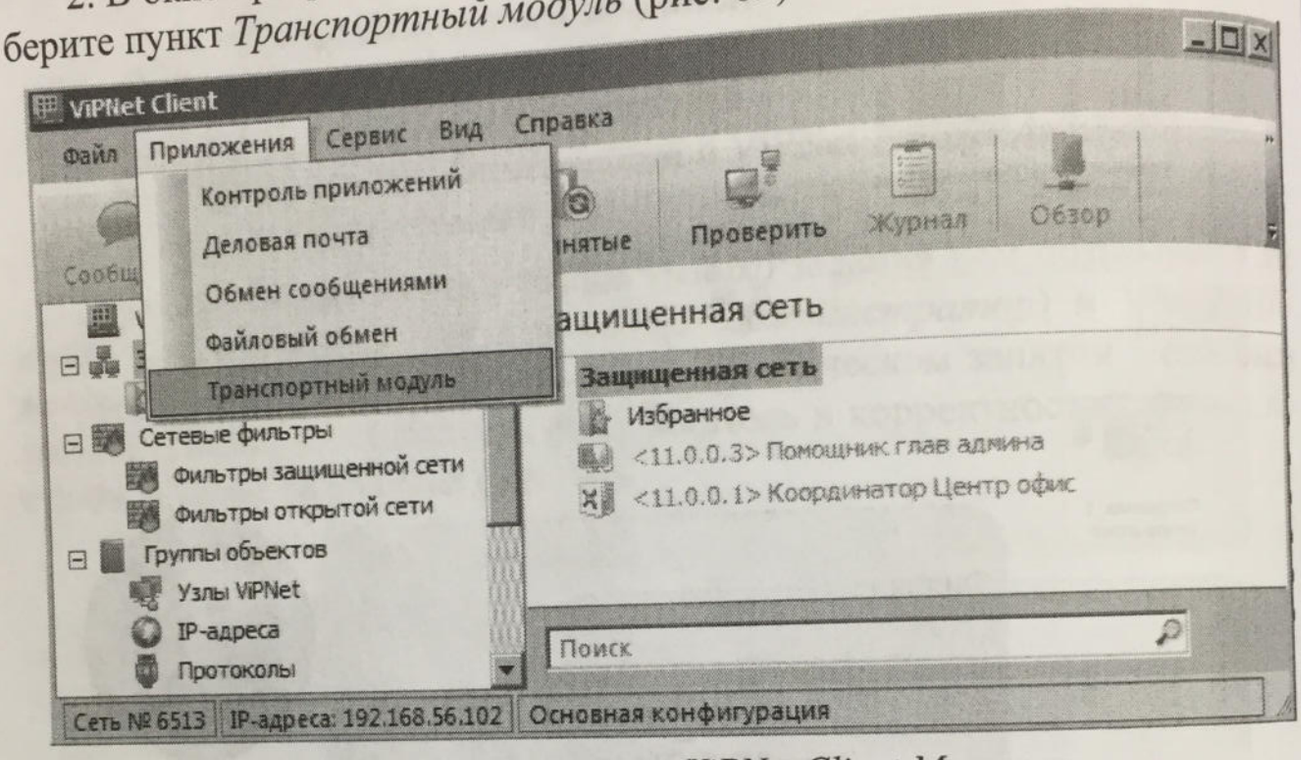

Рис. 69. Окно программы ViPNet Client Монитор

3. В открывшемся окне приложения ViPNet Client MFTP зайдите в пункт меню *Настройки* (рис. 70).

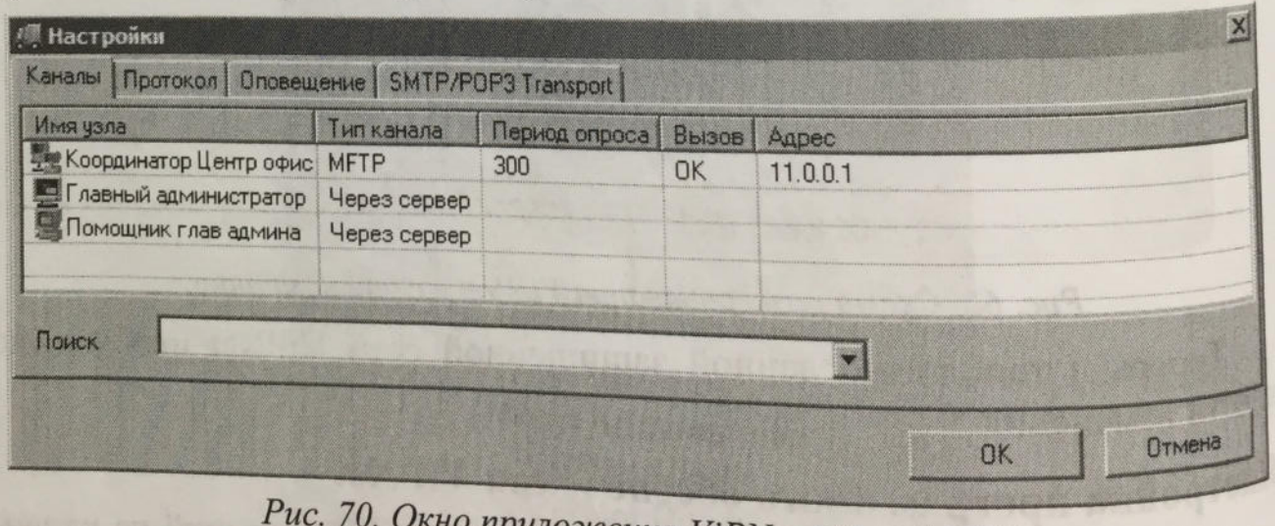

Рис. 70. Окно приложения ViPNet Client MFTP

4. Дважды щелкните левой кнопкой мыши сперва на узел *Главный администратор*, выберите тип канала MFTP, установите период опроса равным 5 секунд, установите флажок напротив строки *Вызывать узел по нажатию кнопки «Опросить»* и нажмите кнопку *ОК* (рис. 71). Затем откройте свойства узла *Помощник глав админа* и выставьте такие же настройки.

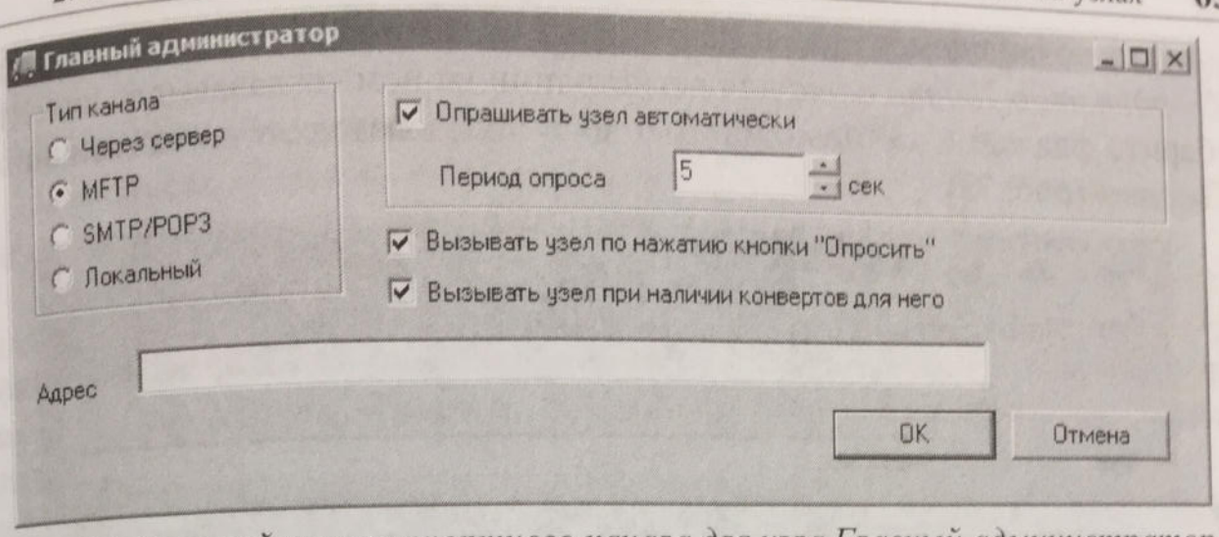

Рис. 71. Настройки транспортного канала для узла Главный администратор

Аналогичным образом выполните настройки транспортного модуля ViPNet Client MFTP на рабочем месте *Помощник глав админа* (VM_2).

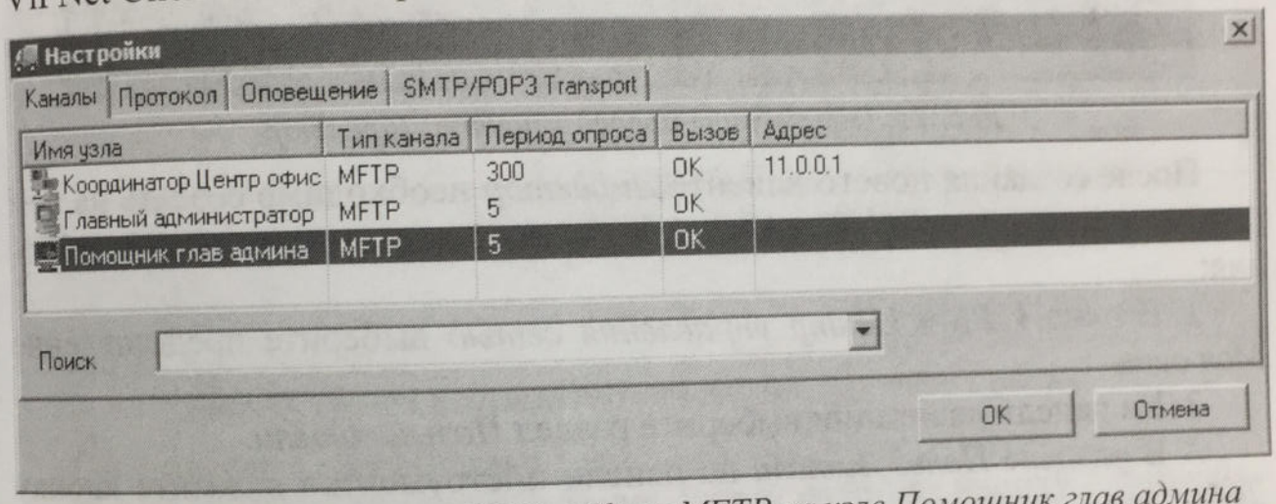

Рис. 72. Окно приложения ViPNet Client MFTP на узле Помощник глав админа (после настройки)

Стоит обратить внимание, на то что после повторной установки ключей посредством мастера установки ключей локально на каждой из машин (такое действие может потребоваться при выполнении задания, если связь была потеряна с Центром управления сетью и требуется обновить справочно-ключевую информацию), настройки *Транспортного модуля* принимают значения по умолчанию, то есть типа канала *MFTP* будет сменен на *Через сервер*.

2.1.1. Добавление сетевого узла

Для добавления нового клиента *Директор* перейдите на рабочее место *Главный администратор* и 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 *Добавить*.

4. В появившемся окне задайте имя *Директор*, выберите координатор *Координатор Центр офис* для регистрации на нем создаваемого клиента, уберите флажок *Создать* одноименного пользователя и нажмите кнопку *Создать* (рис. 73).

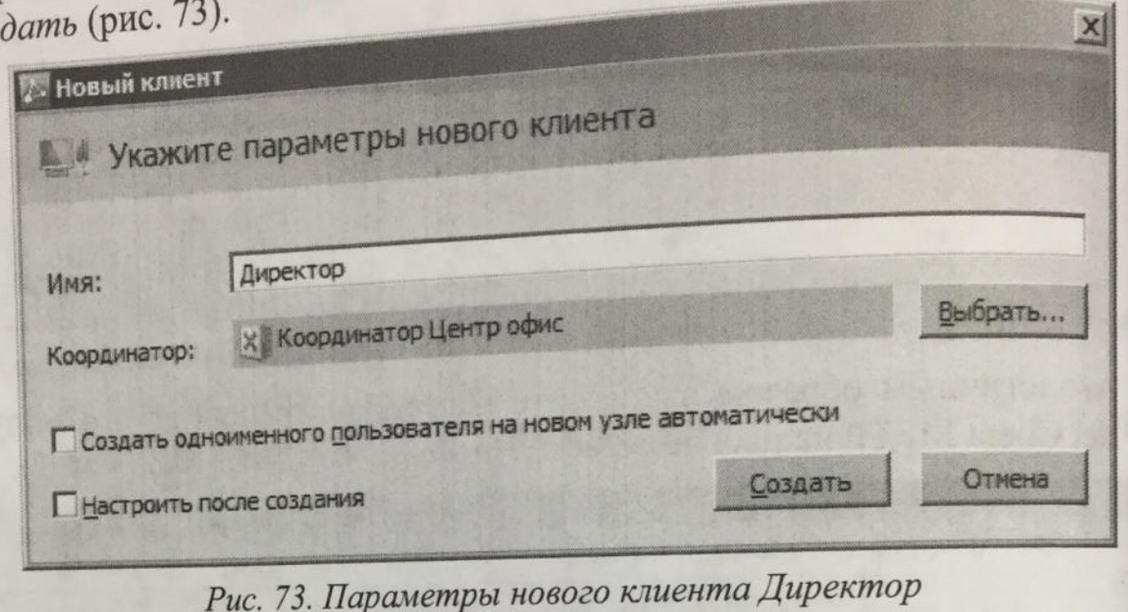

Рис. 73. Параметры нового клиента Директор

После создания нового клиента *Директор* необходимо создать на нем пользователя *Директор Соколов*. 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 *Добавить*.
4. В появившемся окне задайте имя пользователя *Директор Соколов*, выберите сетевой узел *Директор* и нажмите кнопку *Создать* (рис. 74).

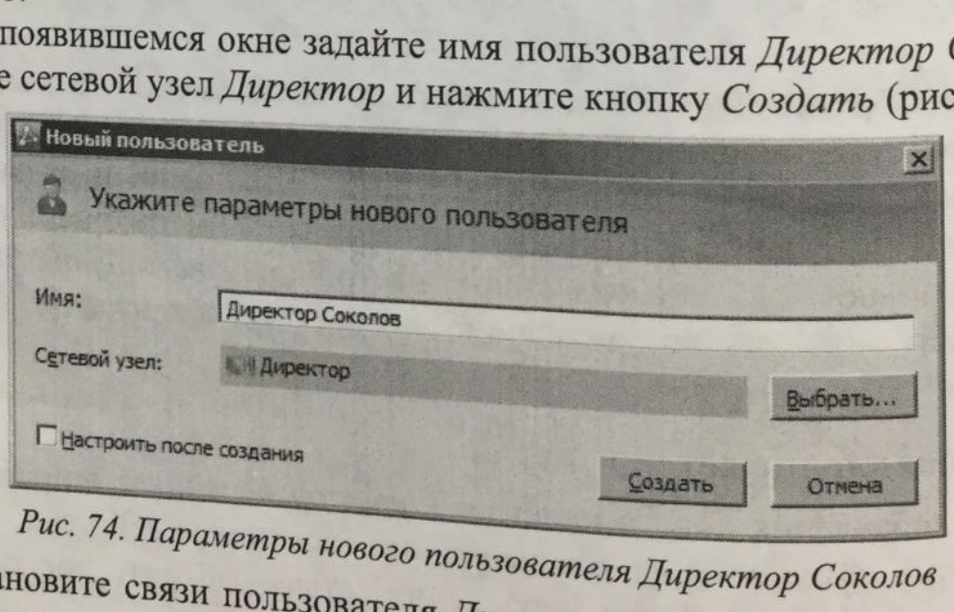

Рис. 74. Параметры нового пользователя Директор Соколов

Установите связи пользователя *Директор Соколов* с пользователями *Помощник глав админа Иванов*, *Сотрудник_1 Центр Кузнецов*, *Сотрудник_2 Филиал Попов*, *Координатор Центр офис*, *Координатор Филиал* (связь между пользователями обеспечивает возможность ведения конфиденциальной переписки в программе ViPNet Client Деловая почта между этими пользователями). Для этого:

1. В окне *ViPNet Центр управления сетью* выберите представление *Моя сеть*.

2. На панели навигации выберите раздел *Пользователи*.

3. В списке *Пользователей* выберите *Директор Соколов* и на панели инструментов нажмите кнопку *Свойства*.

4. В окне *Свойства пользователя: Директор Соколов* выберите вкладку *Связи с пользователями* и добавьте связи с пользователями *Помощник глав админа Иванов, Сотрудник_1 Центр Кузнецов, Сотрудник_2 Филиал Попов, Координатор Центр офис, Координатор Филиал* (рис. 75).

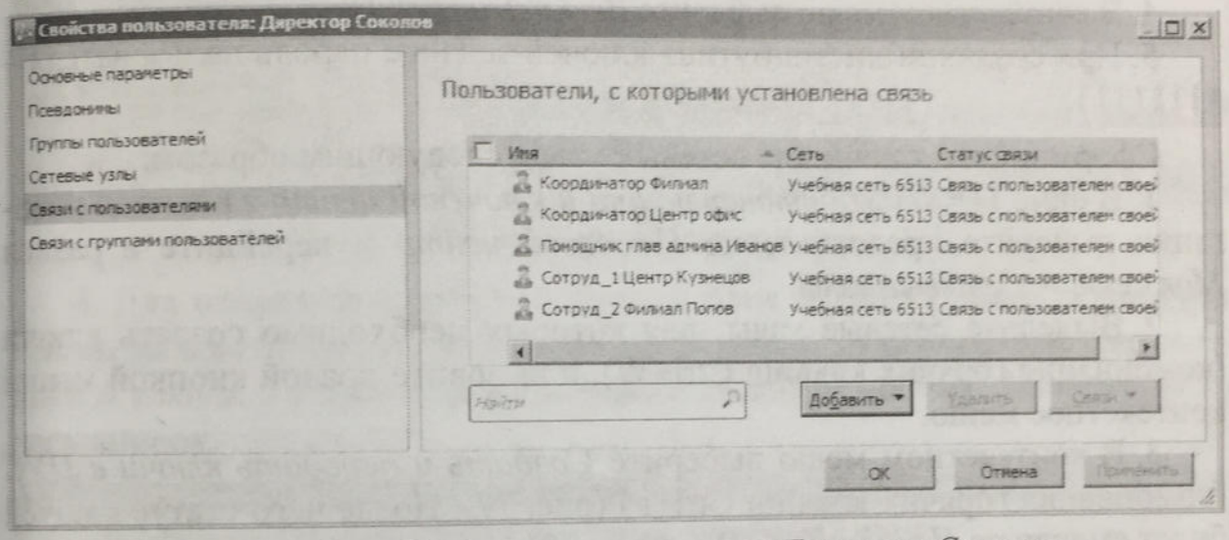

Рис. 75. Окно Свойства пользователя: Директор Соколов

Сформируйте справочники следующим образом:

В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Создать справочники...* и в открывшемся окне нажмите кнопку *Создать для всего списка* (рис. 76).

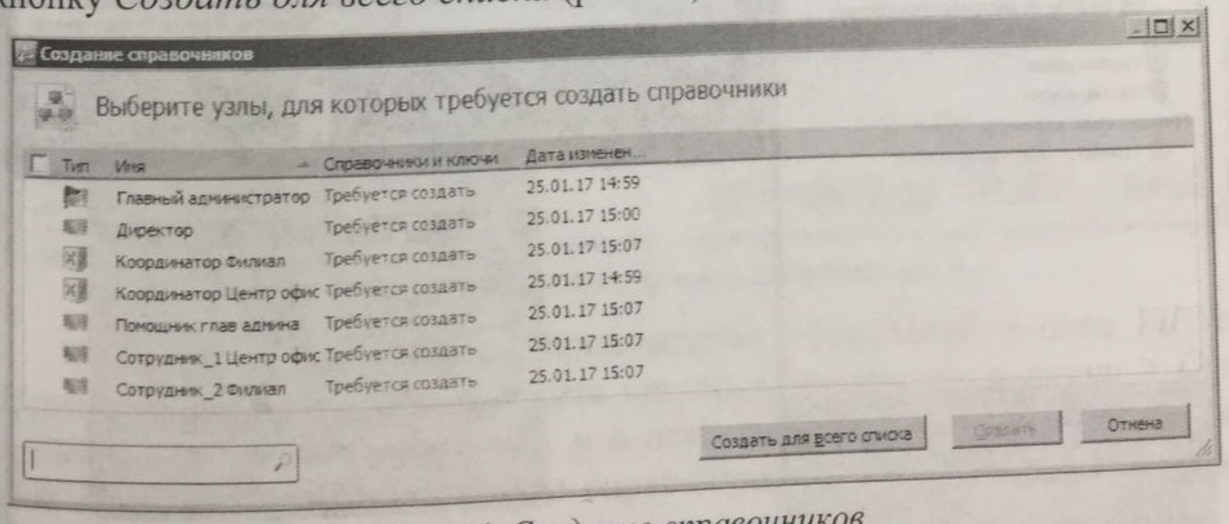

Рис. 76. Создание справочников

После формирования справочников в программе ViPNet Удостоверяющий и ключевой центр необходимо выдать дистрибутив ключей для сетевого узла *Директор* и ключи для сетевых узлов, которых коснулись изменения в ЦУС: *Главный администратор, Помощник глав админа*

Иванов, Сотрудник_1 Центр Кузнецов, Сотрудник_2 Филиал Попов, Координатор Центр офис, Координатор Филиал.

Выдайте дистрибутив ключей для пользователя *Директор Соколов* следующим образом:

1. В окне *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 сетевого узла *Директор*.
3. Выделите сетевой узел *Директор* и вызовите правой кнопкой мыши контекстное меню.
4. В контекстном меню выберите *Выдать новый дистрибутив ключей*.
5. При создании дистрибутива ключей задайте пароль пользователя – 11111111.

Сформируйте ключи для сетевых узлов следующим образом:

1. В окне *ViPNet Удостоверяющий и ключевой центр* на панели навигации выберите представление *Ключевой центр* и перейдите в раздел *Моя сеть > Сетевые узлы*.
2. Выделите сетевые узлы, для которых необходимо создать ключи (комбинация горячих клавиш Ctrl+W), и вызовите правой кнопкой мыши контекстное меню.
3. В контекстном меню выберите *Создать и передать ключи в ЦУС* (комбинация горячих клавиш Ctrl+F) (рис. 77). После чего статус ключей будет сменен на *Переданы в ЦУС* (рис. 78).

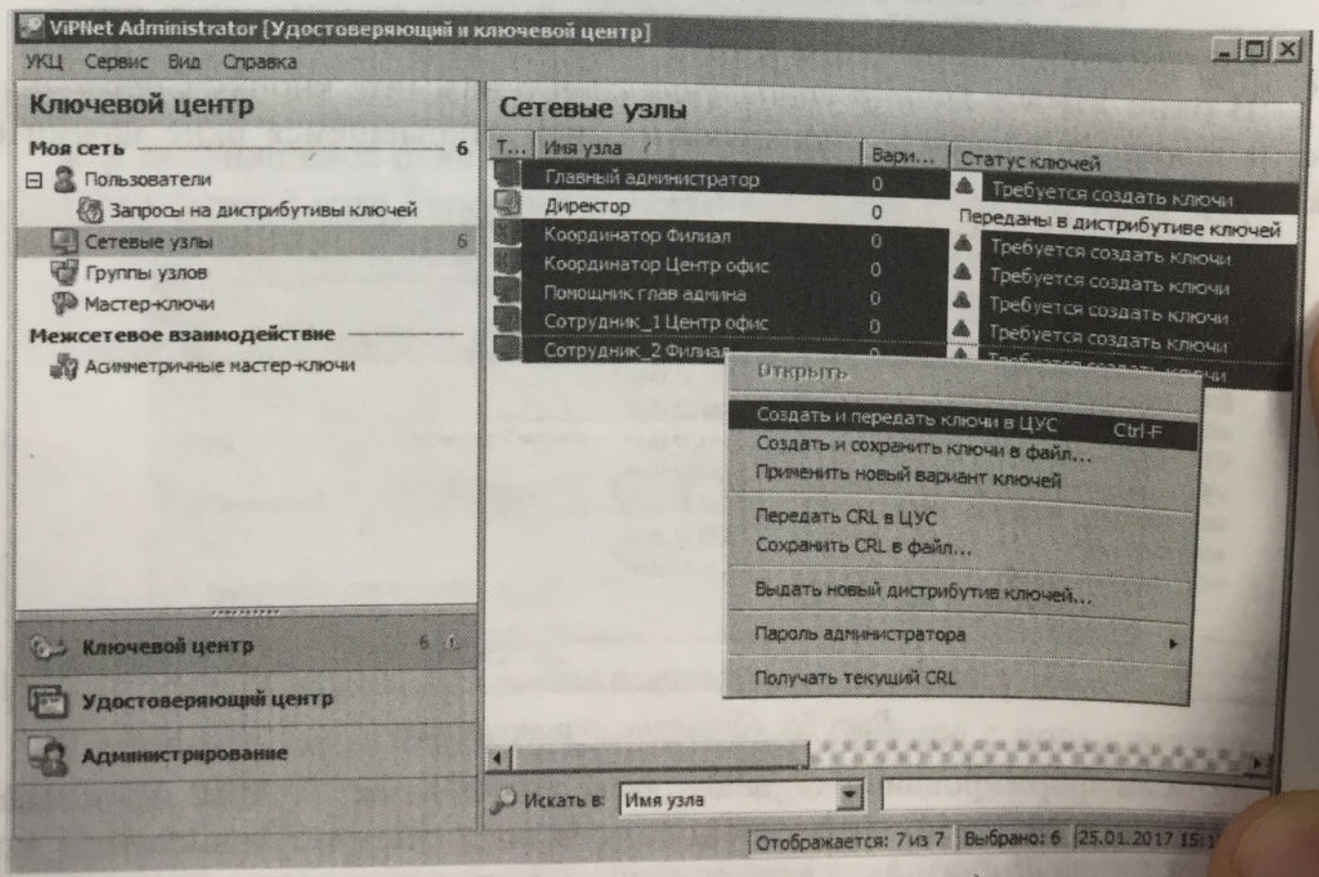

Рис. 77. Сетевые узлы, для которых необходимо создать ключи

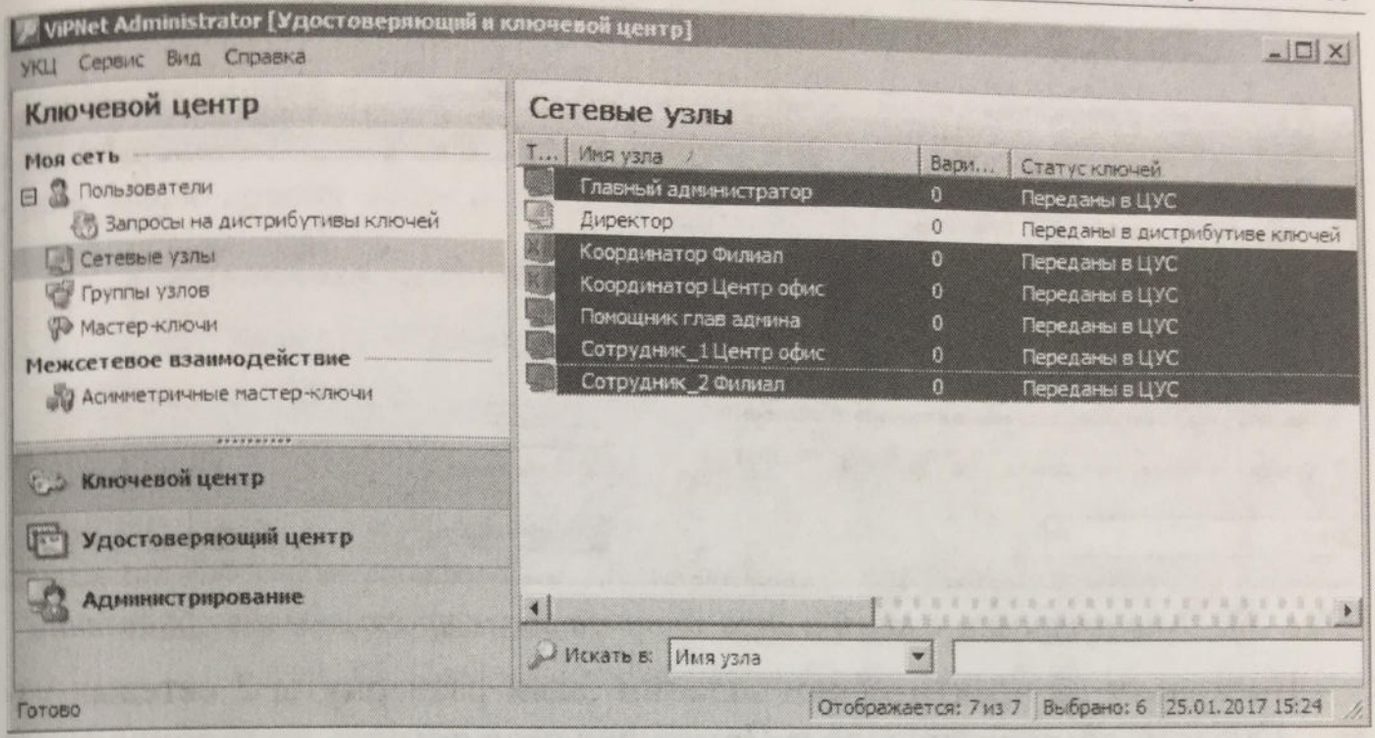

Рис. 78. Статус ключей, переданных в ЦУС

4. Для отправки ключей на узлы в окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Отправить справочники и ключи...* и в открывшемся окне нажмите кнопку *Отправить* на весь список.

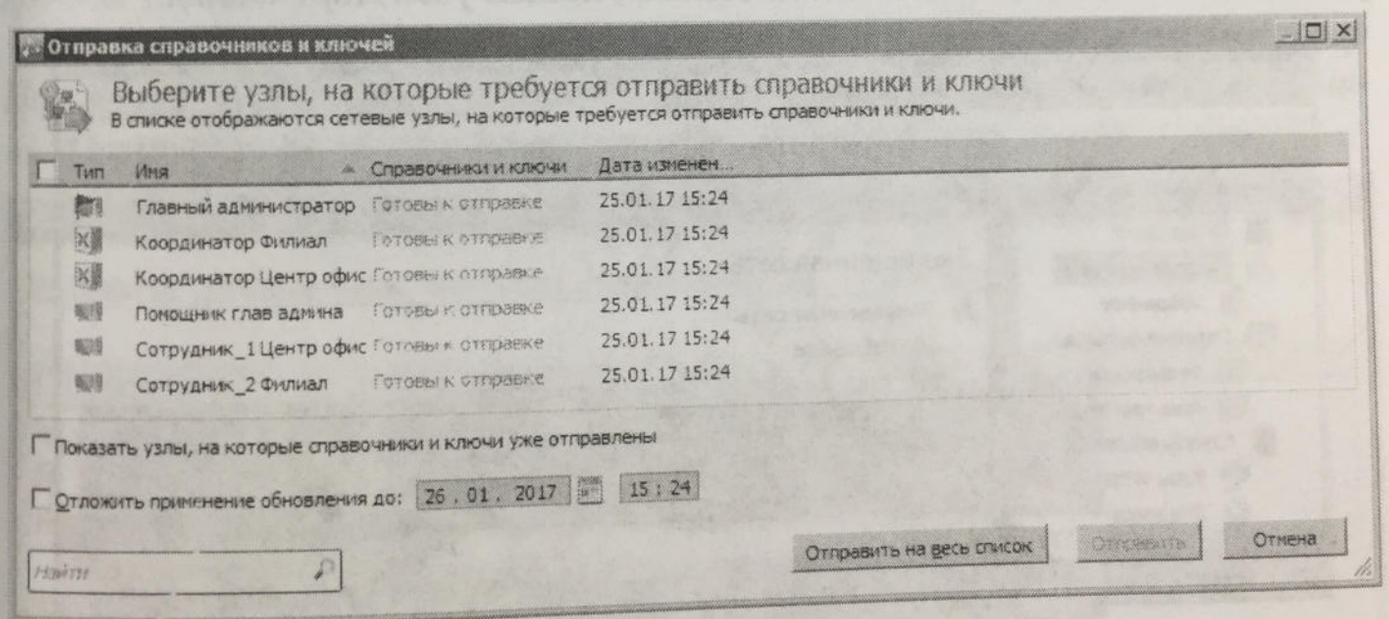

Рис. 79. Окно отправки ключей и справочников

Чтобы проверить процесс прохождения обновлений в окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Отправить справочники и ключи...* и в открывшемся окне установите флажок *Показать узлы*, на которые справочники и ключи уже отправлены (из данного меню можно повторно отправлять).

При успешном прохождении обновлений окно *Отправка справочников и ключей* примет вид, показанный на рис. 80.

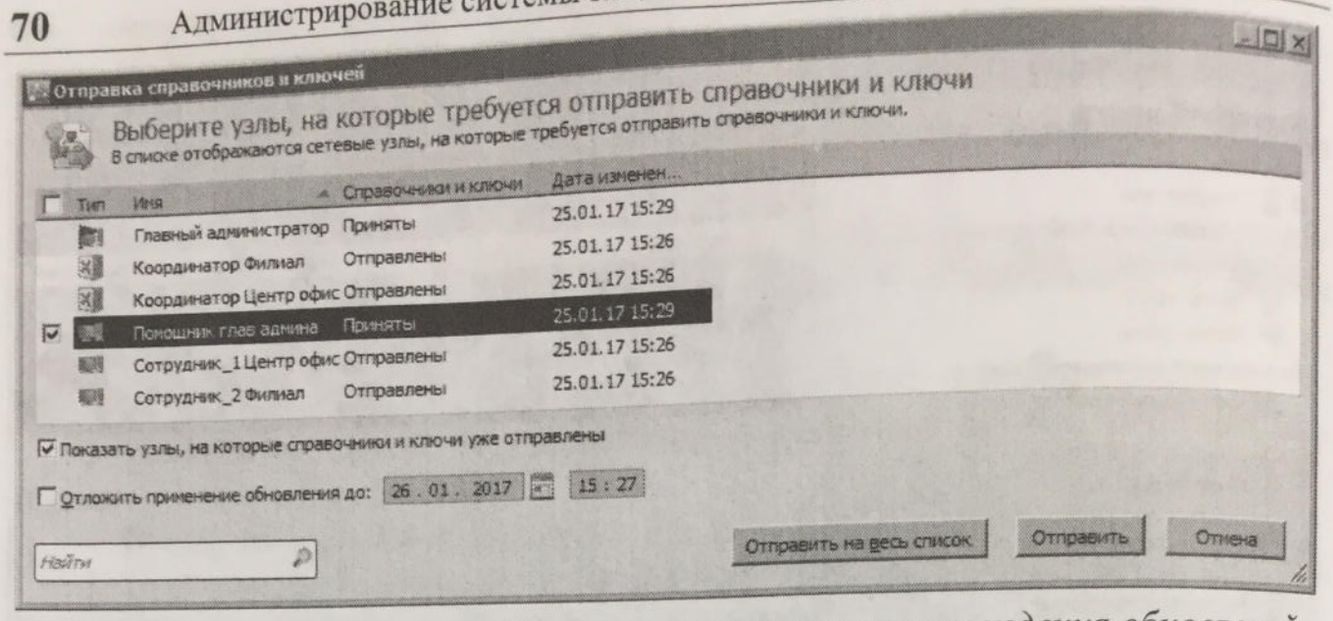

Рис. 80. Окно отправки ключей и справочников после прохождения обновлений

Поскольку на практическом задании были развернуты 2 сетевых узла – *Главный администратор* и *Помощник глав админа*, то и обновления будут приняты только на этих узлах. По умолчанию прием обновлений происходит автоматически.

При успешном обновлении окна программы *ViPNet Client Монитор* на рабочем месте *Помощник глав админа* примет вид, показанный на рис. 81 (в списке узлов должен появиться новый узел *Директор*).

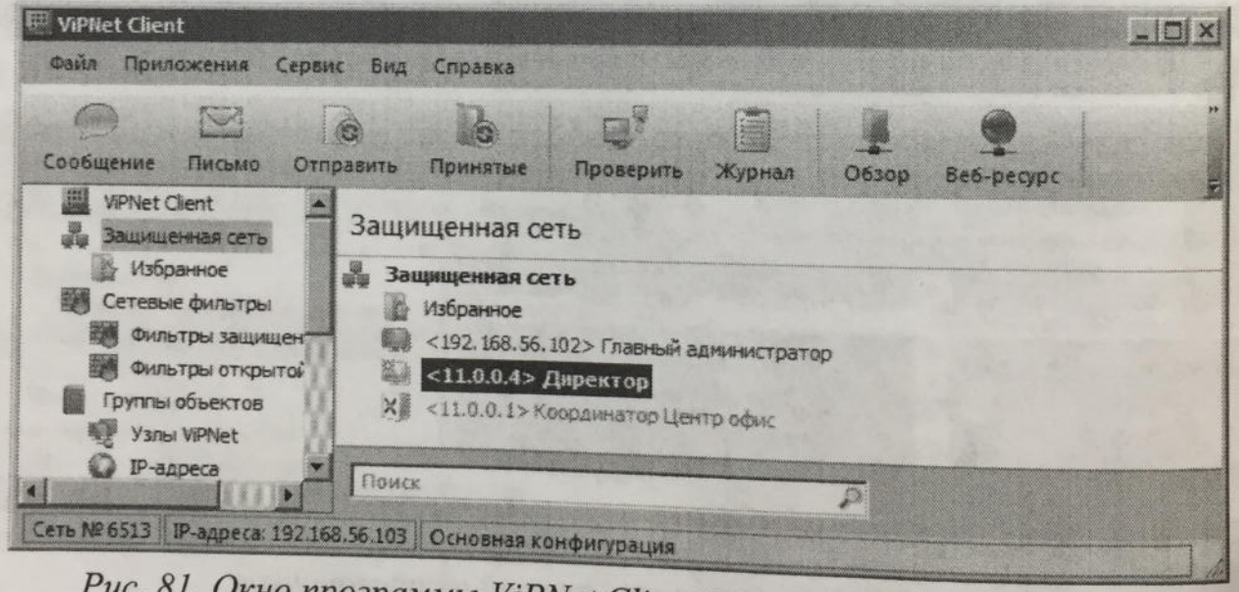

Рис. 81. Окно программы ViPNet Client Монитор после обновления

Далее необходимо создать еще пару новых сетевых узлов – клиент *Бухгалтер* с пользователем *Бухгалтер Прохорова* (для данного пользователя также потребуется установить связь с пользователями *Директор Колов, Помощник глав админа* и *Сотрудник_1 Центр Кузнецов*) в центральном офисе компании, клиент *Сотрудник_3 Филиал* с пользователем *Сотруд_3 Филиал Горохов* (для данного пользователя также потребуется установить связь с пользователем *Сотрудник_2 Филиал Попов*) в филиале компании. Сформировать справочники и ключи, разослать их на узлы.

2.1.2. Создание групп узлов

Для создания групп узлов *Центральный офис* и *Филиал* в разделе *Группы узлов* окна *ViPNet Центр управления сетью* нажмите кнопку *Создать новую группу узлов* и задайте имя *Центральный офис*.

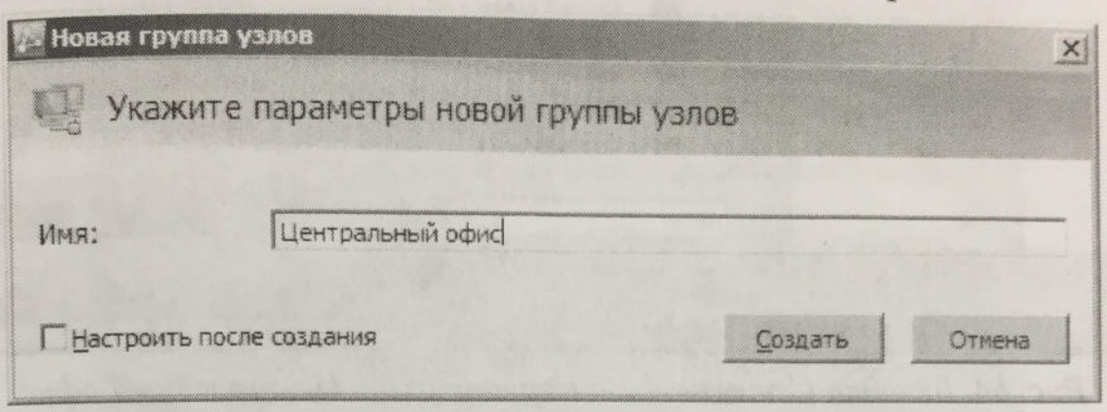

Рис. 82. Создание группы узлов Центральный офис

Аналогичным образом создайте группу узлов *Филиал*.

Добавьте узлы в группу *Центральный офис*. Для этого выполните следующие действия:

1. В разделе *Группы узлов* окна *ViPNet Центр управления сетью* выделите группу узлов *Центральный офис* и нажмите кнопку *Свойства группы узлов*.

2. Перейдите на вкладку Сетевые узлы и добавьте узлы *Координатор Центр офис, Директор, Главный администратор, Помощник глав администратора, Сотрудник_1 Центр офис, Бухгалтер* (рис. 83).

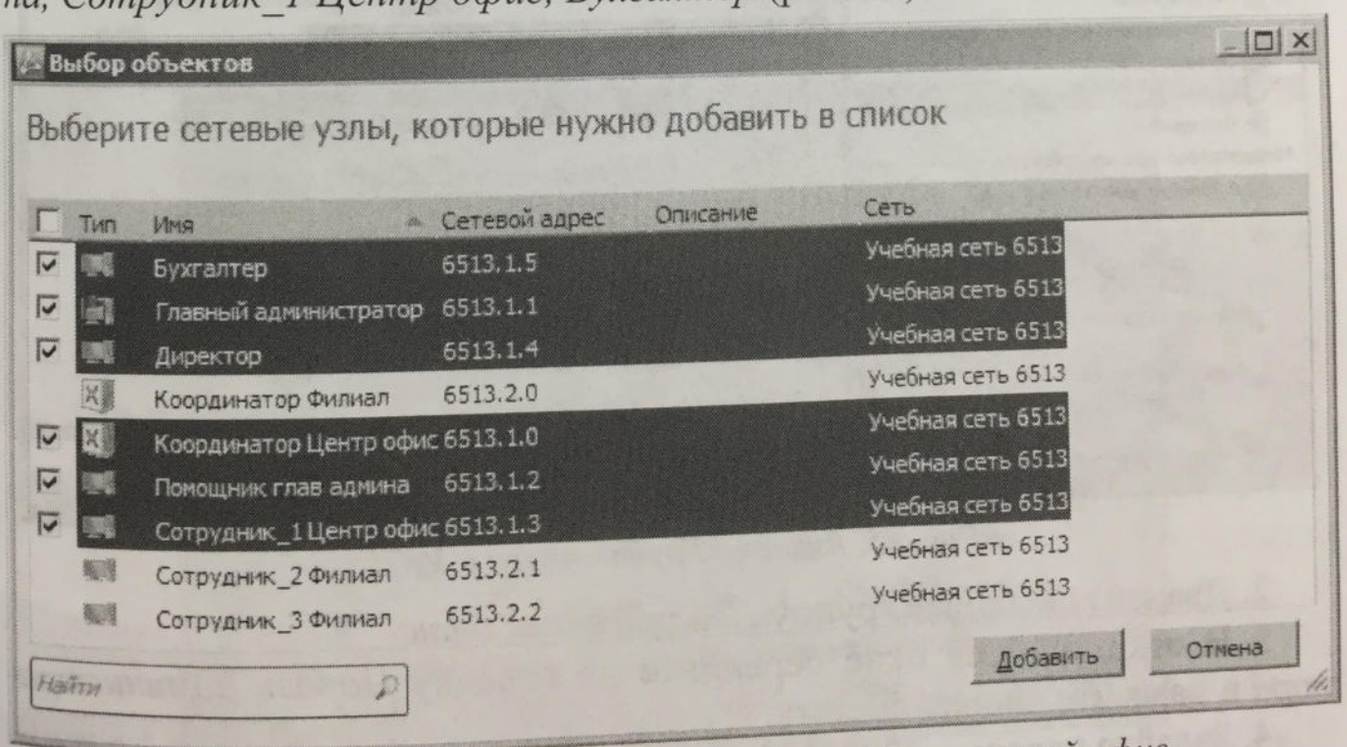

Рис. 83. Добавление узлов в группу узлов Центральный офис

В результате вкладка *Сетевые узлы* примет вид, показанный на (рис. 84).

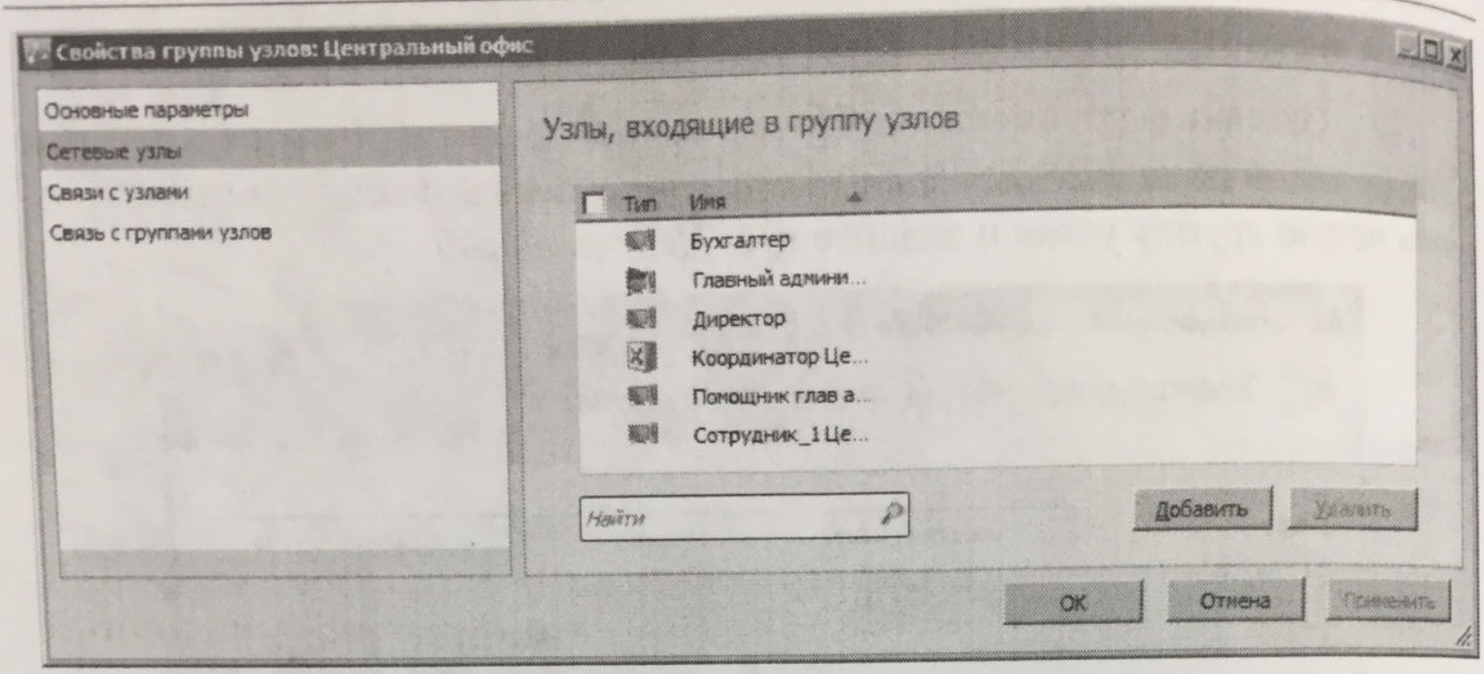

Рис. 84. Вкладка Сетевые узлы в группе узлов Центральный офис

Аналогичным образом добавьте узлы *Координатор Филиал*, *Сотрудник_2 Филиал*, *Сотрудник_3 Филиал в группу узлов Филиал*.

Задайте пароль администратора для группы узлов *Центральный офис*. Для этого выполните следующие действия:

1. Перейдите в раздел *Группы узлов* окна *ViPNet Удостоверяющий и ключевой центр* (рис. 85).

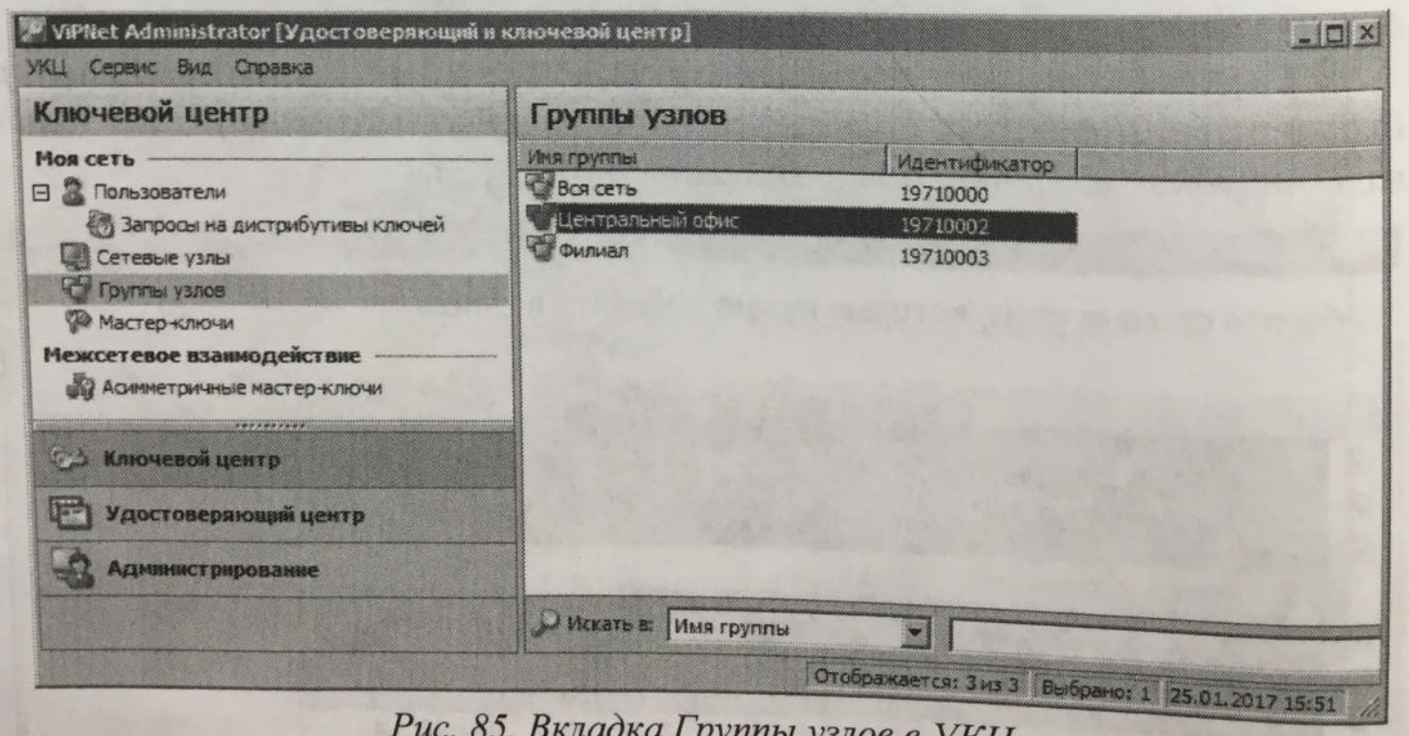

Рис. 85. Вкладка Группы узлов в УКЦ

2. Дважды щелкните группу *Центральный офис*.

3. В открывшемся окне перейдите на вкладку *Пароль администратора* и нажмите кнопку создать.

4. Задайте пароль – 22222222 и нажмите *ОК* (рис. 86).

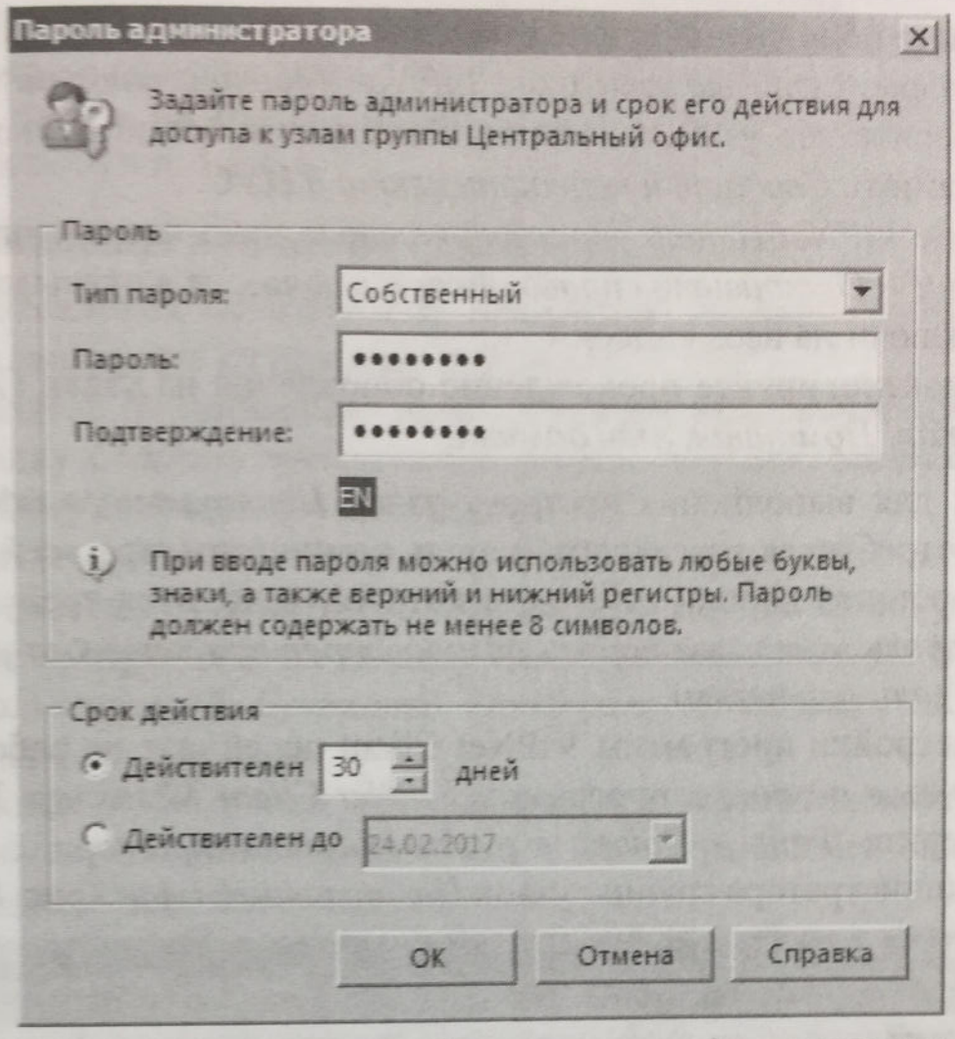

Рис. 86. Создание пароля администратора для группы узлов

Созданный пароль отобразится на вкладке *Пароль администратора* (рис. 87).

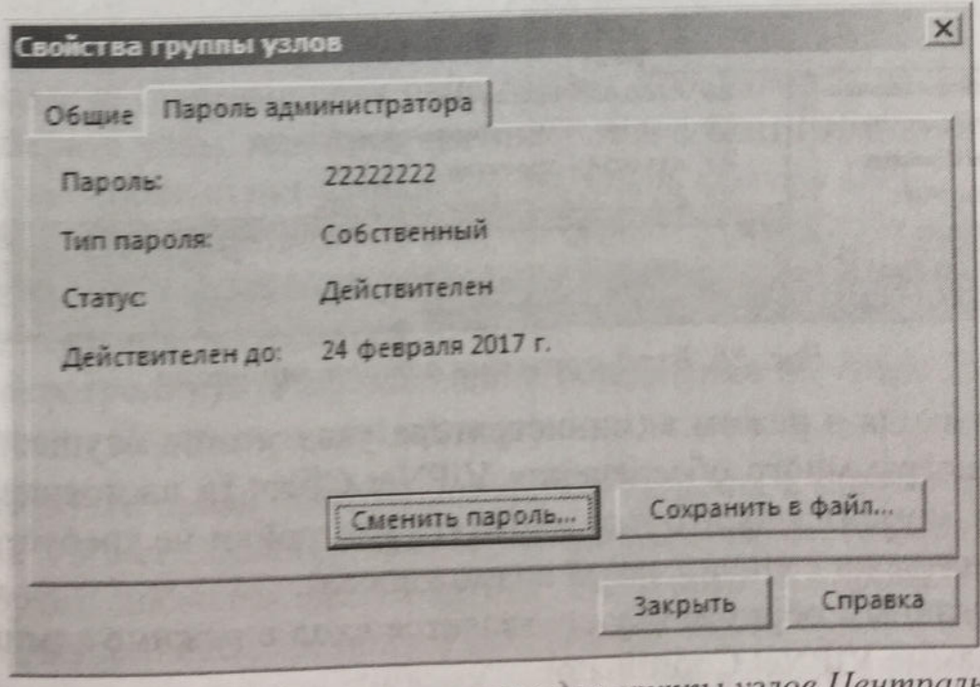

Рис. 87. Вкладка Пароль администратора для группы узлов Центральный офис

Аналогичным образом задайте пароль администратора для группы узлов *Филиал* – 33333333.

Отправьте обновления ключей на узлы следующим образом:

1. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выберите все узлы, вызовите контекстное меню правой кнопкой мыши и нажмите *Создать и передать ключи в ЦУС*.

2. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Отправить справочники и ключи...* и в открывшемся окне отправьте ключи на весь список.

3. Проконтролируйте прохождение обновления на узлах *Главный администратор, Помощник глав админа*.

Теперь для выполнения настроек узлов *Центрального офиса* и *Филиала* не потребуется разглашать пароль администратора всей сети, достаточно сообщить пароль группы, в которой находится требуемый узел *(данный пароль, а также пароль администратора сетевого узла нельзя сообщать пользователям)*.

Для настройки программы ViPNet Client перейдите на рабочее место *Помощник глав админа* в программу *ViPNet Client Монитор*. В верхнем меню выберите *Файл > Войти в режим администратора...* и введите пароль администратора группы узлов *Центральный офис* (рис. 88).

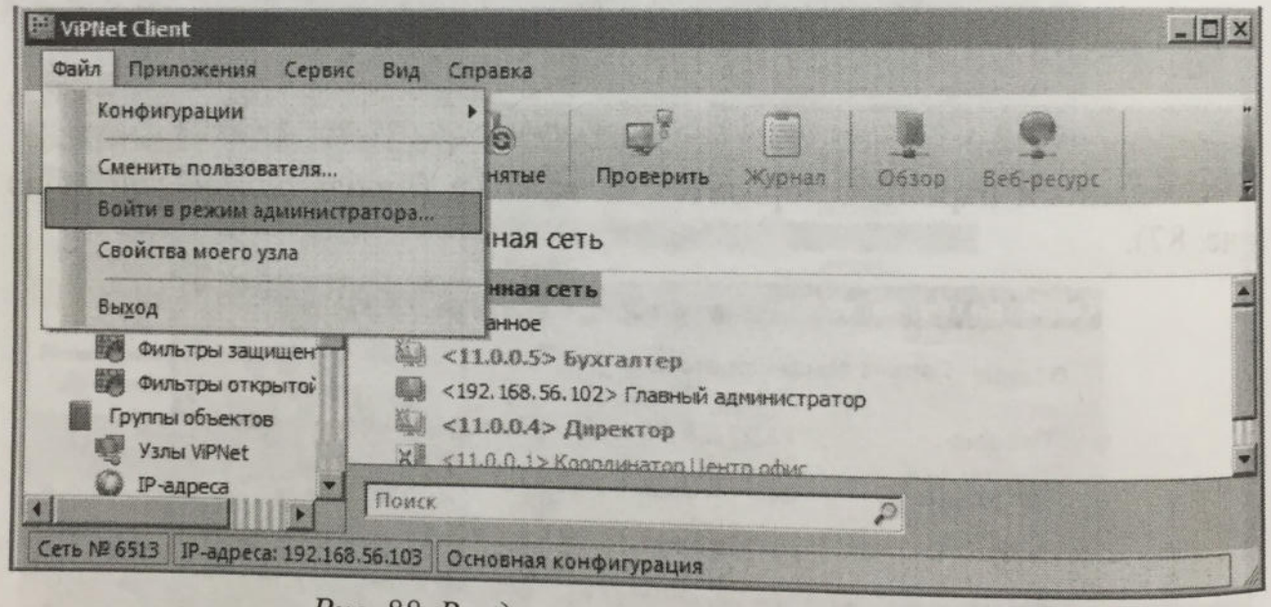

Рис. 88. Вход в режиме администратора

После входа в режим администратора узла можно осуществлять настройку программного обеспечения ViPNet Client (в настоящем задании на данный момент вносить или изменять настройки не требуется, достаточно убедиться в наличии такой возможности).

Аналогичным образом осуществляется вход в режиме администратора в программе ViPNet Coordinator.

Примечание. В случае если по установленным в организации правилам нельзя разглашать пароль администратора группы и нет возможности администратору группы присутствовать в удаленных офисах, но требуется обеспечить возможность производить настройки програм-

мы *ViPNet Client/Coordinator*, нужно задать пароль администратора для каждого сетевого узла. Для этого необходимо кликнуть на узел и задать пароль на вкладке *Пароль администратора*. (Подробно рассказывалось в п. 1.2.5.)

2.1.3. Добавление нового пользователя

Для добавления пользователя *Бухгалтер Захарова* на сетевой узел *Бухгалтер* выполните следующие действия:

1. В разделе *Пользователи* окна *ViPNet Центр управления сетью* нажмите кнопку *Создать нового пользователя*, задайте имя *Бухгалтер Захарова* и выберите сетевой узел *Бухгалтер*.

2. В разделе *Пользователи* окна *ViPNet Центр управления сетью* выделите пользователя *Бухгалтер Захарова*, нажмите кнопку *Свойства пользователя*, перейдите на вкладку *Связи с пользователями* и добавьте в список пользователей *Бухгалтер Прохорова, Помощник глав админа, Сотруд_1 Центр Кузнецов.*

3. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Создать справочники...* и в открывшемся окне нажмите кнопку *Создать* для всего списка.

4. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выделите узел *Бухгалтер*, в контекстном меню выберите пункт *Выдать новый дистрибутив ключей*. При создании дистрибутива ключей задайте пароль пользователя *Бухгалтер Захарова* – 11111111.

5. Передайте доверенным способом дистрибутив ключей и пароль пользователю *Бухгалтер Захарова (в рамках настоящего задания передавать дистрибутив ключей никуда не надо).*

6. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выберите узлы, для которых требуется создать ключи, в контекстном меню выберите пункт *Создать и передать ключи в ЦУС.*

7. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Отправить справочники и ключи...* и в открывшемся окне отправьте ключи на весь список.

8. Проконтролируйте прохождение обновления на узлах *Главный администратор, Помощник глав админа.*

В результате правильного выполнения задания в списке адресатов в программе ViPNet Client Деловая почта на рабочем месте *Помощник глав админа* будет добавлен пользователь *Бухгалтер Захарова.* Чтобы это проверить, выполните следующие действия:

1. Откройте программу ViPNet Client Деловая почта на рабочем месте *Помощник глав админа* (*Пуск > Все программы > ViPNet > ViPNet Client > Деловая почта*) (рис. 89).

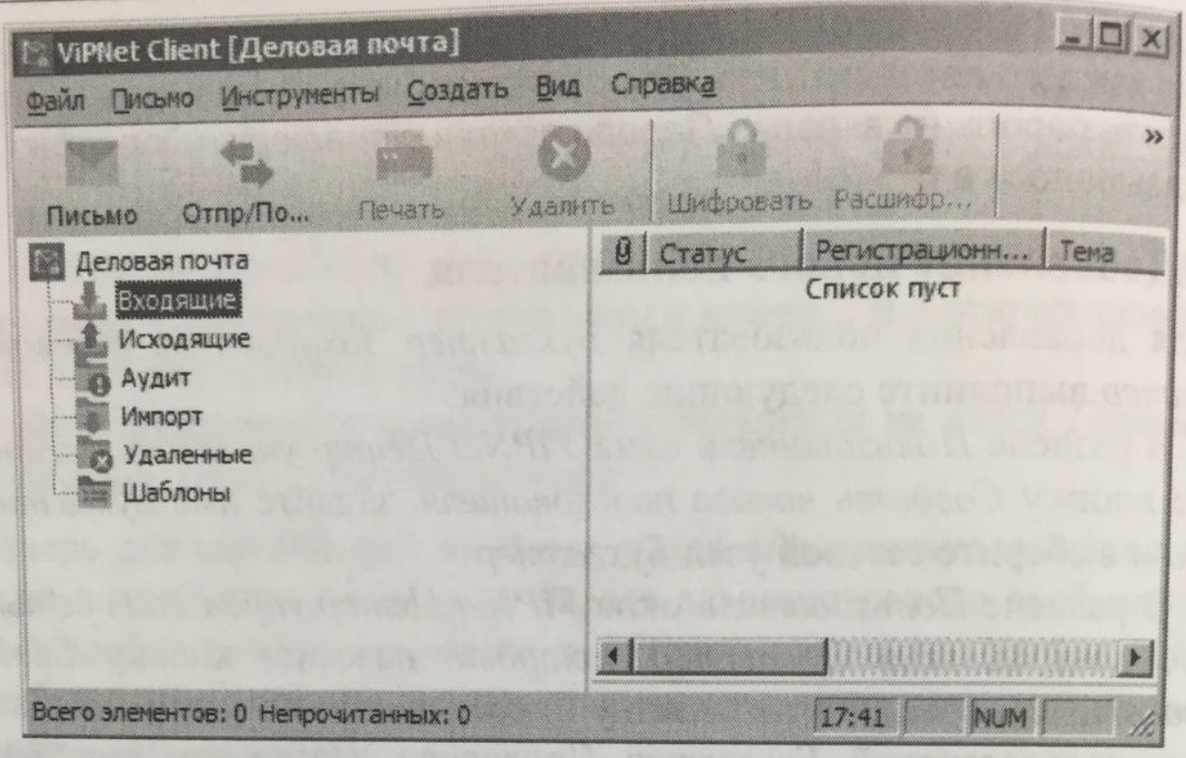

Рис. 89. Общий вид программы ViPNet Client Деловая почта

2. В меню *Инструменты* выберите пункт *Адресная книга...* и убедитесь, что пользователь *Бухгалтер Захарова* добавилась в список (рис. 90).

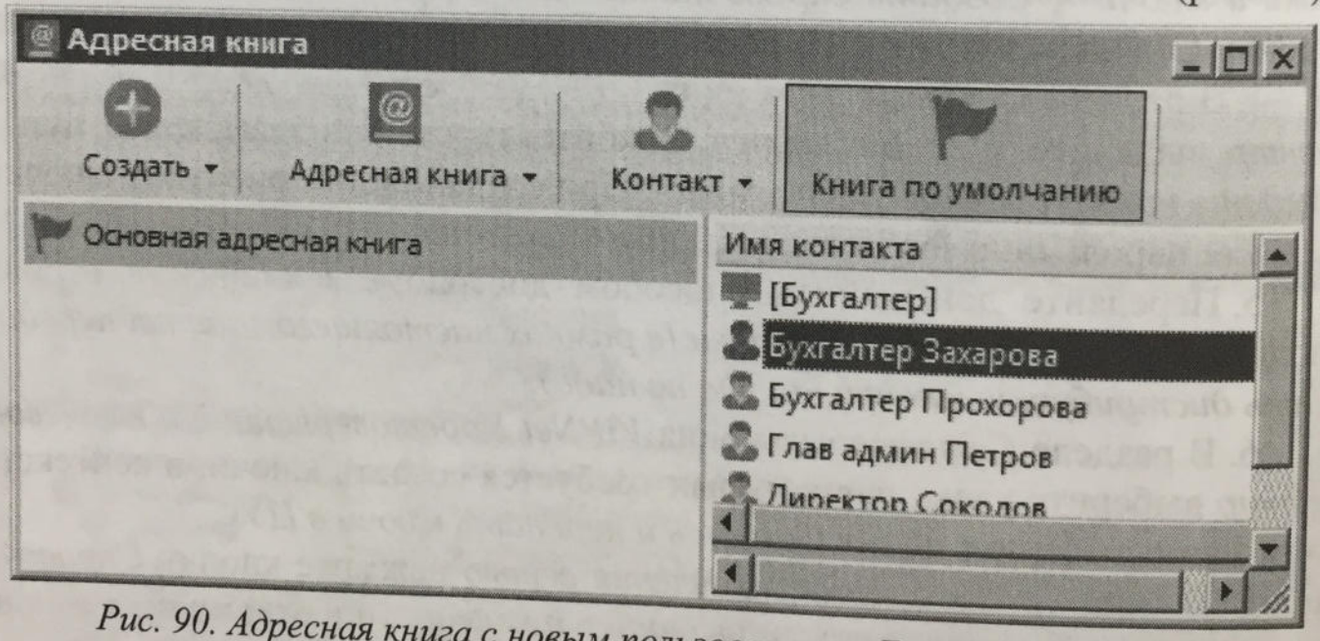

Рис. 90. Адресная книга с новым пользователем Бухгалтер Захарова

2.1.4. Удаление связей пользователей

Для удаления связи пользователей *Бухгалтер Захарова* и *Помощник глав админа Иванов* выполните следующие действия:

1. В разделе *Пользователи* окна *ViPNet Центр управления сетью* выделите пользователя *Бухгалтер Захарова*, нажмите кнопку *Свойства пользователя*.

2. Перейдите на вкладку *Связи с пользователями*, в списке пользователей отметьте *Помощник глав админа Иванов* и нажмите кнопку *Удалить*.

3. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Создать справочники...* и в открывшемся окне нажмите кнопку *Создать для всего списка*.

4. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выберите узлы, для которых требуется создать ключи, в контекстном меню выберите пункт *Создать и передать ключи в ЦУС*.

5. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Отправить справочники и ключи...* и в открывшемся окне отправьте ключи на весь список.

6. Проконтролируйте прохождение обновления на узле *Помощник глав админа*.

В результате правильного выполнения задания в списке адресатов в программе ViPNet Client Деловая почта на рабочем месте *Помощник глав админа* будет удален пользователь *Бухгалтер Захарова* (рис. 91).

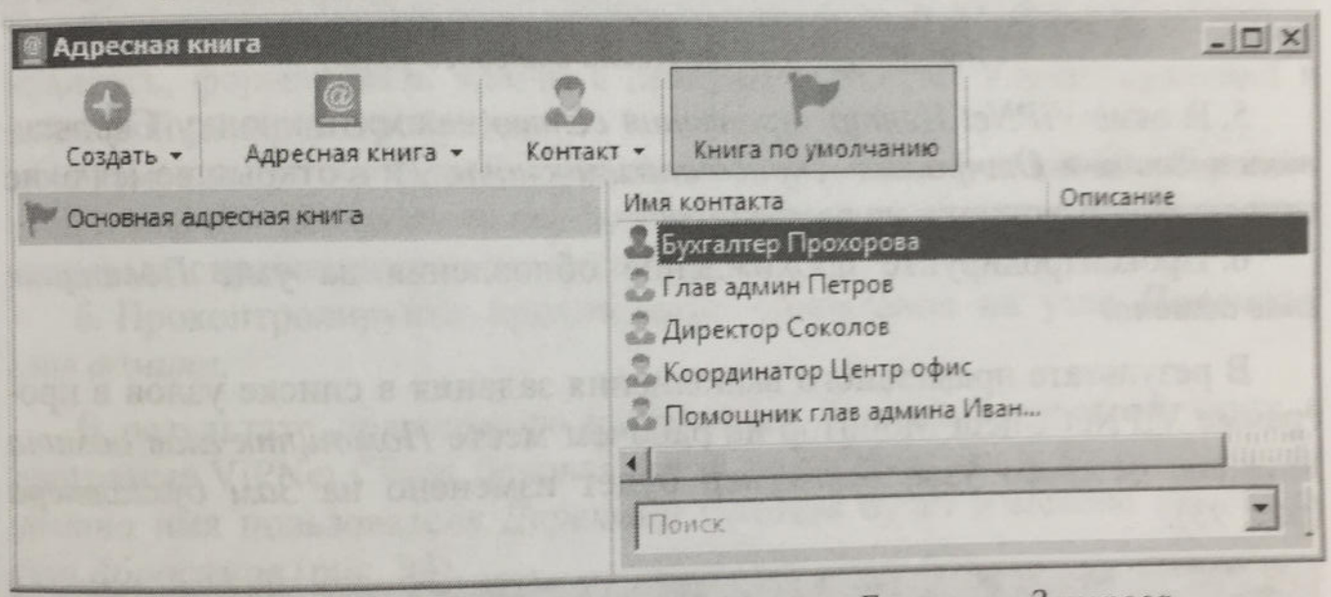

Рис. 91. Адресная книга без пользователя Бухгалтер Захарова

2.1.5. Изменение названия сетевого узла

Для изменения названия сетевого узла *Бухгалтер* на *Зам бухгалтера* выполните следующие действия:

1. В окне *ViPNet Центр управления сетью* выберите раздел *Клиенты*, выделите узел *Бухгалтер* и нажмите кнопку *Свойства клиента*.

2. В свойствах клиента *Бухгалтер* измените название сетевого узла на *Зам бухгалтера* и нажмите кнопку *ОК* (рис. 92).

3. В окне *ViPNet Центр управления* сетью нажмите кнопку *Справочники и ключи > Создать справочники...* и в открывшемся окне нажмите кнопку Создать для всего списка.

4. Поскольку изменений в связях узлов или пользователей не производилось, формировать ключи в программе ViPNet Удостоверяющий и ключевой центр не требуется.

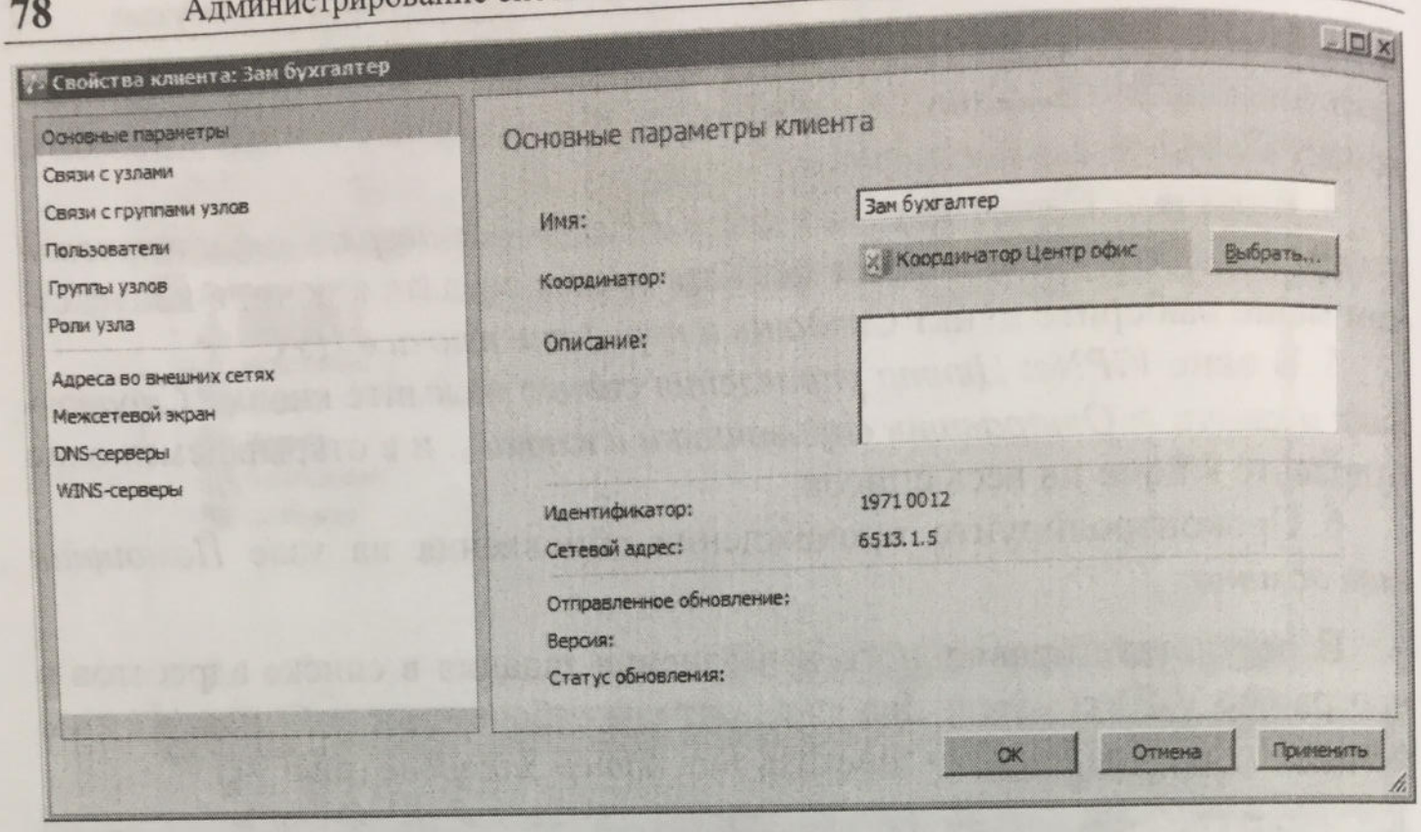

Рис. 92. Изменение имени сетевого узла

5. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи > Отправить справочники и ключи...* и в открывшемся окне отправьте справочники на весь список.

6. Проконтролируйте прохождение обновления на узле *Помощник глав админа*.

В результате правильного выполнения задания в списке узлов в программе ViPNet Client Монитор на рабочем месте *Помощник глав админа* название сетевого узла *Бухгалтер* будет изменено на *Зам бухгалтера* (рис. 93).

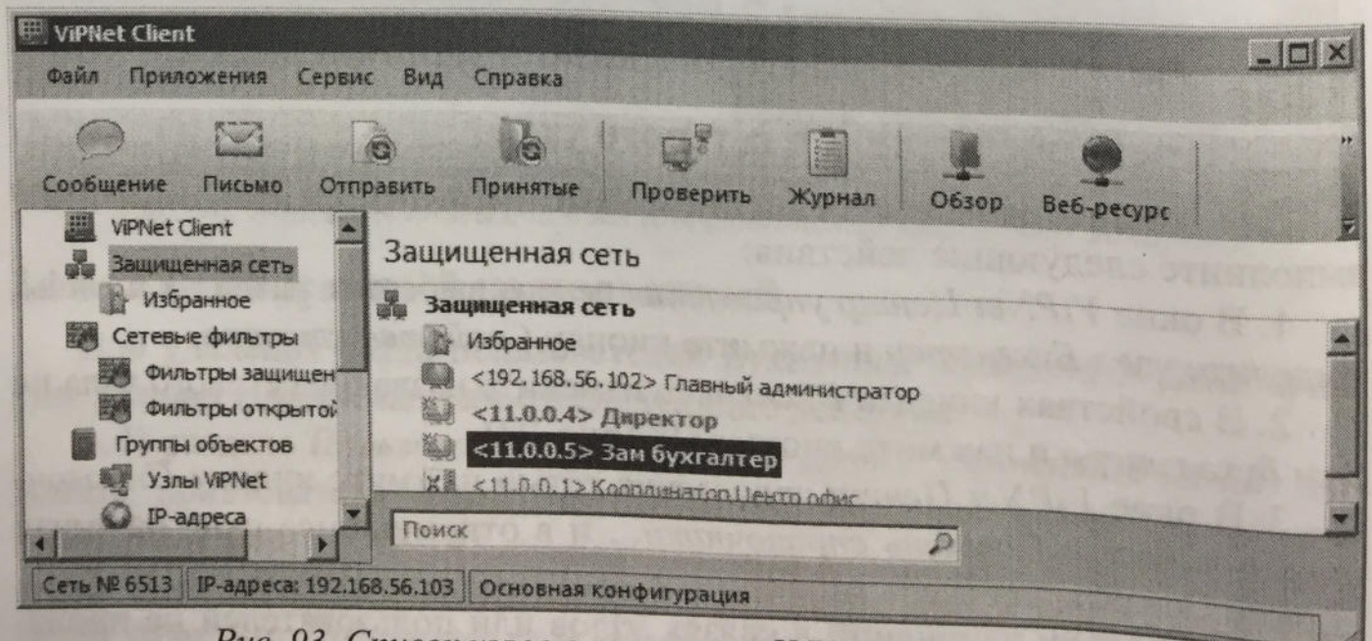

Рис. 93. Список узлов в программе ViPNet Client Монитор

2.1.6. Изменение имени пользователя

Для изменения имени пользователя *Директор Соколов* на *Директор Абросимов* выполните следующие действия:

1. В окне *ViPNet Центр управления сетью* выберите раздел *Пользователи*, выделите пользователя *Директор Соколов* и нажмите кнопку *Свойства пользователя*.

2. В свойствах пользователя *Директор Соколов* измените имя на *Директор Абросимов* и нажмите кнопку *ОК*. Появиться диалоговое окно, в котором будет сообщаться, что данный пользователь единственный на данном узле и вам нужно выбрать переименовывать узел или нет. В данной ситуации переименование узла не требуется, поэтому нажмите кнопку *Нет*.

3. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Создать справочники…* и в открывшемся окне нажмите кнопку *Создать для всего списка*.

4. Поскольку изменений в связях узлов или пользователей не производилось, формировать ключи в программе ViPNet Удостоверяющий и ключевой центр не требуется.

5. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Отправить справочники и ключи…* и в открывшемся окне отправьте справочники на весь список.

6. Проконтролируйте прохождение обновления на узле *Помощник глав админа*.

В результате правильного выполнения задания в адресной книге в программе ViPNet Client Деловая почта на рабочем месте *Помощник глав админа* имя пользователя *Директор Соколов* будет изменено на *Директор Абросимов* (рис. 94).

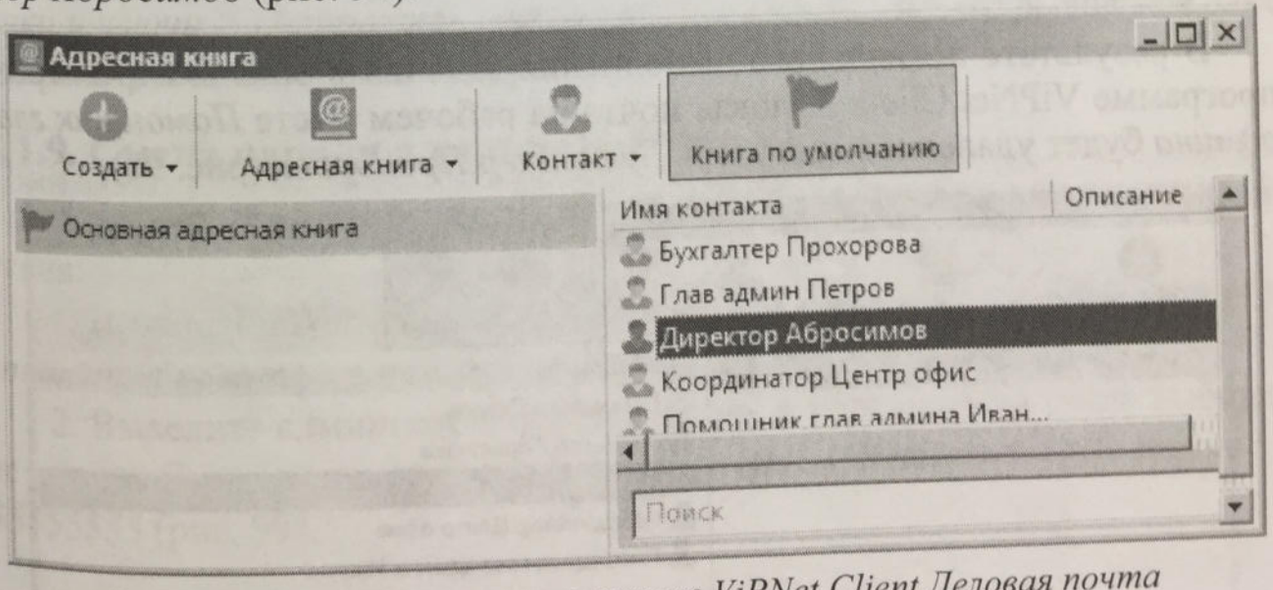

Рис. 94. Адресная книга в программе ViPNet Client Деловая почта

Аналогичным образом переименуйте пользователя *Бухгалтер Захарова* в *Зам бухгалтера Захарова*, так как в предыдущем задании имя ее узла было изменено.

2.1.7. Удаление пользователя

Для удаления пользователя *Бухгалтер Прохорова* выполните следующие действия:

1. В разделе *Пользователи* окна *ViPNet Центр управления сетью* выберите пользователя *Бухгалтер Прохорова* и нажмите кнопку *Удалить*. При этом удалять клиента, на котором зарегистрирован пользователь не требуется (рис. 95).

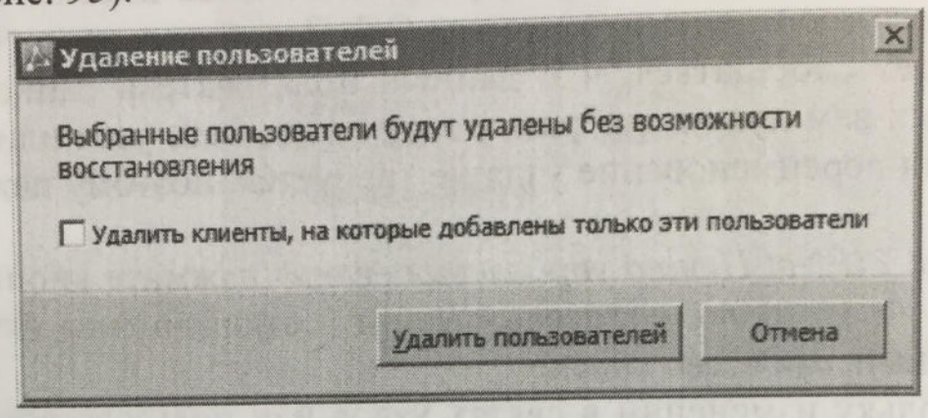

Рис. 95. Удаление пользователя

2. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Создать справочники...* и в открывшемся окне нажмите кнопку *Создать для всего списка*.

3. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выберите узлы, для которых требуется создать ключи, в контекстном меню выберите пункт *Создать и передать ключи в ЦУС*.

4. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Отправить справочники и ключи...* и в открывшемся окне отправьте ключи на весь список.

5. Проконтролируйте прохождение обновления на узле *Помощник глав админа*.

В результате правильного выполнения задания в списке адресатов в программе ViPNet Client Деловая почта на рабочем месте *Помощник глав админа* будет удален пользователь *Бухгалтер Прохорова* (рис. 96).

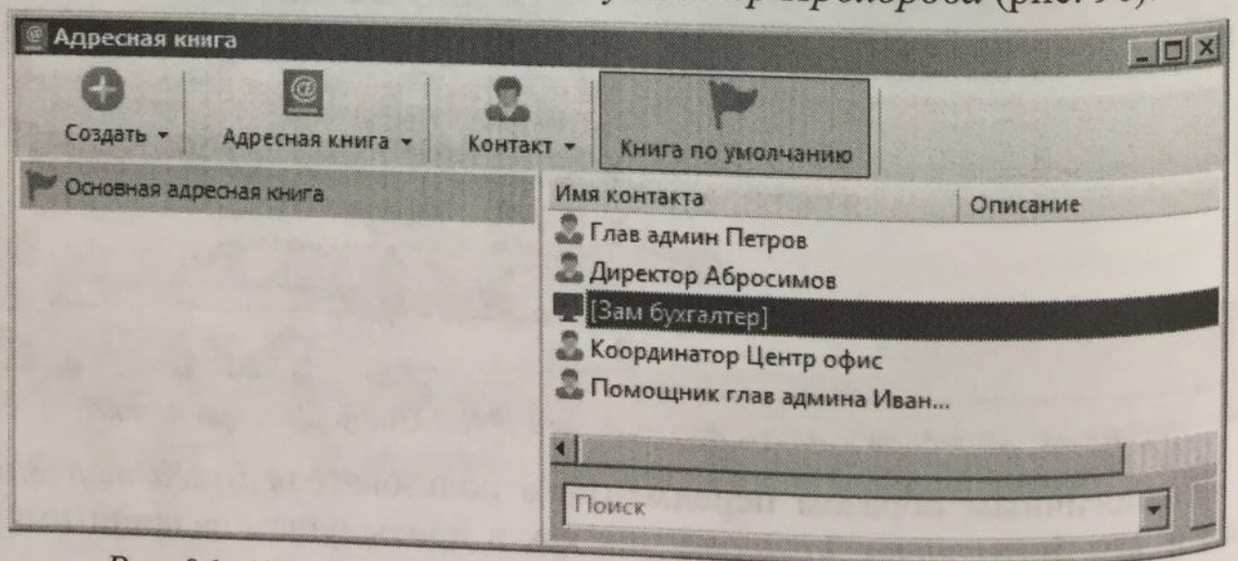

Рис. 96. Адресная книга без пользователя Бухгалтер Прохорова

2.1.8. Удаление сетевого узла

Для удаления сетевого узла *Сотрудник_3 Филиал* выполните следующие действия:

1. В разделе *Клиенты окна ViPNet Центр управления сетью* выделите сетевой узел *Сотрудник_3 Филиал*, нажмите кнопку *Удалить* и установите флажок Удалить пользователей, зарегистрированных только на удаляемых сетевых узлах в диалоговом окне (рис. 97).

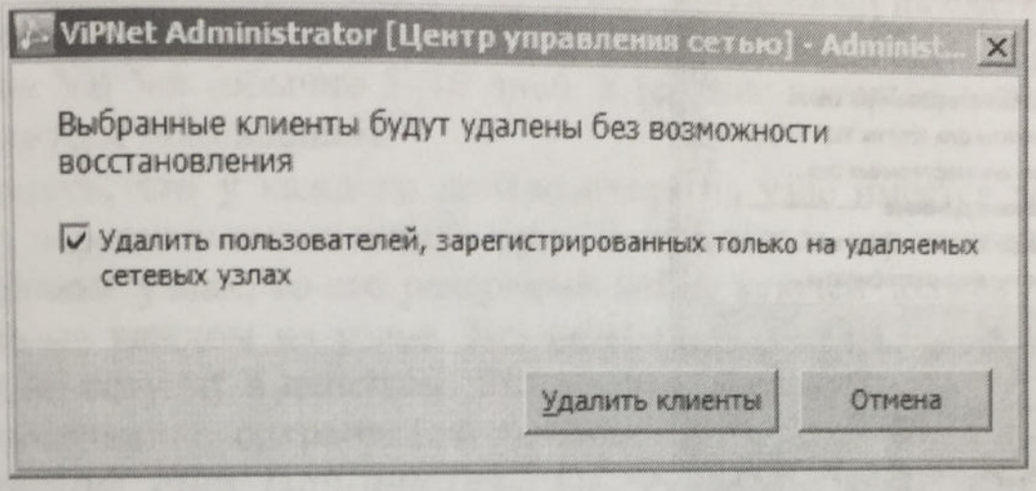

Рис. 97. Удаление сетевого узла

2. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи* > *Создать справочники...* и создайте справочники для всех узлов, которые были связаны с клиентом *Сотрудник_3 Филиал*.

3. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выберите узлы, для которых требуется создать ключи, в контекстном меню выберите пункт *Создать и передать ключи в ЦУС*.

4. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи* > *Отправить справочники и ключи...* и в открывшемся окне отправьте ключи на весь список.

2.1.9. Смена пароля администратора УКЦ

Для смены пароля администратора УКЦ выполните следующие действия:

1. В окне *ViPNet Удостоверяющий и ключевой центр* выберите *Администрирование*, а в нем раздел *Администраторы* (рис. 98).

2. Выделите администратора *Владимир*, в контекстном меню выберите пункт *Сменить пароль администратора...* Задайте новый пароль – 55555555 (рис. 99).

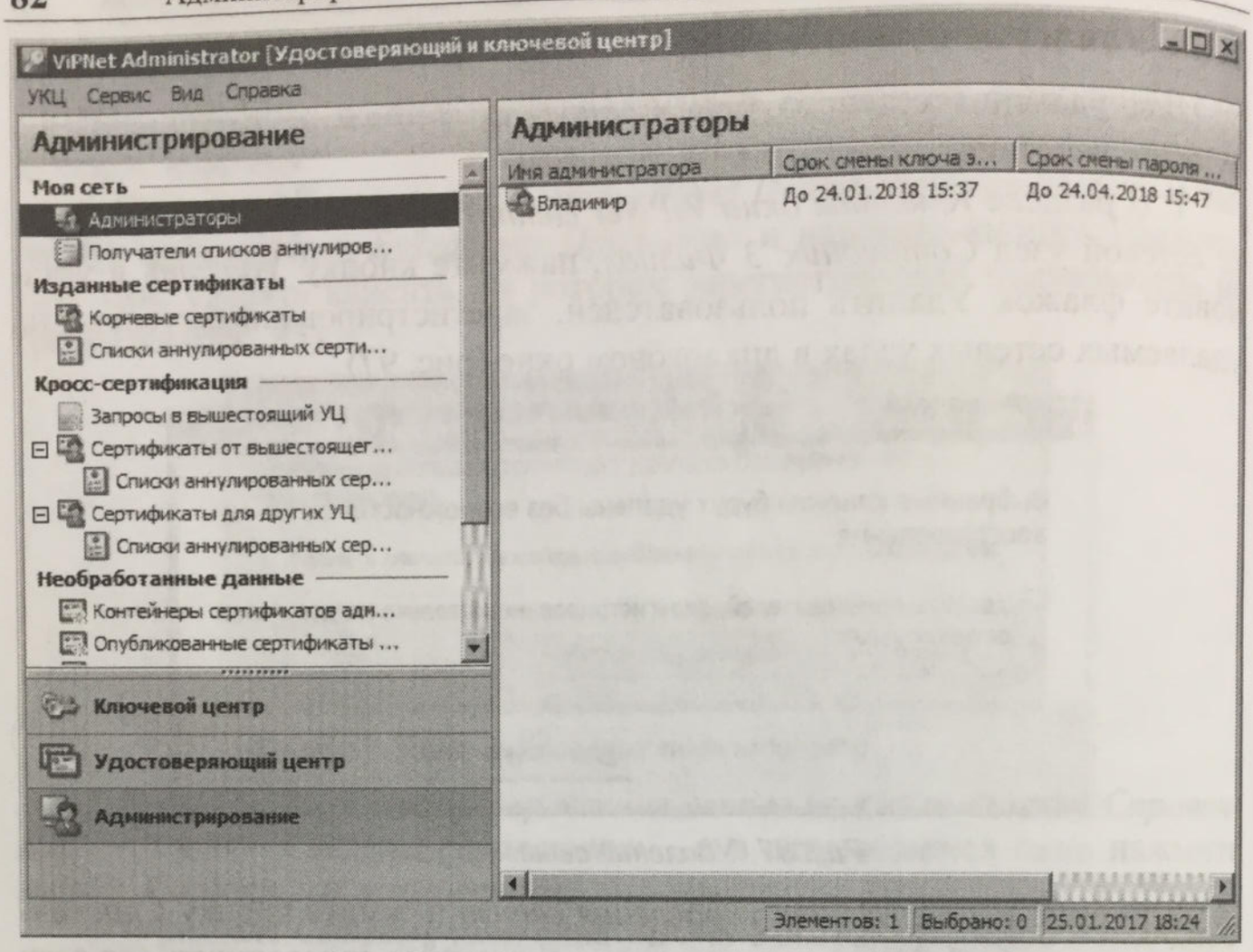

Рис. 98. Раздел Администраторы в УКЦ

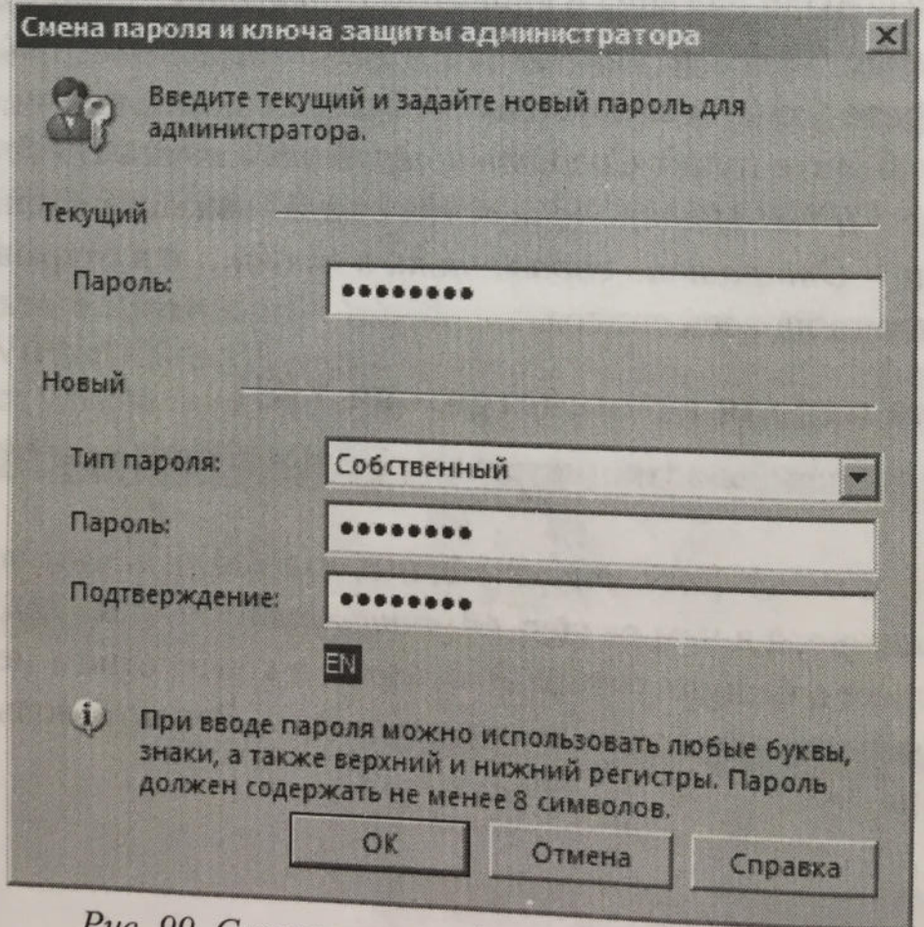

Рис. 99. Смена пароля администратора УКЦ

2.1.10. Смена мастер-ключей

Смена мастер-ключей влечет за собой смену всех ключей в сети ViPNet. Она может быть, как плановой, так и внеплановой. Плановая смена мастер-ключей проводится с определенной периодичностью, обычно не реже одного раза в год. Внеплановая смена мастер-ключей производится при компрометации ключей.

Перед сменой мастер-ключей выполните следующие действия:

- Убедитесь, что в промежуток времени, отведенный на смену мастер-ключей, все пользователи сети ViPNet смогут выполнить вход в программу ViPNet (обычно 5–10 дней, в течение которых нельзя проводить другие обновления).
- Убедитесь, что у каждого пользователя на узле имеется резервный набор персональных ключей. Если пользователь зарегистрирован на нескольких узлах, то его резервный набор ключей должен присутствовать на каждом из узлов. Без резервного набора новые ключи на узлах не вступят в действие. Резервный набор персональных ключей по умолчанию сохраняется в папке установки ViPNet (пример: *C:\Program Files (x86)\InfoTeCS\ViPNet Client\user_<**** - вместо звездочек должен быть идентификатор узла>\key_disk\dom*.pk*)
- Проинформируйте всех пользователей и администраторов сети ViPNet о планируемом обновлении ключей и сроках его проведения.
- Рекомендуйте пользователям расшифровать все сообщения программы ViPNet Деловая почта, включая архивные сообщения. После того как будет принято обновление с новыми мастер-ключами, сообщения, зашифрованные на старых ключах, невозможно будет прочитать.
- Перед сменой мастер-ключей рекомендуется выгрузить РНПК в файл: *УКЦ> Ключевой центр> Пользователи*, правой кнопкой мыши по пользователю, выбрать раздел *Ключи пользователя> Создать и сохранить РНПК в файл…*

Для смены мастер-ключей перейдите на рабочее место *Главного администратора* и выполните следующие действия:

1. В окне *ViPNet Удостоверяющий и ключевой центр* выберите представление *Ключевой центр* и выберите раздел *Моя сеть> Мастер-ключи*.
2. Поочередно в контекстном меню каждого из трех мастер-ключей выберите пункт *Сменить*.
3. В появившемся окне с сообщением о смене мастер-ключа установите флажок *Сменить <название мастер-ключа>* и нажмите кнопку *Продолжить* (рис. 100).
4. В окне *ViPNet Удостоверяющий и ключевой центр* перейдите в раздел *Пользователи*, выделите всех пользователей, в контекстном меню выберите пункт *Ключи пользователя> Создать и передать ключи в ЦУС*.

5. В разделе *Сетевые узлы* окна *ViPNet Удостоверяющий и ключевой центр* выберите все узлы, в контекстном меню выберите пункт *Создать и передать ключи в ЦУС*.

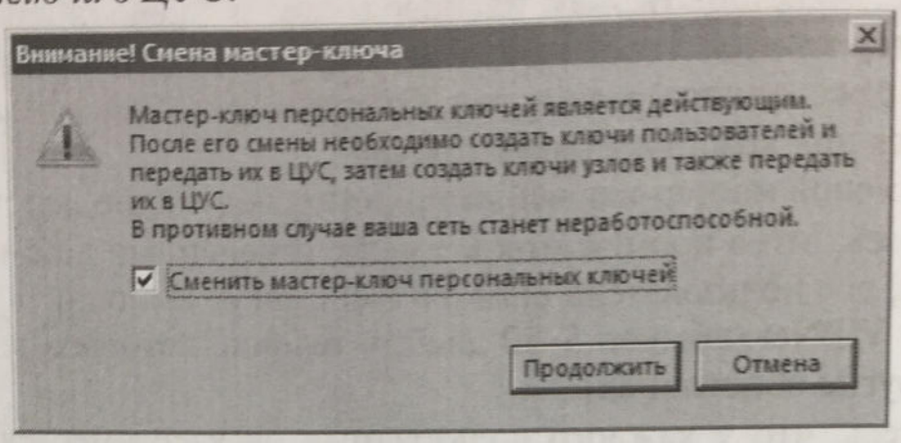

Рис. 100. Смена мастер-ключа

6. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Отправить справочники и ключи…*

7. В открывшемся окне установите флажок *Отложить применение обновления до,* установите дату и время таким образом, чтобы обновление было применено через 5 минут от текущей даты и времени ***(обратите внимание на дату, по умолчанию при активации отложенного применения обновления дата сдвинута на 1 день вперед)*** и нажмите кнопку *Отправить на весь список* (в реальной сети при смене мастер-ключей необходимо применять обновления через 5–10 дней после их отправки, стоит учитывать тот факт, что сетевые узлы могут быть выключены, и если они будут неактивны большее время, то может возникнуть ситуация при которой обновления вообще не дойдут до сетевого узла. Это связано с тем, что на координаторе, за которым находятся такие узлы, установит обновления, ключи изменятся и те сетевые узлы станут не доступны. Поэтому рекомендуется распланировать рассылку обновлений при смене мастер-ключей (рис. 101).

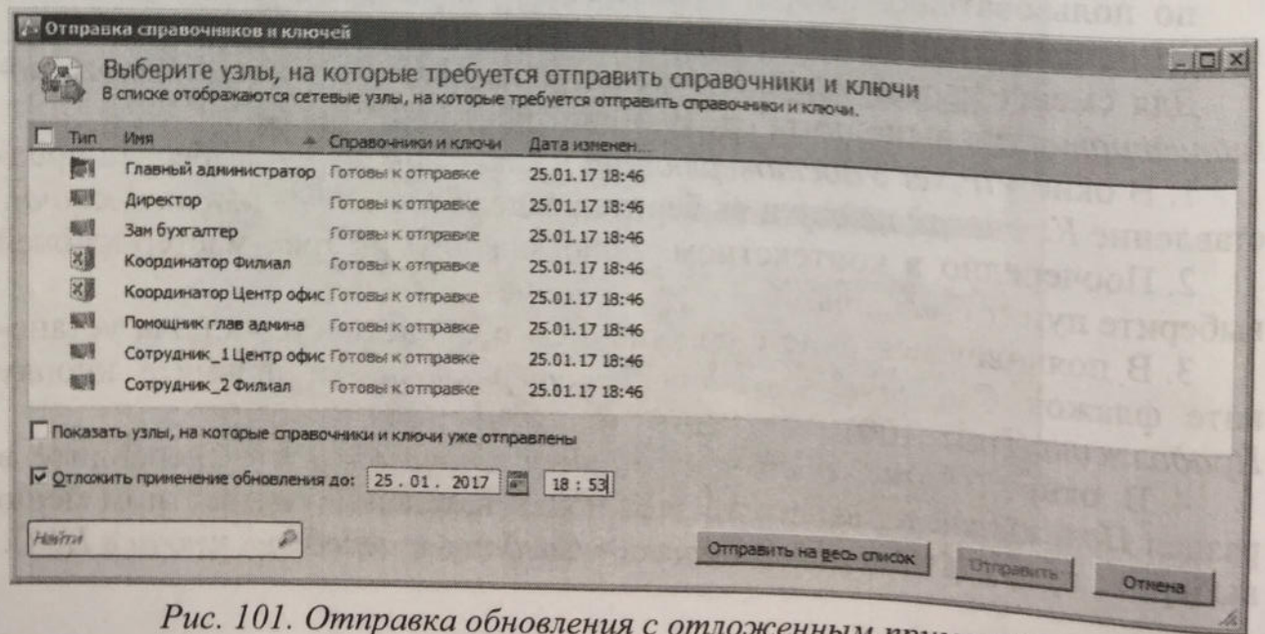

Рис. 101. Отправка обновления с отложенным применением

8. Проконтролируйте доставку обновлений на узлы *Главный администратор*, *Помощник глав админа*.

В зависимости от настроек конкретных узлов обновления вступят в силу после перезапуска программы ViPNet Client Монитор, которое произойдет автоматически или может потребоваться перезапустить *ViPNet Client Монитор* вручную (должно всплыть окно с уведомление о необходимости перезапуска). Во втором случае необходимо будет выполнить следующие действия:

1. На рабочем месте *Главного администратора* в области уведомлений на панели задач Windows щелкните значок программы ViPNet Client Монитор и в открывшемся окне нажмите *Файл> Выход*.

2. Теперь откройте программу ViPNet Client Монитор – меню *Пуск > Все программы > ViPNet > ViPNet Client > Монитор*.

Аналогично перезапустить ViPNet Client Монитор на рабочем месте *Помощник глав админа*.

После перезагрузки на экран будет выведено сообщение о необходимости указать путь до места расположения резервного набора персональных ключей. Указываете путь до файла резервного набора персональных ключей и вводите пароль пользователя.

В случае корректного обновления загрузиться ViPNet Client Монитор.

2.1.11. Формирование нового сертификата ключа проверки электронной подписи

Если пользователь на сетевом узле по каким-то причинам не смог сделать запрос на сертификат ключа проверки электронной подписи самостоятельно (например, срок действия сертификата закончился), то сформировать новый сертификат и ключ электронной подписи возможно в программе ViPNet Удостоверяющий и ключевой центр в процессе создания ключей пользователя.

Для того чтобы сформировать новый сертификат для пользователя *Помощник глав админа Иванов* выполните следующие действия:

1. В окне *ViPNet Удостоверяющий и ключевой центр* перейдите в раздел *Пользователи*, выделите пользователя *Помощник глав админа Иванов* и в контекстном меню выберите пункт *Ключи пользователя*,

2. Установите флажок *Создавать ключи электронной подписи* и нажмите *Создать и передать ключи в ЦУС* (рис. 102).

3. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Отправить справочники и ключи…*

4. В открывшемся нажмите кнопку *Отправить на весь список*.

5. Проконтролируйте применение обновлений на узле *Помощник глав админа*.

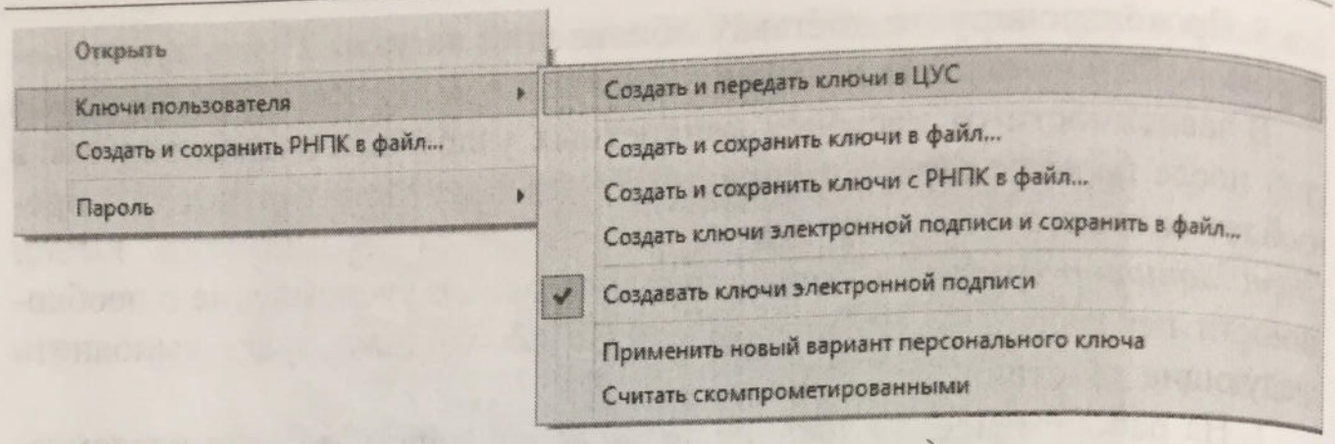

Рис. 102. Контекстное меню в разделе

6. На рабочем месте *Помощник глав админа* в области уведомлений на панели задач Windows щелкните по значку программы ViPNet Client Монитор и в открывшемся окне в меню *Сервис* выберите пункт *Настройка параметров безопасности*.

7. В окне *Настройка параметров безопасности* перейдите на вкладку *Электронная подпись*, нажмите кнопку *Выбрать* и выберите новый сертификат пользователя *Помощник глав админа Иванов* (рис. 103).

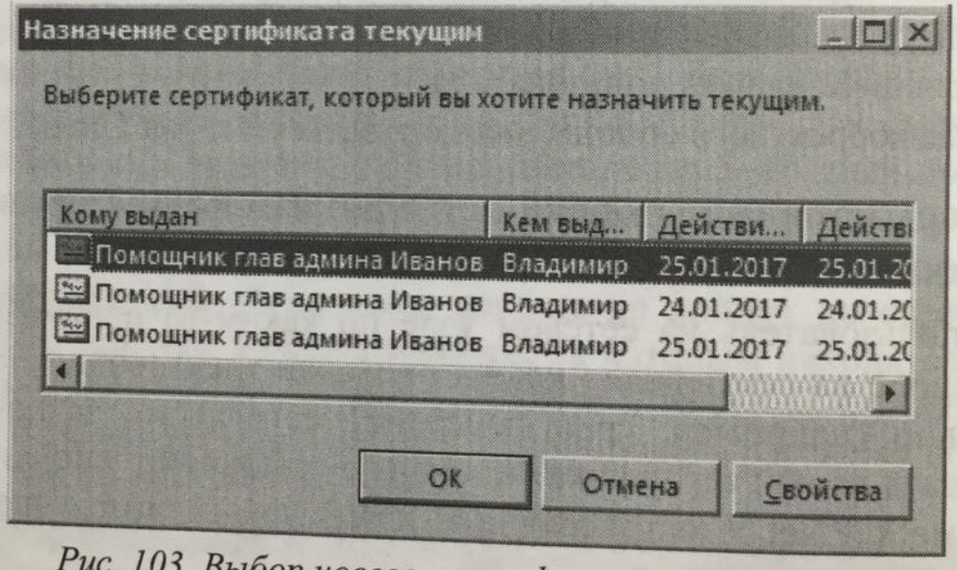

Рис. 103. Выбор нового сертификата пользователя Помощник глав админа Иванов

2.1.12. Обновление программного обеспечения на узлах

Чтобы обновить программное обеспечение ViPNet Client на узле *Помощник глав админа* выполните следующие действия:

1. В окне *ViPNet Центр управления сетью* в меню *Моя сеть* выберите пункт *Обновить программное обеспечение на узлах*.
2. В появившемся окне нажмите кнопку *Далее*.
3. Нажмите кнопку *Загрузить файл обновления*> *Обзор* и выберите файл с обновлением **.lzh*. (файл с обновлением в рамках данного практического занятия находится в папке с дистрибутивом ViPNet Client > *RUS* > *Software* > *SP*).
4. Нажмите кнопку *ОК* (рис. 104).

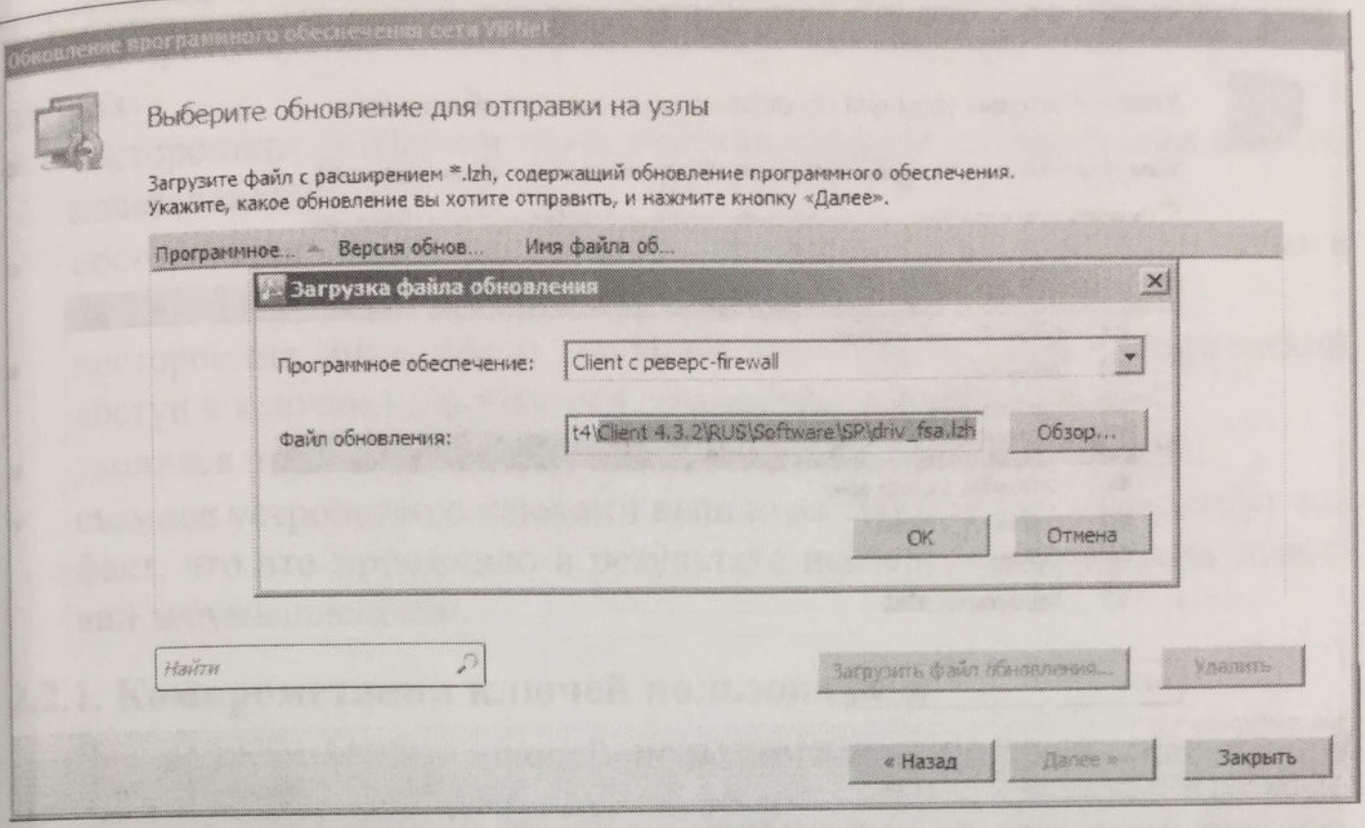

Рис. 104. Загрузка файла обновления программного обеспечения

После загрузки обновления в *ViPNet Центр управления сетью* оно отобразится в списке.

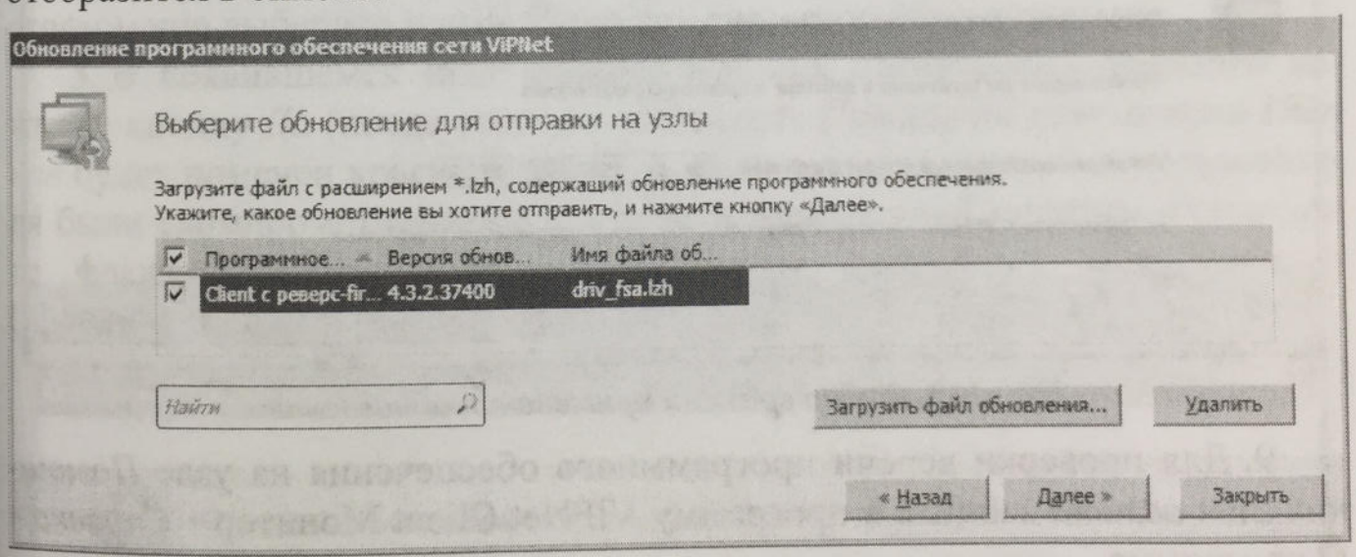

Рис. 105. Список обновлений программного обеспечения

5. Выберите обновление из списка и нажмите *Далее (рис. 105)*.

6. На следующем шаге укажите сетевой узел *Помощник глав админа* (рис. 106).

7. Теперь задайте время применения обновления – текущее время и установите флажок *Перезагружать Windows на сетевых узлах после обновления программного обеспечения* (рис. 107).

8. Следуйте указаниям мастера, нажимая кнопку *Далее*. На заключительном шаге дождитесь окончания отправки обновления и перезагрузки операционной системы.

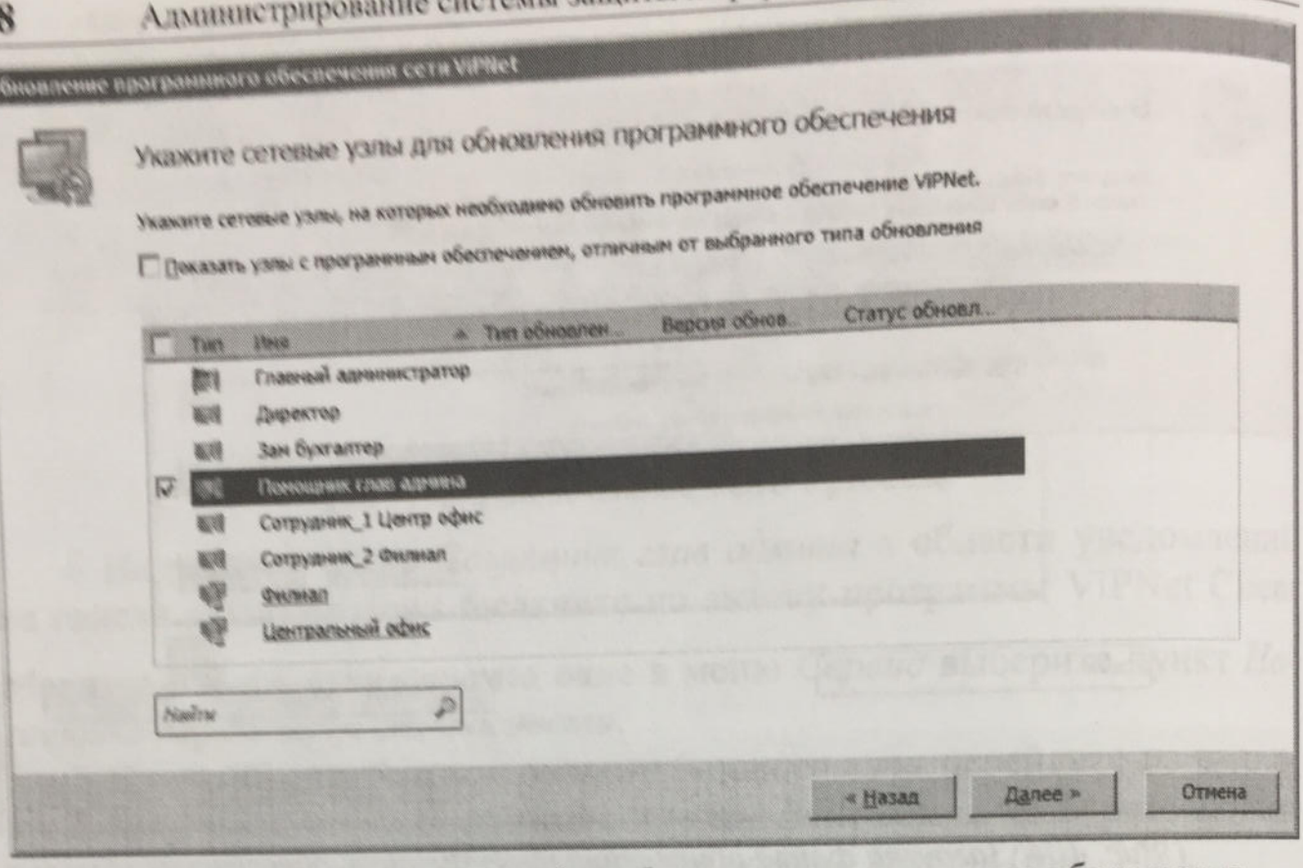

Рис. 106. Выбор сетевых узлов для обновления программного обеспечения

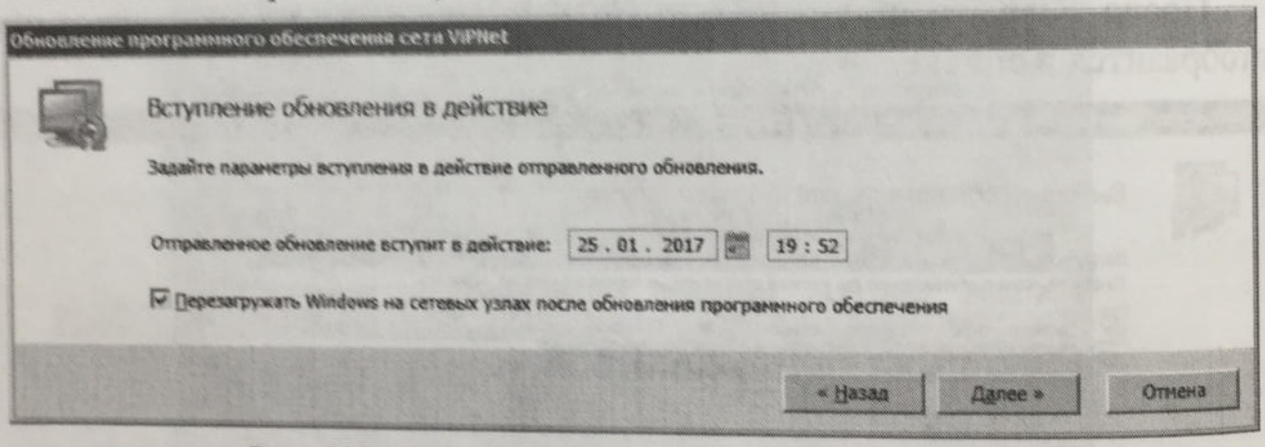

Рис. 107. Выбор времени применения обновления

9. Для проверки версии программного обеспечения на узле *Помощник глав админа* зайдите в программу ViPNet Client Монитор> *Справка*> *О программе*.

В рамках данного практического занятия явных изменений в версии не будет, так как был использован файл обновления той же версии ViPNet Client, но этого достаточно чтобы изучить процедуру обновления ПО.

Задание 2.2. Компрометация

Формулировка задания. В настоящем задании необходимо скомпрометировать ключи пользователя *Помощник глав админа Иванов*.

О КОМПРОМЕТАЦИИ

Компрометация может происходить с удалением или без удаления сетевого узла, пользователя.

Как правило, ключи считаются скомпрометированными в следующих случаях:

- посторонним лицам мог стать доступным файл дистрибутива ключей пользователя;
- посторонним лицам могло стать доступным съемное устройство с ключами пользователя;
- посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере;
- уволился пользователь, имевший доступ к паролям и ключам;
- съемное устройство с ключами вышло из строя, и не опровергнут тот факт, что это произошло в результате несанкционированных действий злоумышленника.

2.2.1. Компрометация ключей пользователя

Для компрометации ключей пользователя *Помощник глав админа Иванов* выполните следующие действия:

1. В окне ViPNet Удостоверяющий и ключевой центр перейдите в раздел *Пользователи*,

2. Выделите пользователя *Помощник глав админа Иванов* и в контекстном меню выберите пункт *Считать скомпрометированными.*

3. В появившемся окне *Компрометация ключей пользователей* нажмите кнопку *Да* (после этого пользователь *Помощник глав админа Иванов* будет помечен красным цветом). Если вместе с ключами пользователя были скомпрометированы его ключи электронной подписи, установите флажок *Аннулировать сертификаты выбранных пользователей* (рис. 108).

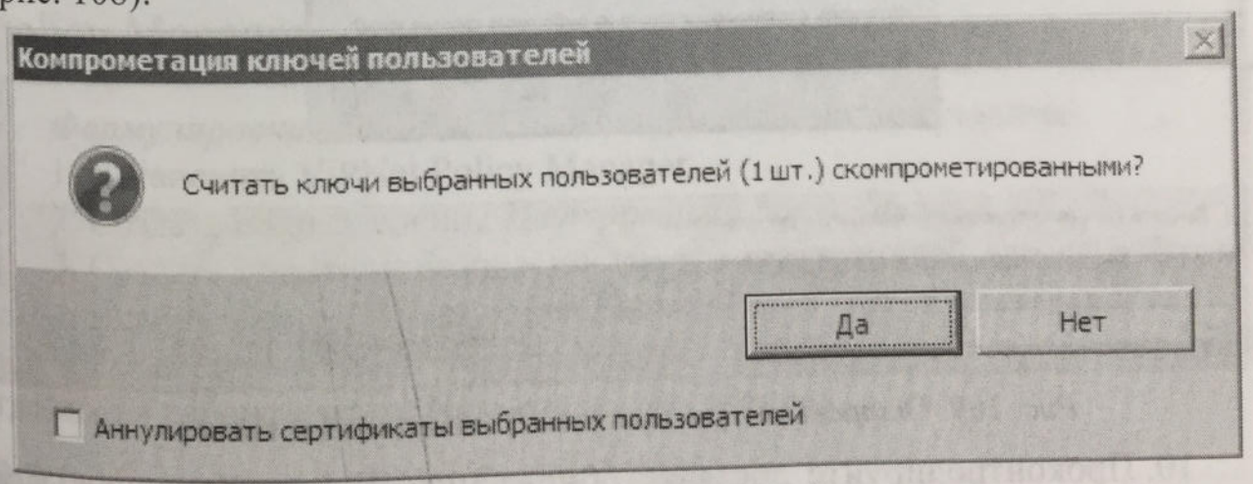

Рис. 108. Окно Компрометация ключей пользователя

4. Повторно вызовите нажатием правой кнопки мыши на пользователя *Помощник глав админа Иванов* контекстное меню и выберите пункт *Ключи пользователя> Создать и передать ключи в ЦУС.*

5. В окне ViPNet Удостоверяющий и ключевой центр перейдите в раздел Сетевые узлы.

6. После этого создайте и передайте в ЦУС ключи для узла *Помощник глав админа.*

7. Затем выделите правой кнопкой мыши (или сочетанием клавиш Ctrl+W) остальные узлы, для которых нужно создать ключи и в контекстном меню выберите пункт *Создать и передать ключи в ЦУС* (или сочетанием клавиш Ctrl+F).

Примечание. Если у скомпрометированного пользователя есть в наличии ключи электронной подписи и сертификат, которые хранятся на его узле, то создайте для него новые ключи и сертификат. Это связано с тем, что на узле ключи электронной подписи защищены персональным ключом пользователя. Поэтому после смены персонального ключа пользователь не сможет получить доступ к своим текущим ключам электронной подписи и сертификату.

8. В окне *ViPNet Центр управления сетью* нажмите кнопку *Справочники и ключи> Отправить справочники и ключи…*

9. В открывшемся окне выберите узел *Помощник глав админа* и нажмите кнопку *Отправить* (рис. 109).

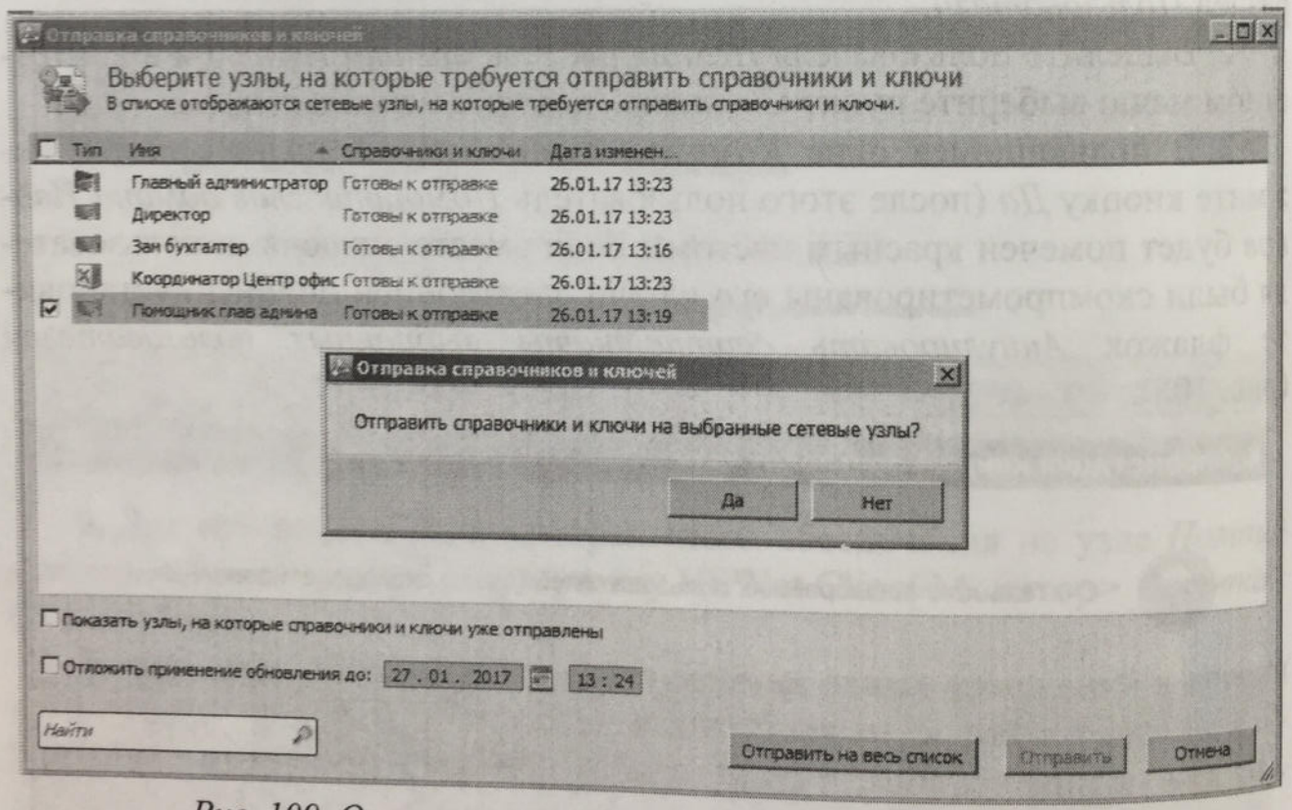

Рис. 109. Отправка ключей на узел Помощник глав админа

10. Проконтролируйте доставку обновления на узел *Помощник глав админа.*

11. Проконтролируйте применение обновления на скомпрометированном узле *Помощник глав админа.*

12. После перезапуска ПО ViPNet Client, появиться диалоговое окно, в котором необходимо будет указать путь до РНПК и ввести пароль пользователя.

13. После успешного обновления на узле *Помощник глав админа*, появиться диалоговое окно с информацией о том, что текущий пароль истек и его следует сменить. Для смены пароля необходимо выбрать пункт *Открыть настройки пароля и установить новый пароль* – 11111111 (рис. 110).

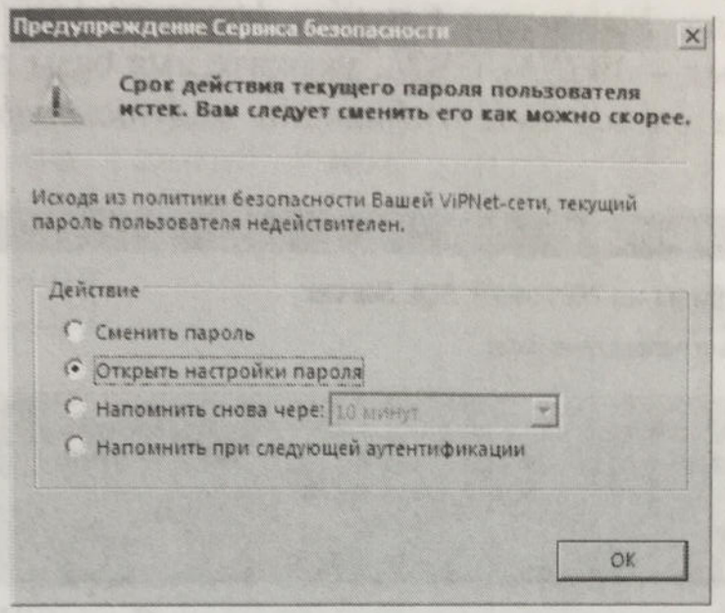

Рис. 110. Смена пароля на узле Помощник глав админа

14. Отправьте обновления на остальные узлы.

В результате правильного выполнения задания на сетевом узле *Помощник глав админа* должен быть доступен *Главный администратор* (в программе ViPNet Client Монитор в разделе *Защищенная сеть* выберите *Главный администратор* и нажмите клавишу F5).

Задание 2.3. Настройка политик безопасности в ViPNet Policy Manager

Формулировка задания. В настоящем задании необходимо:

1. Установить ViPNet Policy Manager
2. Создать подразделения *Центральный офис, Филиал*.
3. Создать политики безопасности, ограничивающей доступ работников компании к социальным сетям *Вконтакте* и *Одноклассники*.
4. Создать политики безопасности, блокирующей весь открытый трафик на рабочем месте *Помощник глав админа*.

2.3.1. Установка ViPNet Policy Manager

ПО ViPNet Policy Manager допускается развертывать только на клиенте с ролью *Network Control Center*, поэтому клиенту *Главный администратор* была автоматически назначена роль *Policy Manager*.

1. На рабочем месте *Главный администратор* запустите установочный файл программного обеспечения ViPNet Policy Manager *<имя_файла>.exe*.

2. Следуйте указаниям мастера установки, для этого нажимайте кнопку *Далее*, не меняя параметры по умолчанию.

3. На одном из шагов мастера установки ознакомьтесь с условиями лицензионного соглашения, установите соответствующий флажок и нажмите кнопку *Продолжить*.

4. На странице *Установка базы на Microsoft SQL Server* выберите сервер баз данных – *.\WINNCCSQL*, укажите имя базы данных – *ViPNet-PolicyManager* и способ аутентификации – *Аутентификация Windows* (рис. 111).

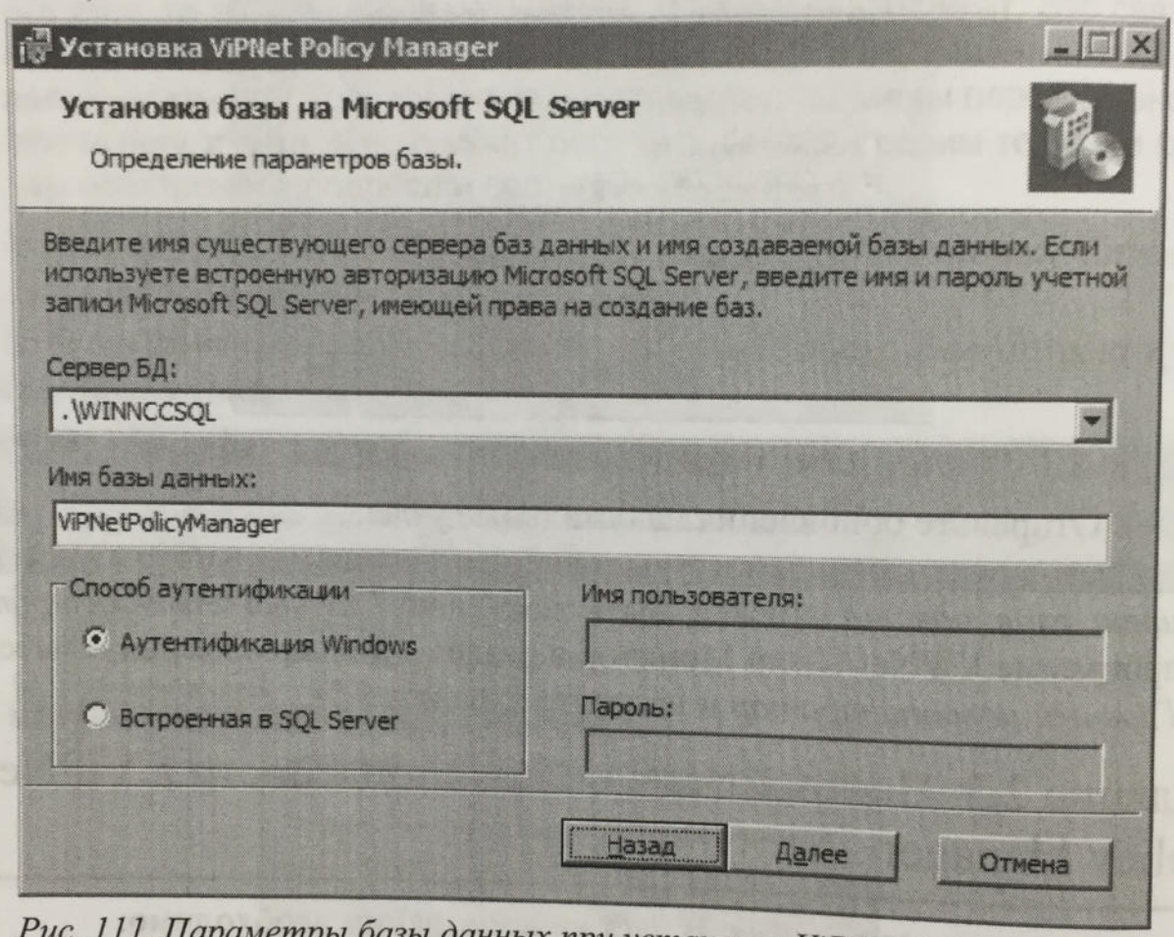

Рис. 111. Параметры базы данных при установке ViPNet Policy Manager

5. В процессе установки может появиться окно со списком приложений, которые требуется закрыть. Выберите *Закрыть приложения и попытаться перезапустить их* и нажмите кнопку *ОК*.

Для обеспечения нормальной работы продукта ViPNet Policy Manager выполните следующие действия:

1. В окне *ViPNet Центр управления сетью* перейдите в раздел *Клиенты*.

2. В свойствах клиента *Главный администратор* выберите *Роли узла > Policy Manager > Свойства* и добавьте в список все узлы сети (рис. 112).

3. Создайте и отправьте справочники на все узлы сети. Дождитесь пока обновятся справочники на узле *Помощник глав админа*.

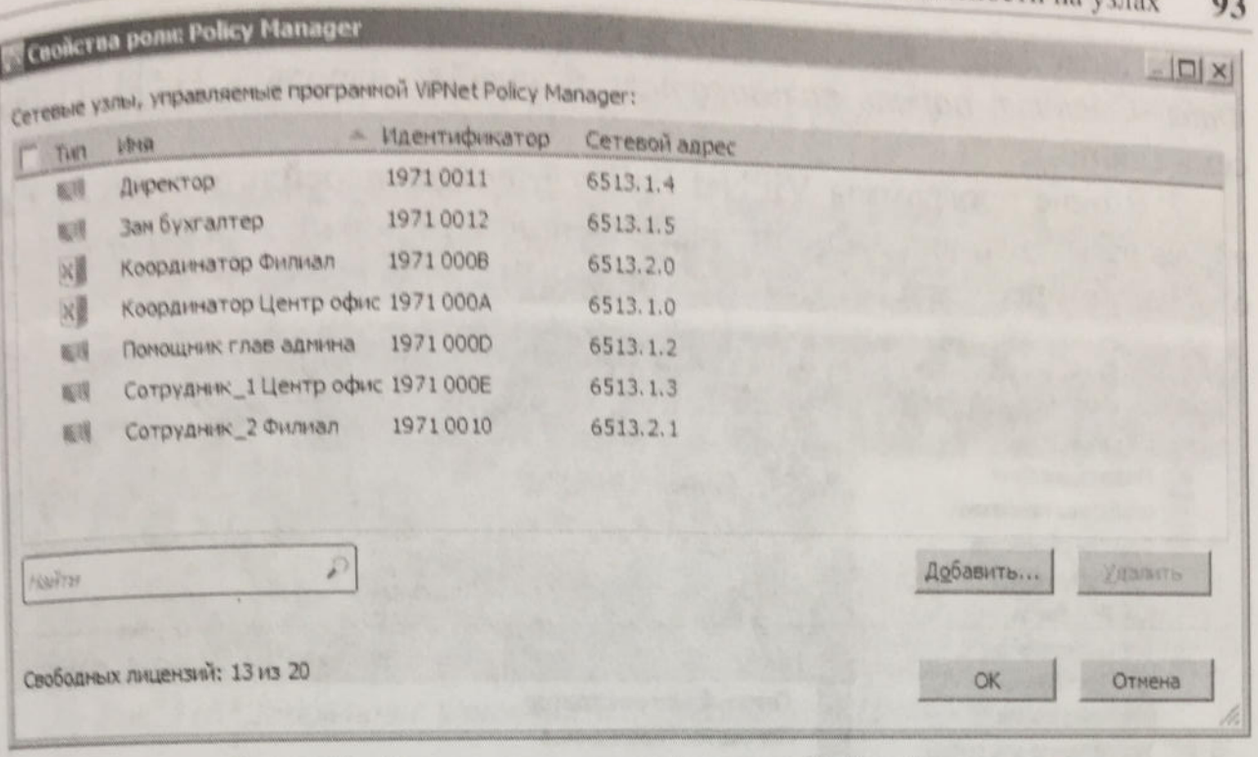

Рис. 112. Добавление узлов для роли Policy Manager

4. Откройте программу ViPNet Policy Manager (*Пуск* > *Все программы* > *ViPNet* > *ViPNet Policy Manager*) и введите имя пользователя и пароль – *Supervisor* (рис. 113).

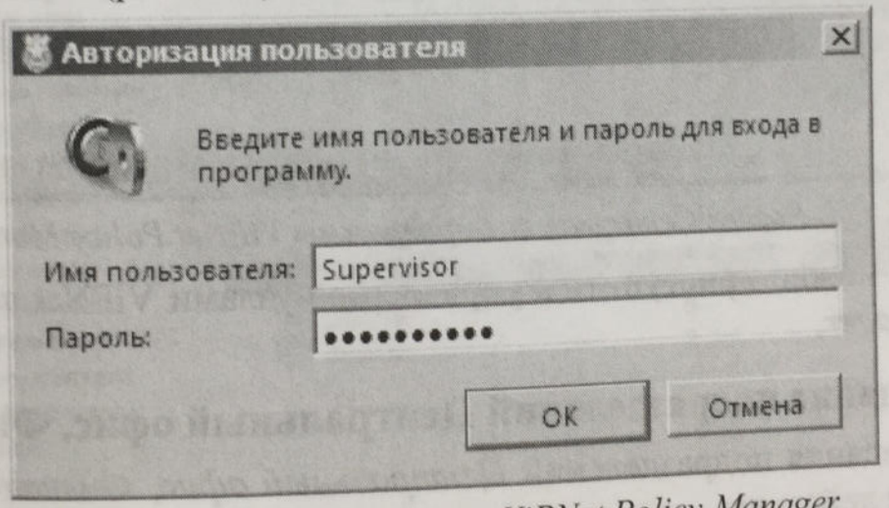

Рис. 113. Вход в программу ViPNet Policy Manager

5. На экран будет выведено предупреждение о необходимости смены пароля пользователя *Supervisor* (рис. 114).

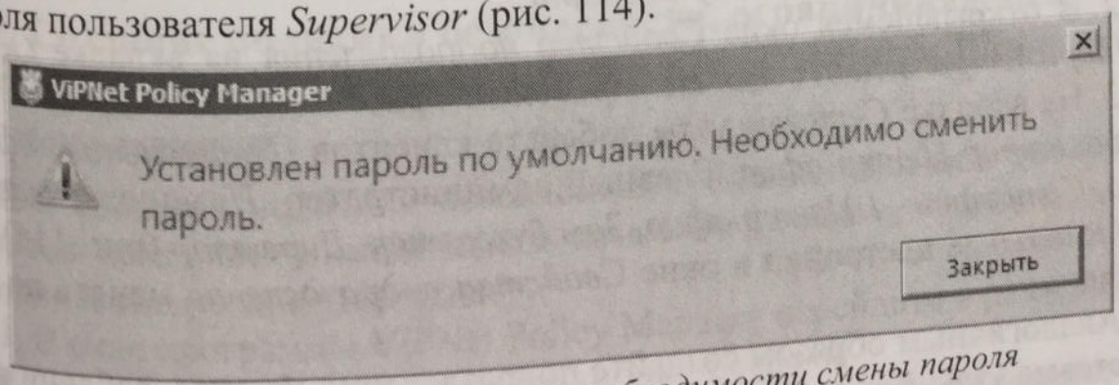

Рис. 114. Предупреждение о необходимости смены пароля

6. После авторизации под стандартным паролем перейдите в раздел *Файл>Сменить пароль пользователя* и задайте пароль – 11111111 (восемь единиц).

7. В окне программы ViPNet Policy Manager перейдите в раздел *Сетевые узлы*. Если предыдущие шаги выполнены верно, то в списке будут отображены все узлы сети ViPNet (рис. 115).

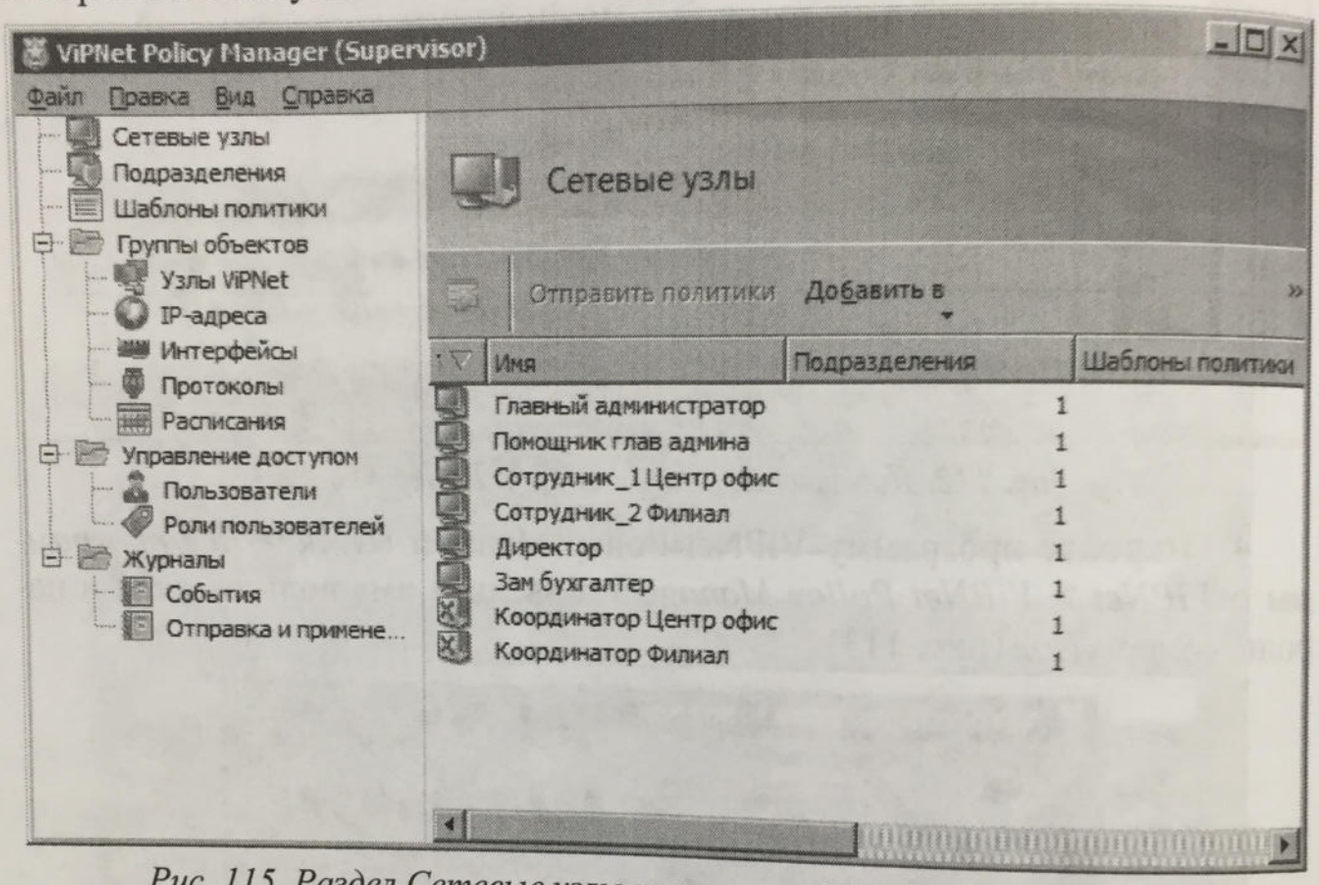

Рис. 115. Раздел Сетевые узлы программы ViPNet Policy Manager

Теперь можно приступить к управлению узлами ViPNet через *ViPNet Policy Manager*.

2.3.2. Создание подразделений Центральный офис, Филиал

Для создания подразделений *Центральный офис, Филиал* выполните следующие действия:

1. В окне программы ViPNet Policy Manager перейдите в раздел *Подразделения* и нажмите кнопку *Создать*.

2. В открывшемся окне *Свойства подразделения* на вкладке *Основные параметры* задайте имя *Центральный офис*.

3. На вкладке *Сетевые узлы* добавьте клиентов *Центрального офиса*: *Координатор Центр офис*, Главный администратор, *Помощник глав администратора*, *Сотрудник_1 Центр офис*, *Зам бухгалтер*, *Директор* (рис. 116).

Остальные настройки в окне *Свойства подразделения* менять не требуется.

Аналогичным образом создайте подразделения *Филиал*, добавив в него сетевые узлы *Координатор Филиал*, *Сотрудник_2 Филиал*.

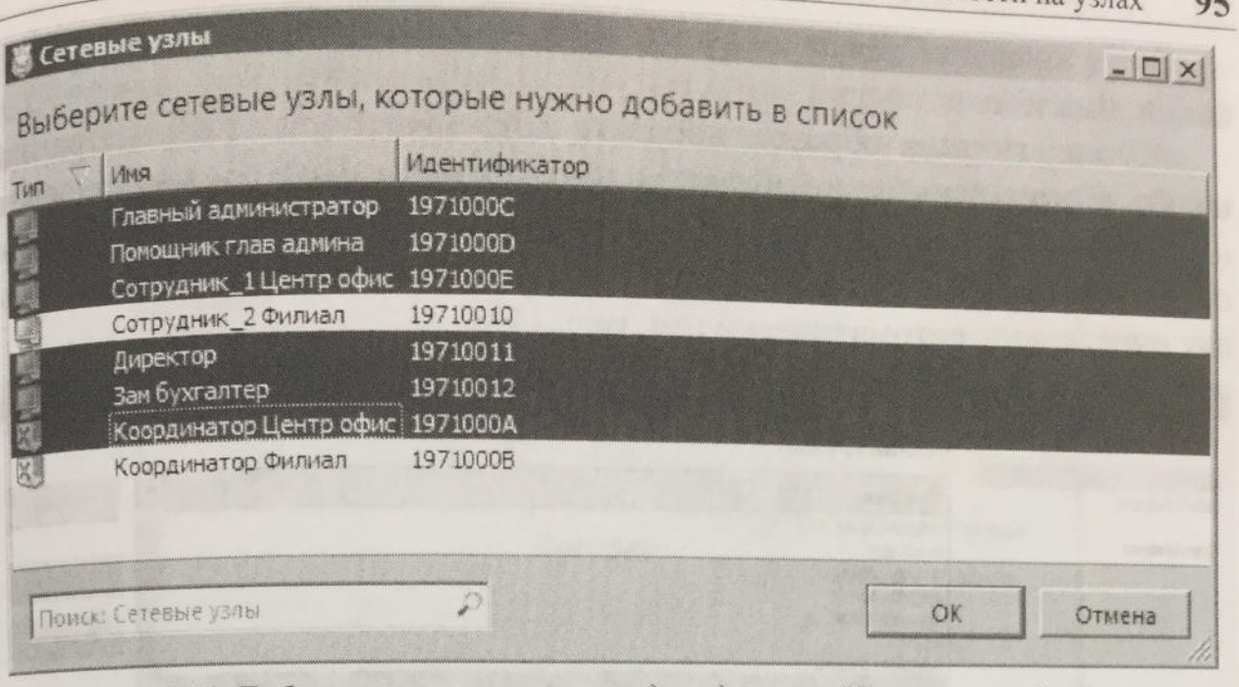

Рис. 116. Добавление клиентов в подразделение Центральный офис

Если все выполнено правильно, раздел *Подразделения* программы ViPNet Policy Manager примет вид, показанный на рис. 117.

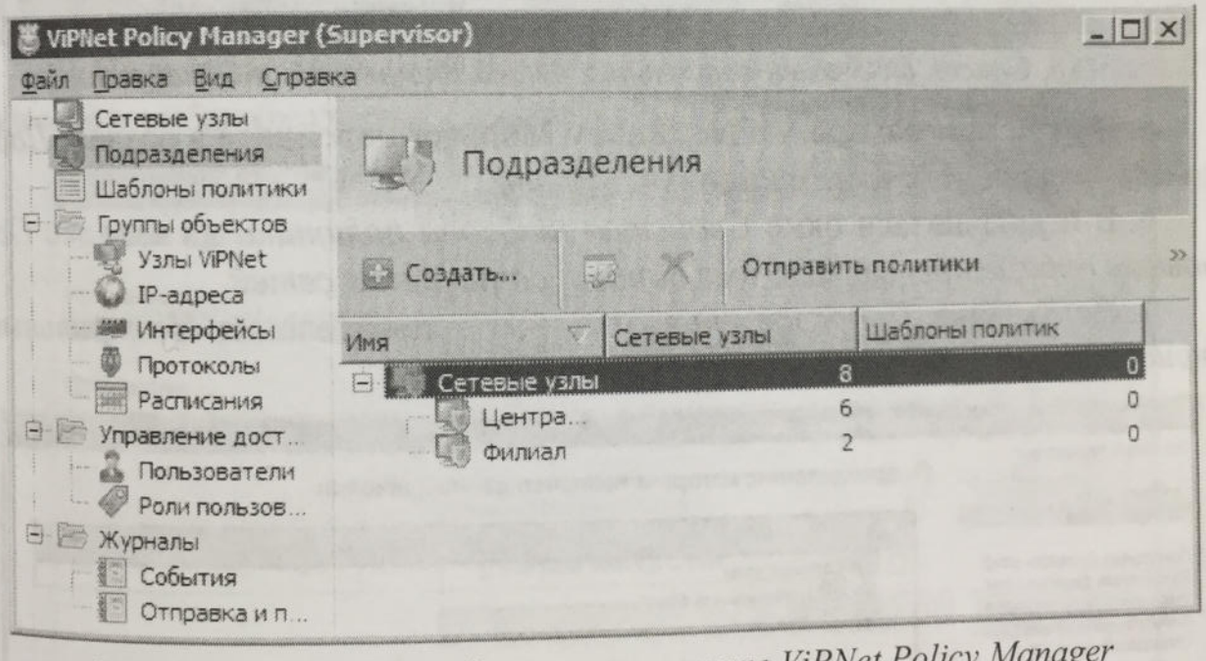

Рис. 117. Раздел Подразделения программы ViPNet Policy Manager

2.3.3. Создание политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники

Для создания политики безопасности, ограничивающей доступ работников компании к социальным сетям Вконтакте и Одноклассники, выполните следующие действия:

1. В окне программы ViPNet Policy Manager перейдите в раздел *Группы объектов* > *IP-адреса* и нажмите кнопку *Создать*.

2. В открывшемся окне *Свойства группы IP-адресов* на вкладке *Основные параметры* задайте имя *Социальные сети*.

3. На вкладке *Состав* нажмите кнопку *Добавить* > *DNS-имя...* и добавьте имя *vk.com*.

4. Аналогичным образом добавьте *DNS-имена* (рис. 118). (В рамках практического занятия не обязательно вбивать все *DNS-имена*, приведенные в качестве примера, чтобы было понятно, как действовать в реальной ситуации закрытия доступа к ресурсам). Соответствующие IP-адреса будут определены автоматически (см. рис. 118).

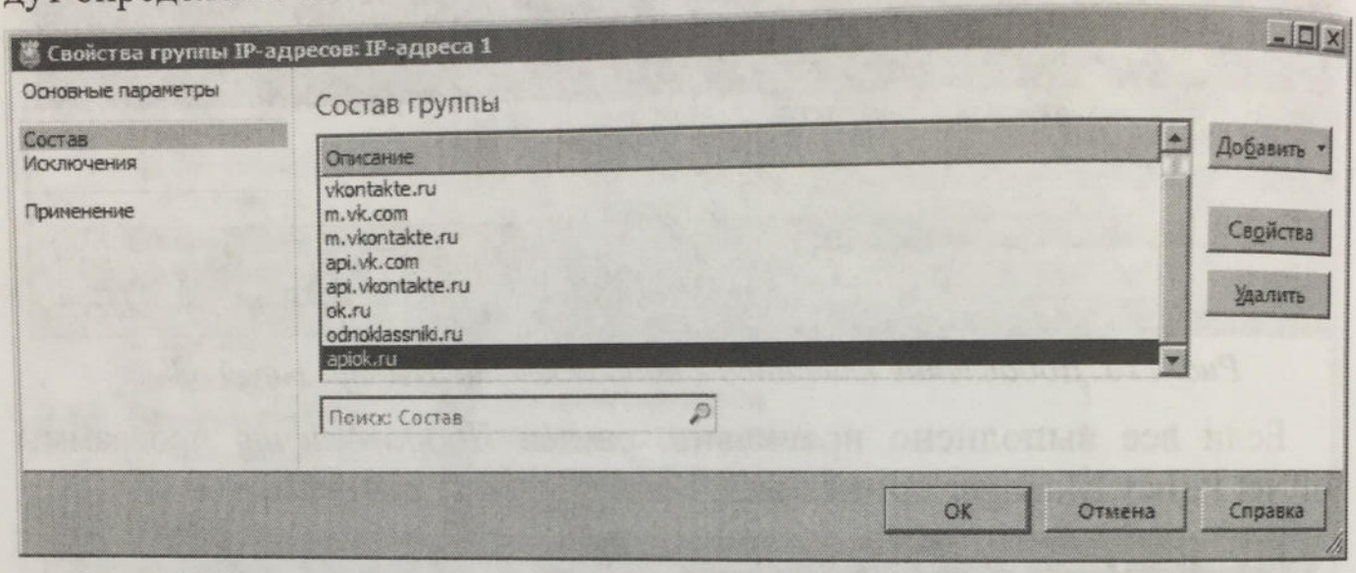

Рис. 118. Список DNS-имен социальных сетей Вконтакте и Одноклассники

5. В окне программы ViPNet Policy Manager перейдите в раздел *Шаблоны политики* и нажмите кнопку *Создать*.

6. В открывшемся окне *Свойства шаблона политики* на вкладке *Основные параметры* задайте имя *Запрет социальных сетей*.

7. На вкладке *Подразделения* отметьте подразделения *Центральный офис* и *Филиал* (рис. 119).

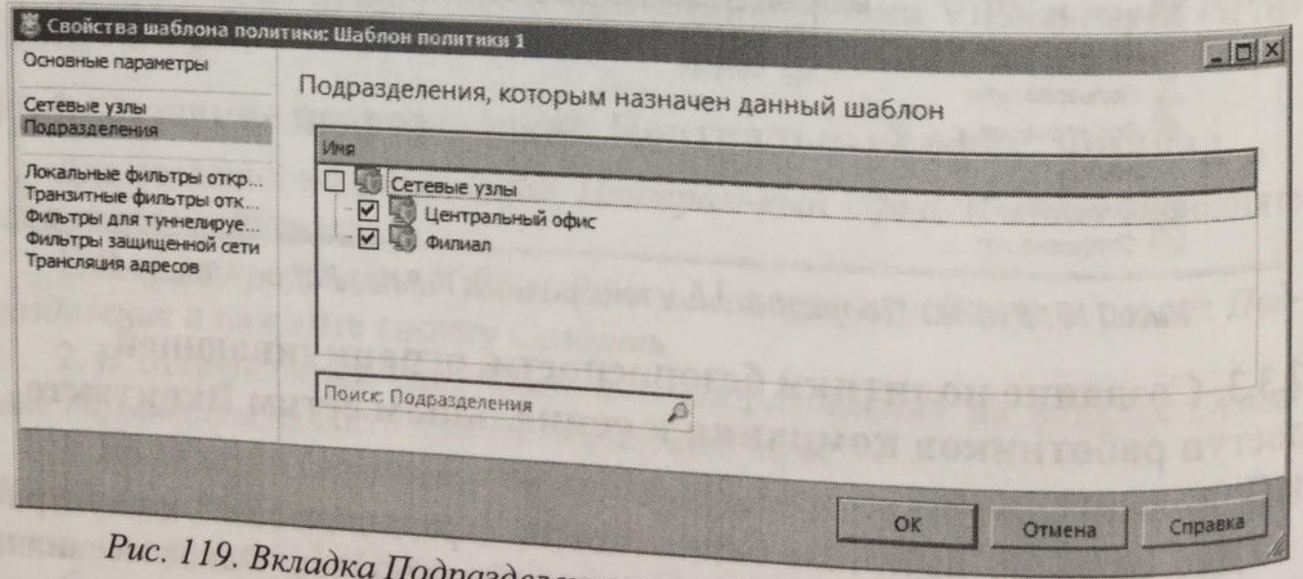

Рис. 119. Вкладка Подразделения окна Свойства шаблона политики

8. На вкладке *Локальные фильтры открытой* сети нажмите кнопку *Создать...*

9. В открывшемся окне *Свойства фильтра открытой сети* на вкладке *Основные параметры* задайте имя фильтра *Запрет социальных сетей* и установите переключатель в положение *Блокировать трафик* (рис. 120).

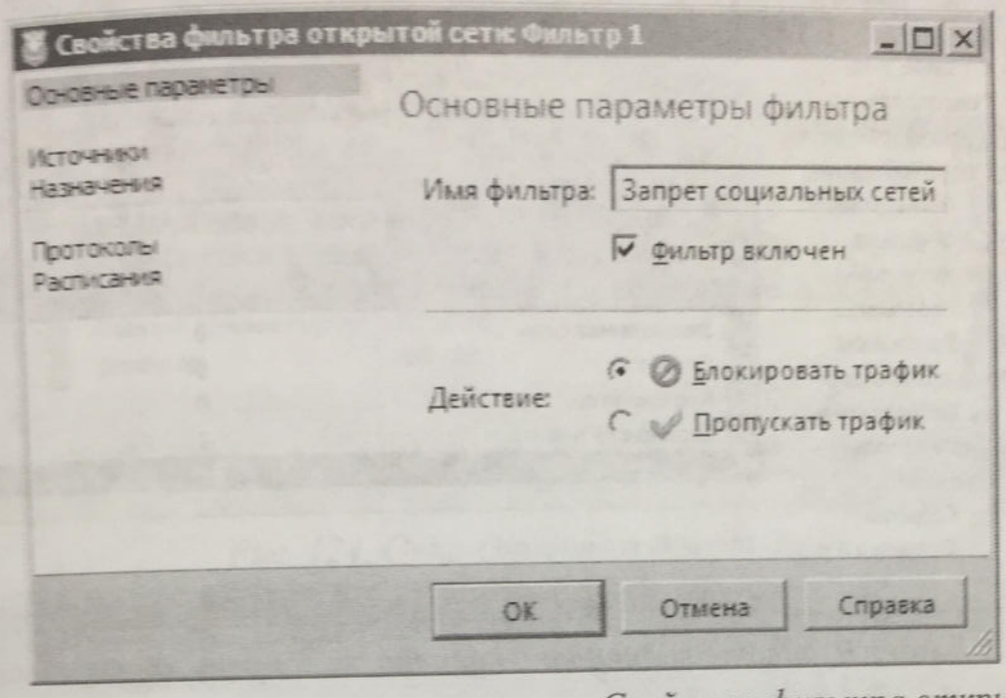

Рис. 120. Вкладка Основные параметры окна Свойства фильтра открытой сети

10. На вкладке *Назначения* нажмите кнопку *Добавить... > Группы IP-адресов* и выберите группу *Социальные сети* (рис. 121).

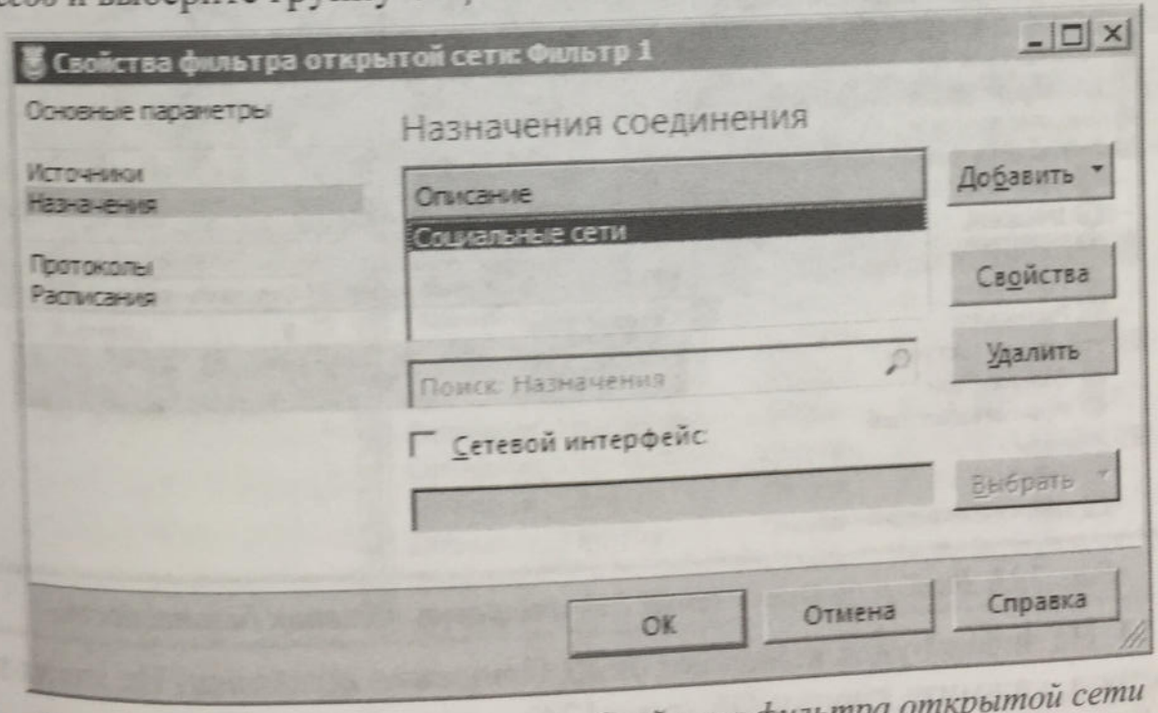

Рис. 121. Вкладка Назначения окна Свойства фильтра открытой сети

11. Остальные параметры окна *Свойства фильтра открытой сети* и *Свойства шаблона политики* менять не требуется.

После создания политики *Запрет социальных сетей* раздел *Шаблоны политики* примет вид, показанный на рис. 122.

12. Отправьте политики на узлы. Для этого в окне программы ViPNet Policy Manager перейдите в раздел *Подразделения*.

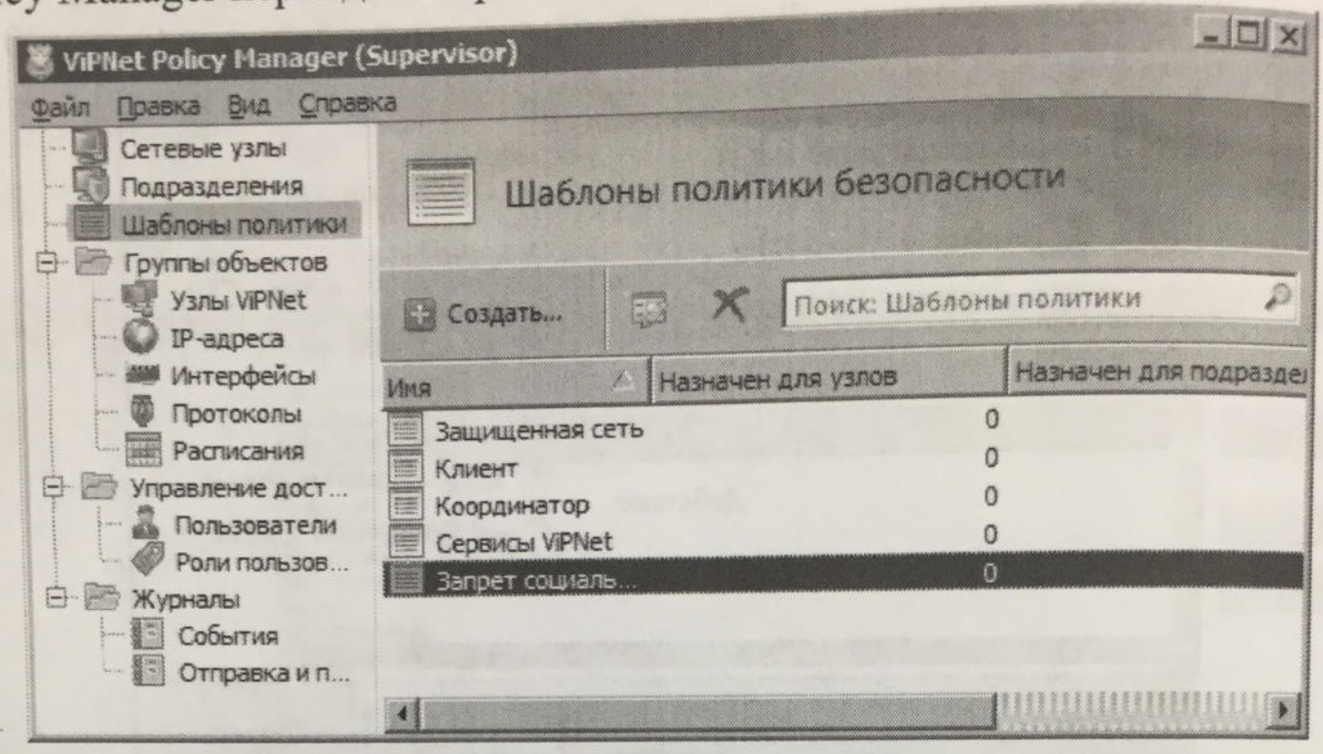

Рис. 122. Раздел Шаблоны политики с политикой Запрет социальных сетей

13. Выделите подразделения *Центральный офис и Филиал*, нажмите кнопку *Отправить политики* (рис. 123).

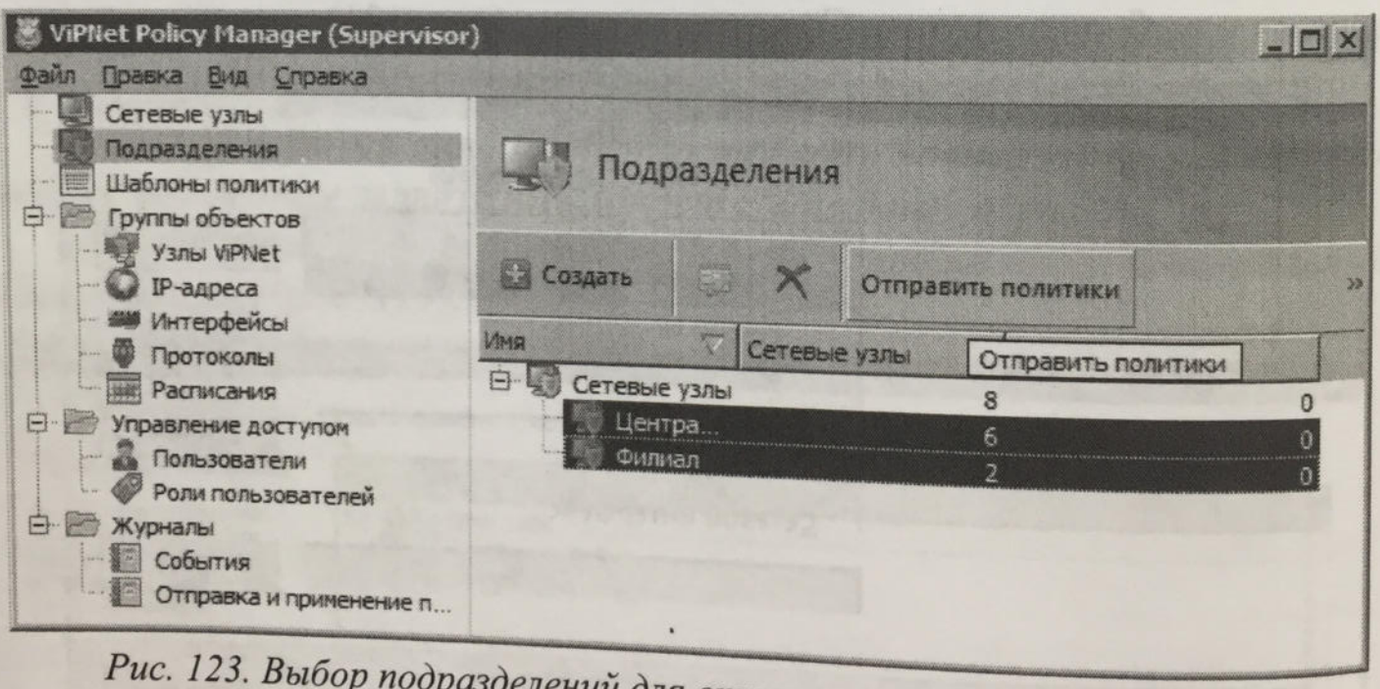

Рис. 123. Выбор подразделений для отправки политик безопасности

14. На экран будет выведено окно *Отправка политики*. Не меняя параметров, нажмите кнопку *ОК* (рис. 124).

Для контроля за ходом отправки политик на узлы в окне программы ViPNet Policy Manager перейдите в раздел *Журналы* > *Отправка и применение политик*. Статус политик на узлах *Главный администратор* и *Помощник глав админа* должен измениться на *Применена* (рис. 125).

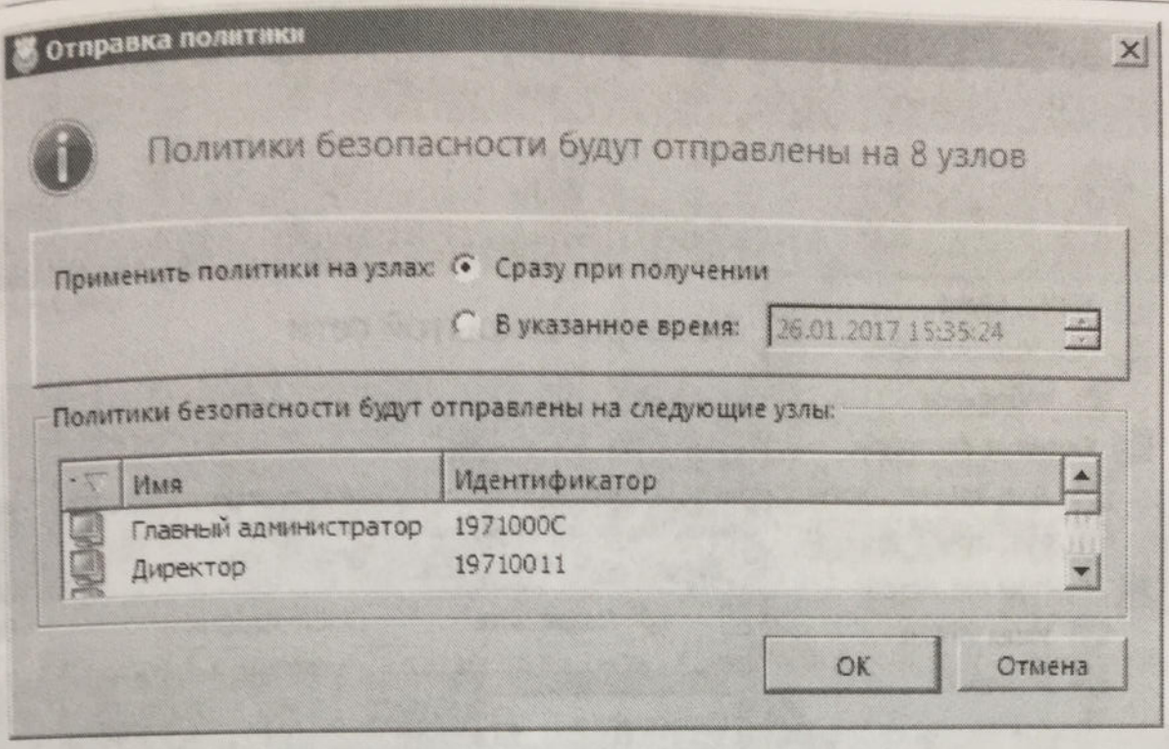

Рис. 124. Окно Отправка политики

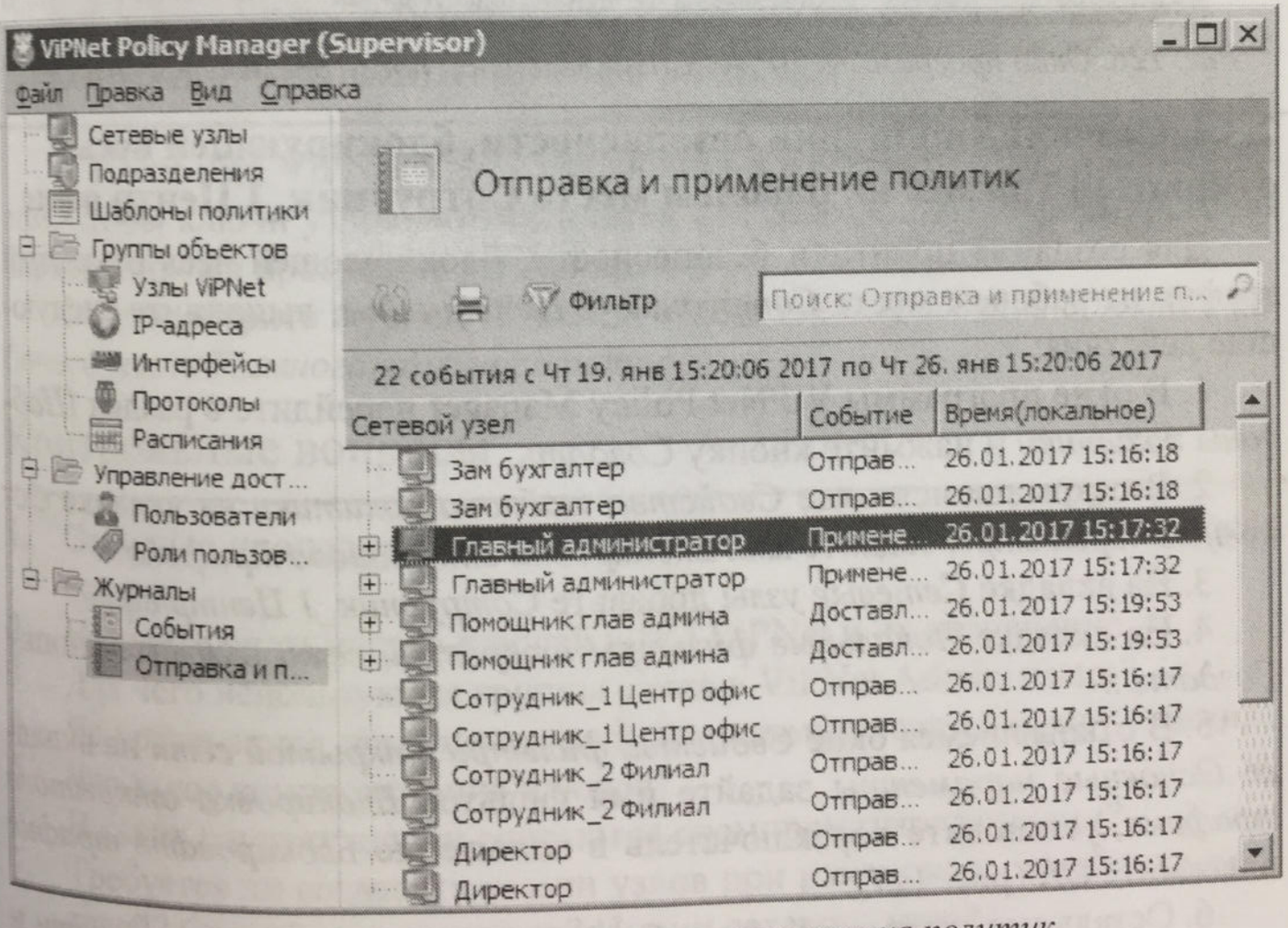

Рис. 125. Контроль отправки и применения политик

Для проверки применения политик на рабочих местах *Главный администратор* и *Помощник глав админа* зайдите в программу ViPNet Client Монитор > *Сетевые фильтры* > *Фильтры открытой сети*. Убедитесь, что добавлен новый фильтр *Запрет социальных сетей* (рис. 126).

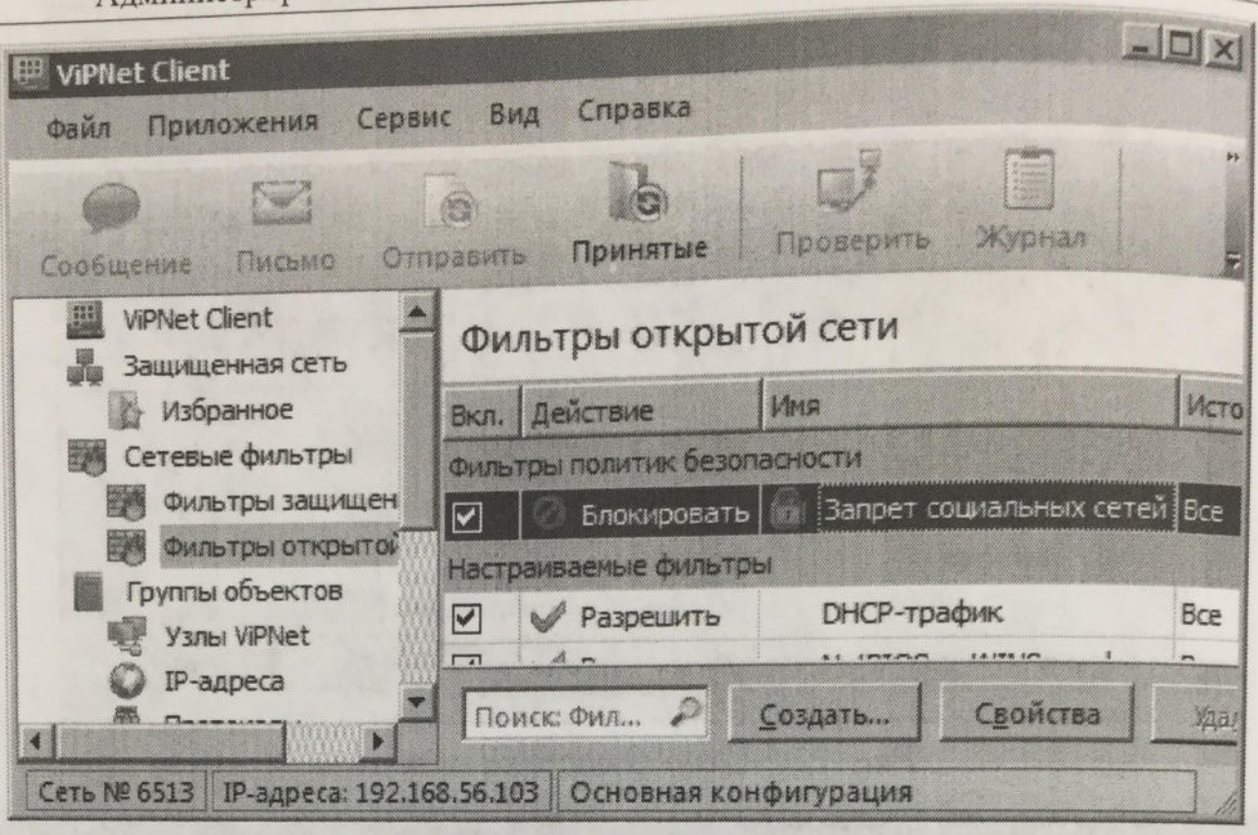

Рис. 126. Окно программы ViPNet Client Монитор после применения политик

2.3.4. Создание политики безопасности, блокирующей весь открытый трафик на рабочем месте Сотрудник_1 Центр офис

Для создания политики безопасности, блокирующей весь открытый трафик на рабочем месте *Сотрудник_1 Центр офис,* выполните следующие действия:

1. В окне программы ViPNet Policy Manager перейдите в раздел *Шаблоны политики* и нажмите кнопку *Создать*.

2. В открывшемся окне *Свойства шаблона политики* на вкладке *Основные параметры* задайте *имя Блокировка открытого трафика*.

3. На вкладке *Сетевые узлы* добавьте *Сотрудник_1 Центр офис*.

4. На вкладке *Локальные фильтры открытой сети* нажмите кнопку *Создать...*

5. В открывшемся окне *Свойства фильтра открытой сети* на вкладке *Основные параметры* задайте имя фильтра *Блокировка открытого трафика*, установите переключатель в положение *Блокировать трафик* и нажмите *ОК* (рис. 127).

6. Остальные параметры окна *Свойства фильтра открытой сети* и *Свойства шаблона политики* менять не требуется.

7. Отправьте теперь политики на узел *Сотрудник_1 Центр офис* (в окне программы ViPNet Policy Manager раздел *Сетевые узлы* выбрать узел *Сотрудник_1 Центр офис*> *Отправить политики*).

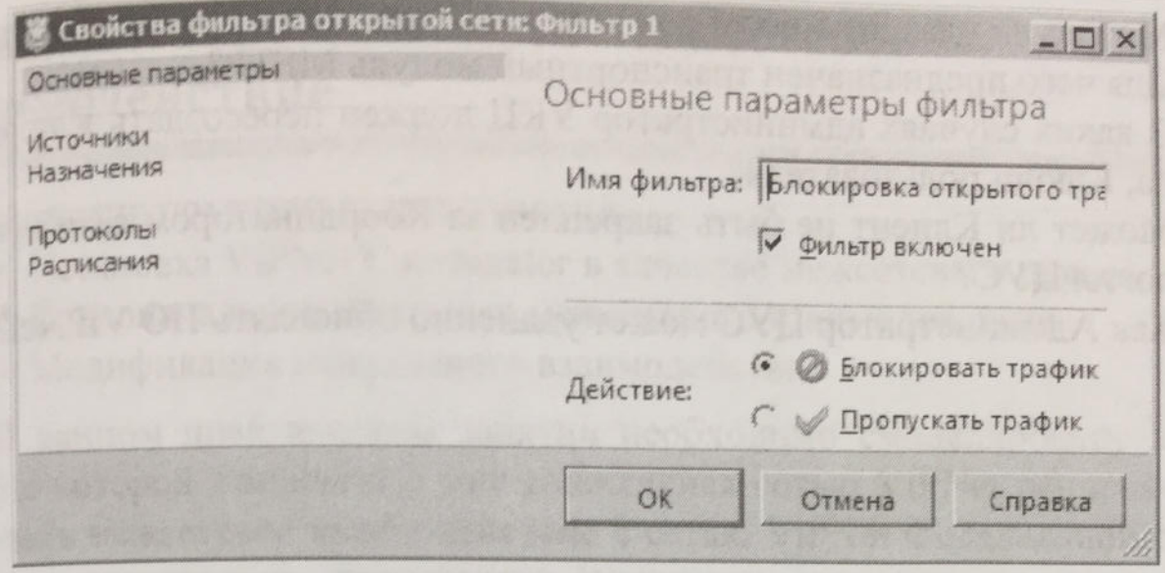

Рис. 127. Вкладка Основные параметры окна Свойства фильтра открытой сети

Проверить были ли приняты политики или нет в данном случае не получится, так как данный узел не был развернут.

Задание 2.4. Дополнительное задание

1. Настройте ViPNet Удостоверяющий и ключевой центр таким образом, чтобы ключи узлов автоматически создавались после формирования справочников в программе *ViPNet Центр управления сетью*.

2. Просмотрите журнал IP-пакетов узла *Помощник глав admина* с рабочего места *Главного администратора*.

Контрольные вопросы

1. Опишите процедуру создания нового сетевого узла и пользователя на нем.
2. Назовите виды мастер-ключей в ПО ViPNet и их назначение.
3. Для чего используются группы узлов в ViPNet Administrator?
4. Чем отличаются связи между пользователями от связей между узлами?
5. Что такое компрометация ключей?
6. В каких случаях ключи считаются скомпрометированными?
7. Требуется ли создавать ключи узлов при изменении связей пользователей? Связей сетевых узлов? Имени сетевого узла?
8. Что делать при компрометации ключей пользователя?
9. Что делать при компрометации ключей Администратора сети?
10. Что содержится в дистрибутиве ключей *.dst?
11. Перечислите назначение всех компонентов, входящих в состав *.dst.
12. Что содержится в ключах пользователя?
13. Что содержится в справочниках?
14. Что содержится в ключах узла?
15. Для чего используются группы объектов в ViPNet Policy Manager?

16. Можно ли удаленно получить журнал IP-пакетов с другой машины?
17. Для чего предназначен транспортный модуль MFTP?
18. В каких случаях администратор УКЦ должен пересоздать Ключи узла, Ключи пользователя?
19. Может ли Клиент не быть закреплен за Координатором сети в топологии ЦУС?
20. Как Администратор ЦУС может удаленно обновлять ПО ViPNet?