ViPNet Центр управления сетью 4

Руководство администратора

infotecs

ФРКЕ.00109-07 32 01

Версия продукта 4.6.4

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: https://infotecs.ru/

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение ... **9**
О документе ... 10
Для кого предназначен документ ... 10
Соглашения документа ... 10
О программе ... 12
Новые возможности 4.6.4 ... 13
Системные требования ... 15
Серверное приложение ... 15
Клиентское приложение ... 16
Комплект поставки ... 18
Обратная связь ... 19

Глава 1. Общие сведения о сетях ViPNet ... **20**
Принцип функционирования сети ViPNet ... 21
Лицензия на сеть ViPNet ... 23
Программа ViPNet Центр управления сетью ... 24
Назначение программы ViPNet Центр управления сетью ... 24
Архитектура программы ViPNet Центр управления сетью ... 24
Взаимодействие с программой ViPNet Удостоверяющий и ключевой центр ... 25
Взаимодействие с программой ViPNet Registration Point ... 26
Связи между объектами сети ViPNet ... 29
Роли сетевых узлов ... 31
Справочники и ключи ViPNet ... 32
Функции координатора в защищенной сети ViPNet ... 33
Туннелирование ... 35
Параметры подключения защищенных узлов к внешней сети ... 37
Принципы осуществления соединений в сети ViPNet ... 37
Подключение без использования межсетевого экрана ... 39
Подключение через координатор ... 40
Подключение через межсетевой экран с динамической трансляцией адресов ... 42
Подключение через межсетевой экран со статической трансляцией адресов ... 44

Глава 2. Начало работы с программой ViPNet Центр управления сетью ... **47**
Установка программы ViPNet Центр управления сетью ... 48
Запуск и завершение работы программы ViPNet Центр управления сетью ... 49

Запуск серверного приложения 49
Запуск и завершение работы клиентского приложения 49
Первый запуск клиентского приложения 51
Интерфейс программы ViPNet Центр управления сетью 54
Представление «Моя сеть» 55
Представление «Доверенные сети» 56
Представление «Администрирование» 58
Создание сети ViPNet: порядок действий 60
Создание структуры сети ViPNet с помощью мастера 62
Загрузка существующей структуры сети из программы версии 3.x 67

Глава 3. Управление сетью ViPNet 69
Основные возможности программы ViPNet Центр управления сетью 70
Управление учетными записями администраторов 72
Многопользовательская работа в программе 72
Создание учетной записи 72
Удаление учетной записи 73
Изменение пароля учетной записи 74
Настройка параметров программы по умолчанию 75
Параметры работы с объектами сети 75
Параметры безопасности узлов 76
Роли узлов по умолчанию 79
Параметры журналов 81
Проверка конфигурации сети 83
Создание отчета о структуре сети 85
Отправка обновлений на сетевые узлы 87
Обновление справочников и ключей 87
Создание справочников 88
Отправка справочников и ключей 91
Обновление программного обеспечения 94
Резервное копирование и восстановление данных 99
Просмотр журналов 100
Журналы аудита 100
Журналы транспортных конвертов 102
Работа с лицензией 106
Просмотр сведений о лицензии для своей сети 106
Обновление лицензии 108
Создание отчетов о лицензии на сеть 110

Глава 4. Настройка параметров сетевых узлов ... 111
Создание сетевого узла ... 112
Добавление координатора ... 112
Добавление клиента ... 113
Удаление сетевого узла ... 116
Удаление координатора ... 116
Удаление клиента ... 117
Настройка параметров координатора ... 118
Просмотр и изменение основных параметров координатора ... 119
Изменение списка узлов, зарегистрированных на координаторе ... 120
Настройка межсерверных каналов между координаторами, выполняющими функции VPN-сервера ... 122
Настройка туннелирования ... 123
Перенос координатора без функций VPN-сервера на другой координатор ... 125
Настройка параметров клиента ... 128
Просмотр и изменение основных параметров клиента ... 128
Перенос клиента на другой координатор ... 129
Перенос клиента, являющегося Центром управления сетью, на другой координатор ... 132
Смена сервера IP-адресов ... 134
Изменение списка пользователей сетевого узла ... 136
Изменение связей между сетевыми узлами ... 138
Связи с сетевыми узлами ... 138
Связи с группами узлов ... 140
Добавление ролей на сетевые узлы ... 142
Изменение списка ролей сетевого узла ... 142
Групповое добавление ролей на сетевые узлы ... 144
Изменение уровня полномочий пользователя ... 146
Настройка параметров роли «Обмен сообщениями и файлами» ... 147
Добавление ролей «DNS-Сервер» и «WINS-Сервер» ... 148
Настройка списка управляемых узлов для роли «Policy Manager» ... 149
Изменение числа узлов мониторинга для роли «StateWatcher» ... 150
Изменение допустимого числа запросов для роли «Registration Point» ... 151
Настройка параметров роли «Terminal» ... 152
Настройка полномочий пользователя ViPNet Terminal ... 153
Настройка параметров подключения USB-модема в терминальной сессии ... 155
Настройка параметров прокси-сервера для веб-браузера ... 157
Настройка дополнительных параметров терминала ... 159
Изменение списка терминальных серверов ... 160

Настройка параметров подключения к терминальному серверу ... 160
Добавление пользовательских параметров ... 164
Включение функции защищенного интернет-шлюза ... 165
Изменение числа элементов кластера для роли «Cluster Windows» ... 166
Настройка типа межсетевого экрана ПАК ViPNet Coordinator IG ... 166
Настройка защищенных DNS-серверов ... 168
Настройка списка защищенных DNS-серверов и доменных зон ... 168
Настройка списков DNS- и WINS-серверов сетевого узла ... 172
Задание адресов сетевого узла ... 175
Задание IP-адресов сетевого узла ... 175
Задание DNS-имен сетевого узла ... 177
Задание адреса для связи по каналу SMTP ... 177
Настройка параметров подключения к внешней сети ... 178
Параметры межсетевого экрана координатора ... 178
Параметры межсетевого экрана клиента ... 180
Настройка подключения через межсетевой экран с динамической трансляцией адресов ... 182
Настройка подключения через межсетевой экран со статической трансляцией адресов ... 183
Настройка подключения через координатор в качестве межсетевого экрана ... 185
Настройка параметров межсетевого экрана клиентов на сервере IP-адресов ... 186
Изменение списка групп, в которые входит сетевой узел ... 189
Работа с шаблонами сетевых узлов ... 191
Создание шаблона сетевых узлов ... 191
Настройка шаблона сетевых узлов ... 192
Применение шаблонов для редактирования свойств сетевых узлов ... 194
Удаление шаблона сетевых узлов ... 195
Работа с группами узлов ... 196
Добавление группы узлов ... 196
Удаление группы узлов ... 197
Изменение списка сетевых узлов в группе ... 197
Изменение связей с сетевыми узлами ... 198
Изменение связей с группами узлов ... 199

Глава 5. Настройка параметров пользователей ... 202
Создание пользователя и настройка его параметров ... 203
Добавление пользователя ... 204
Удаление пользователя ... 204
Основные параметры пользователя ... 205

Изменение списка сетевых узлов пользователя ... 206
Изменение связей между пользователями ... 207
Изменение псевдонимов пользователя ... 210
Изменение списка групп, в которые входит пользователь ... 211
Изменение связей пользователя с группами пользователей ... 212
Работа с группами пользователей ... 215
Добавление группы пользователей ... 215
Удаление группы пользователей ... 216
Изменение списка участников группы пользователей ... 216
Изменение связей группы пользователей ... 218

Глава 6. Иерархическая система сетей ViPNet ... 220
Принцип работы иерархической системы сетей ViPNet ... 221
Развертывание иерархической системы сетей ViPNet ... 223
Распределение общей лицензии между сетями ... 225
Распределение лицензии для всех сетей ... 225
Назначение лицензионных ограничений для отдельной сети ... 227
Просмотр сведений об общей лицензии ... 230

Глава 7. Межсетевое взаимодействие ... 232
Организация межсетевого взаимодействия ... 233
Инициация межсетевого взаимодействия ... 234
Особенности создания межсетевой информации в ПО ViPNet Administrator 3.x ... 236
Прием и обработка полученной межсетевой информации ... 236
Завершение организации межсетевого взаимодействия ... 240
Связи с объектами доверенных сетей ... 242
Изменение списка объектов, участвующих в межсетевом взаимодействии ... 243
Изменение связей с объектами доверенной сети ... 245
Изменение статуса связей с объектами доверенных сетей ... 247
Изменение шлюзового координатора своей сети ... 249
Отправка межсетевой информации ... 251
Создание межсетевой информации ... 252
Отправка межсетевой информации через сеть ViPNet ... 252
Групповая отправка межсетевой информации ... 253
Передача межсетевой информации в виде файла ... 254
Прием межсетевой информации ... 255
Обработка межсетевой информации для отдельной сети ... 256
Групповая обработка межсетевой информации ... 257
Загрузка межсетевой информации из файла ... 259

Прекращение межсетевого взаимодействия ... 261

Приложение A. Возможные неполадки и способы их устранения ... 262

Не удается установить соединение с сервером ViPNet Центр управления сетью ... 262

Не удается установить соединение с SQL-сервером ... 263

Ошибка при вводе имени администратора и пароля ... 264

Некорректная обработка межсетевой информации ... 264

Ошибки при загрузке структуры сети из программы ViPNet Центр управления сетью версии 3.x ... 264

Истекает срок действия лицензии на сеть ViPNet ... 265

Превышено максимальное число узлов, на которые добавлена роль ... 265

Ошибки при сохранении отчета о структуре сети ... 265

Приложение B. Роли сетевых узлов ... 266

Приложение C. История версий ... 278

Что нового в версии 4.6.3 ... 278

Что нового в версии 4.6.2 ... 281

Что нового в версии 4.5 ... 285

Что нового в версии 4.4 ... 286

Что нового в версии 4.3 ... 288

Что нового в версии 4.2 ... 291

Что нового в версии 4.1 ... 294

Что нового в версии 4.0 ... 296

Приложение D. Глоссарий ... 299

Приложение E. Указатель ... 311

Введение

О документе 10

О программе 12

Новые возможности 4.6.4 13

Системные требования 15

Комплект поставки 18

Обратная связь 19

О документе

Данный документ является руководством по работе с программой ViPNet® Центр управления сетью. Документ содержит общие сведения о технологии ViPNet, краткое описание установки программы ViPNet Центр управления сетью, а также основные сценарии работы администратора сети ViPNet с программой: создание сети, изменение параметров объектов сети, установление межсетевого взаимодействия, настройка программы и другие.

Также рекомендуется ознакомиться с другой документацией, входящей в комплект поставки программного обеспечения ViPNet Administrator (см. «Комплект поставки» на стр. 18).

Для кого предназначен документ

Настоящий документ предназначен для администраторов, в обязанности которых входит создание, настройка и управление защищенной сетью ViPNet с помощью программы ViPNet Центр управления сетью.

Предполагается, что читатель данного руководства имеет общее представление о сетевых технологиях и принципах организации сетей ViPNet.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.

Обозначение	Описание
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

О программе

Программа ViPNet Центр управления сетью является составной частью программного обеспечения ViPNet Administrator®, которое используется для администрирования сетей ViPNet. Программа ViPNet Центр управления сетью предназначена для формирования структуры сети ViPNet, задания основных параметров сетевых узлов и пользователей, централизованной отправки обновлений ключей, справочников и программного обеспечения на сетевые узлы ViPNet.

Программа ViPNet Центр управления сетью включает два компонента:

- Серверное приложение, с помощью которого осуществляется работа с базой данных, содержащей полную информацию о структуре и объектах сети ViPNet.
- Клиентское приложение, которое представляет собой удобный графический интерфейс для управления структурой сети ViPNet и свойствами сетевых объектов.

  Возможно удаленное подключение клиентского приложения к серверному приложению, а также одновременное подключение к серверу нескольких клиентских приложений.

Новые возможности 4.6.4

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью по сравнению с версией 4.6.3. Информация об изменениях в предыдущих версиях программы приведена в приложении История версий (на стр. 278).

- **Настройка типа межсетевого экрана для ПАК ViPNet Coordinator IG**

  В зависимости от требований, предъявляемых к функциям безопасности межсетевых экранов, вы можете настроить межсетевой экран ПАК ViPNet Coordinator IG для применения в промышленных сетях (тип «Д») или для использования в традиционной инфраструктуре IP-сетей (тип «А», настроен по умолчанию). Тип межсетевого экрана определяется классификацией ФСТЭК. Вы можете выбрать тип межсетевого экрана (см. «Настройка типа межсетевого экрана ПАК ViPNet Coordinator IG» на стр. 166) в свойствах роли координатора на базе ПАК ViPNet Coordinator IG.

  Информация о типе межсетевого экрана записывается в справочники и ключи и передается на сетевой узел по сети ViPNet. После получения справочников и ключей на сетевом узле администратор ПАК ViPNet Coordinator IG сможет управлять режимами работы в соответствии с выбранным типом межсетевого экрана. Подробнее о режимах работы см. в комплекте документации на ПАК ViPNet Coordinator IG.

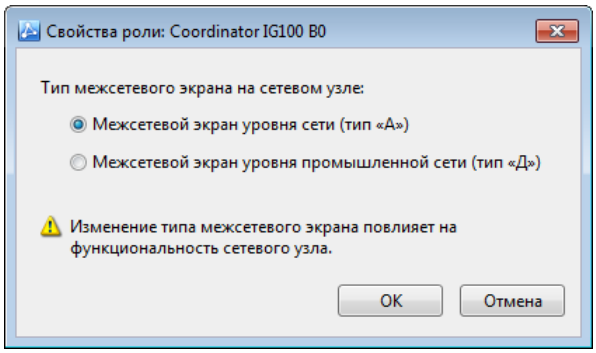

Рисунок 1. Настройка типа межсетевого экрана для ПАК ViPNet Coordinator IG

- **Поддержка нового клиента с ПО ViPNet Client for Linux**

  В программу ViPNet Центр управления сетью была добавлена новая роль «Client for Linux», которая позволяет установить ПО ViPNet Client for Linux для защиты IP-трафика на клиентах с ОС Linux.

- **Поддержка нового координатора на базе ПАК ViPNet Coordinator KB5000**

  В программу ViPNet Центр управления сетью была добавлена новая роль «Coordinator KB5000», которая позволяет развернуть координатор на базе ПАК ViPNet Coordinator KB5000. При этом для ViPNet CSP должна быть установлена самая последняя версия программного обеспечения.

- **Обновление ПО ViPNet Connect для разных операционных систем (Windows или Android)**

  Раньше при отправке обновлений ПО ViPNet Connect был один тип обновлений, которое рассылалось на все сетевые узлы с ролью «Connect» без учета разницы между

операционными системами. Теперь при обновлении ПО ViPNet Connect на сетевых узлах с ОС Windows и Android вы можете выбрать соответствующий тип обновления ПО «Connect для Windows» или «Connect для Android».

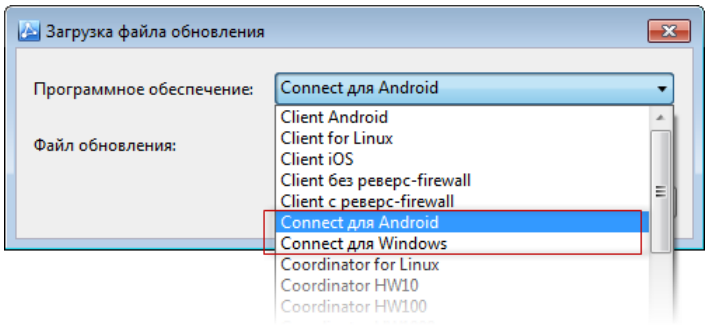

Рисунок 2. Выбор типа обновления ПО ViPNet Connect

- **Автоматическое использование имени и координатора узла из шаблона при создании сетевого узла**

  Раньше при создании сетевого узла вам приходилось вводить имя и выбирать координатор сетевого узла, даже если был добавлен шаблон сетевого узла с соответствующими заданными параметрами узла. Теперь при создании сетевых узлов, если вы применяете шаблон, новому узлу автоматически назначаются имя и координатор сетевого узла из шаблона. Параметры сетевого узла из шаблона в окне создания нового сетевого узла становятся недоступными для редактирования. В случае добавления нескольких шаблонов сетевых узлов, меняя приоритет шаблона, вы можете задавать необходимые имя или координатор узла из шаблона.

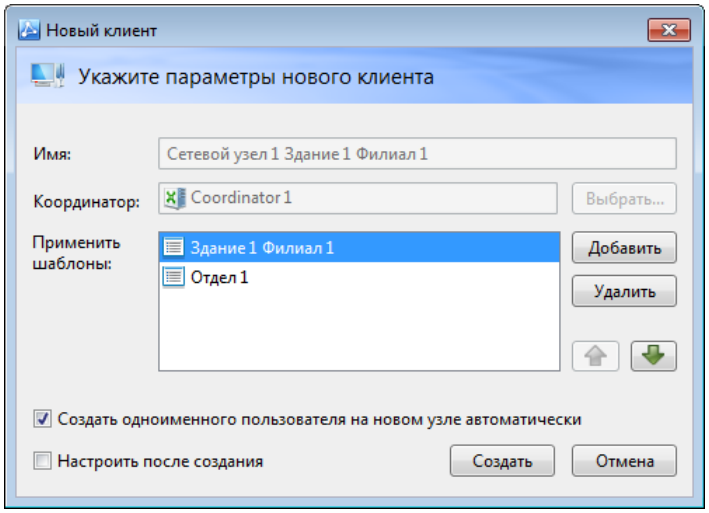

Рисунок 3. Создание сетевых узлов на основании шаблона

Системные требования

Требования к компьютеру для установки программы ViPNet Центр управления сетью определяются в соответствии с требованиями для ее компонентов.

Примечание. При установке всех приложений ViPNet Центр управления сетью на один компьютер он должен удовлетворять максимальным требованиям из указанных.

Серверное приложение

Требования к аппаратному обеспечению компьютера для установки серверного приложения ViPNet Центр управления сетью:

- Процессор — Intel Core 2 Quad или другой схожий по производительности x86-совместимый процессор с количеством ядер 4 и более.
- Объем оперативной памяти — не менее 4 Гбайт.

Примечание. При большом количестве узлов и связей в сети ViPNet рекомендуется использовать более мощный компьютер:

- Процессор — Intel Core i7 или другой схожий по производительности x86-совместимый процессор с количеством ядер 8 и более.
- Объем оперативной памяти — не менее 16 Гбайт.
- Редакция Microsoft SQL Server выше, чем Express Edition.

- Свободное место на жестком диске — не менее 20 Гбайт.
- Операционная система — Windows 7 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

  Для операционной системы должен быть установлен самый последний пакет обновлений.
- При использовании Internet Explorer — версия 8 или выше.

Примечание. Перед установкой серверного приложения ViPNet Центр управления сетью убедитесь, что на вашем компьютере в разделе **Программы и компоненты** > **Включение или отключение компонентов Windows** включен компонент **Возможности .Net Framework 3.5**.

Для установки и функционирования серверного приложения ViPNet Центр управления сетью необходимо следующее программное обеспечение сторонних производителей:

- На компьютере должны быть установлены следующие приложения:
  - Microsoft .NET Framework версии 4.6.2 (программная платформа). Поставляется в комплекте.
  - Microsoft Visual C++ 2010 Redistributable Package (набор компонентов среды выполнения библиотек Visual C++).

  Указанные приложения включены в комплект поставки программного обеспечения ViPNet Центр управления сетью.
- Для размещения базы данных на компьютере с серверным приложением или на другом компьютере, доступном по сети, должна быть установлена система управления базами данных (СУБД). Поддерживаются следующие версии СУБД:
  - Microsoft SQL Server 2008 SP3 и выше.
  - Microsoft SQL Server 2008 R2 SP1 и выше.
  - Microsoft SQL Server 2012.
  - Microsoft SQL Server 2014 (рекомендуется).

  Редакция указанных СУБД может быть любой, в том числе и Express Edition. В комплект поставки программного обеспечения ViPNet Центр управления сетью включена СУБД Microsoft SQL Server 2014 Express. При необходимости она может быть автоматически установлена вместе с серверным приложением.

Внимание! В процессе эксплуатации программы ViPNet Центр управления сетью необходимо отслеживать выпуск обновлений безопасности для указанного ПО Microsoft и своевременно их устанавливать.

Клиентское приложение

Требования к аппаратному обеспечению компьютера для установки клиентского приложения ViPNet Центр управления сетью:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт (при использовании 64-разрядных версий ОС Microsoft Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 1 Гбайт.
- Операционная система — Windows 7 (32/64-разрядная), Windows Server 2008 R2 (64-разрядная), Windows 8 (32/64-разрядная), Windows Server 2012 (64-разрядная), Windows 8.1 (32/64-разрядная), Windows Server 2012 R2 (64-разрядная), Windows 10 (32/64-разрядная).

  Для операционной системы должен быть установлен самый последний пакет обновлений.

- При использовании программы Internet Explorer — версия 11.

Примечание. Перед установкой серверного приложения ViPNet Центр управления сетью убедитесь, что на вашем компьютере в разделе **Программы и компоненты** > **Включение или отключение компонентов Windows** включен компонент **Возможности .Net Framework 3.5**.

Для установки и функционирования клиентского приложения ViPNet Центр управления сетью на компьютере должно быть установлено следующее программное обеспечение сторонних производителей:

- Microsoft .NET Framework версии 4.6.2 (программная платформа).
- Microsoft Visual C++ 2010 Redistributable Package (набор компонентов среды выполнения библиотек Visual C++).

Указанные приложения включены в комплект поставки программного обеспечения ViPNet Центр управления сетью.

Внимание! В процессе эксплуатации программы ViPNet Центр управления сетью необходимо отслеживать выпуск обновлений безопасности для указанного ПО Microsoft и своевременно их устанавливать.

Комплект поставки

В комплект поставки программного обеспечения ViPNet Administrator входит:

- Установочный файл серверного приложения ViPNet Центр управления сетью.
- Установочный файл клиентского приложения ViPNet Центр управления сетью.
- Приложения сторонних производителей, необходимые для работы компонентов программы ViPNet Центр управления сетью.
- Установочный файл программы ViPNet Удостоверяющий и ключевой центр.
- Документация в формате PDF:
  - «ViPNet Administrator. Руководство по установке».
  - «ViPNet Administrator. Руководство по обновлению с версии 3.2.x до версии 4.x».
  - «ViPNet Administrator. Руководство по миграции программного обеспечения на другой компьютер».
  - «ViPNet Administrator. Быстрый старт».
  - «ViPNet Administrator. Лицензионные соглашения на компоненты сторонних производителей».
  - «ViPNet Центр управления сетью. Руководство администратора».
  - «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».
  - «ViPNet CSP. Руководство пользователя».
  - «Развертывание сети под управлением ViPNet Administrator 4.x. Руководство администратора».
  - «Новые возможности ViPNet Administrator. Приложение к документации ViPNet».
  - «Основные термины и определения. Приложение к документации ViPNet».
  - «Классификация полномочий. Приложение к документации ViPNet».
  - «Печать сертификатов. Приложение к документации ViPNet».

Примечание. Список приложений, необходимых для работы программы ViPNet Центр управления сетью, содержится в разделе Системные требования (на стр. 15).

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание продуктов ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Сборник часто задаваемых вопросов (FAQ) https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Техническая поддержка для пользователей продуктов ViPNet: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки https://infotecs.ru/support/request/.
- Консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6192,

  8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения https://infotecs.ru/disclosure.php. Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru.

1

Общие сведения о сетях ViPNet

Принцип функционирования сети ViPNet 21

Лицензия на сеть ViPNet 23

Программа ViPNet Центр управления сетью 24

Связи между объектами сети ViPNet 29

Роли сетевых узлов 31

Справочники и ключи ViPNet 32

Функции координатора в защищенной сети ViPNet 33

Туннелирование 35

Параметры подключения защищенных узлов к внешней сети 37

Принцип функционирования сети ViPNet

Сеть ViPNet представляет собой наложенную сеть, которая может быть развернута поверх локальных или глобальных сетей любой структуры. Для защиты информации в сети ViPNet используются две технологии:

- VPN (см. глоссарий, стр. 301) — технология, обеспечивающая защиту соединений между локальным сетями или отдельными компьютерами с использованием средств криптографии.
- PKI (см. глоссарий, стр. 300) — технология, основным элементом которой является использование пары асимметричных ключей для формирования электронной подписи, аутентификации и других целей.

  В рамках одной сети ViPNet может применяться одна из этих технологий либо обе технологии одновременно. Сеть ViPNet, в которой используется технология VPN, называется защищенной сетью.

Сеть ViPNet состоит из сетевых узлов (см. глоссарий, стр. 307) — компьютеров и других устройств, на которых установлено программное обеспечение ViPNet. Сетевые узлы делятся на две категории:

- Координаторы — серверы сети ViPNet. Основная функция координатора — маршрутизация прикладных и управляющих транспортных конвертов (см. глоссарий, стр. 308), передаваемых между клиентами. На координаторе могут быть отключены функции сервера IP-адресов и транспортного сервера (см. «Функции координатора в защищенной сети ViPNet» на стр. 33). В этом случае координатор не обеспечивает обмен служебной информацией о параметрах доступа узлов друг к другу.
- Клиенты — рабочие места пользователей сети ViPNet.

Для каждого сетевого узла администратор сети ViPNet создает одного или несколько пользователей, которые будут работать на узле, а также задает набор ролей (см. «Роли сетевых узлов» на стр. 31), от которого зависят возможности узла и программное обеспечение, которое может быть установлено на этом узле. Список ролей, которые могут быть использованы в сети, а также ограничения на количество узлов с различными ролями, максимальное количество сетевых узлов и другие ограничения содержатся в файле лицензии на сеть ViPNet (см. «Лицензия на сеть ViPNet» на стр. 23).

Для упрощения процесса управления сетевыми узлами и пользователями администратор сети ViPNet может объединить несколько сетевых узлов в группу узлов (см. «Работа с группами узлов» на стр. 196), несколько пользователей — в группу пользователей (см. «Работа с группами пользователей» на стр. 215).

В защищенной сети ViPNet узлы, на которые установлено программное обеспечение ViPNet называются защищенными узлами (см. глоссарий, стр. 302), узлы без программного обеспечения ViPNet — открытыми (см. глоссарий, стр. 305). В сети ViPNet также могут присутствовать туннелируемые узлы (см. «Туннелирование» на стр. 35).

На защищенных узлах программное обеспечение ViPNet осуществляет две основные функции:

- Фильтрацию всего IP-трафика сетевых узлов.
- Шифрование соединений между защищенными узлами. Для шифрования трафика используются симметричные ключи (см. «Справочники и ключи ViPNet» на стр. 32), которые создаются и распределяются централизованно.

  Возможность соединений между защищенными узлами определяется связями (см. «Связи между объектами сети ViPNet» на стр. 29), которые задает администратор сети ViPNet.

Для управления сетью ViPNet используется программное обеспечение ViPNet Administrator, которое включает два компонента:

- ViPNet Центр управления сетью (см. «Программа ViPNet Центр управления сетью» на стр. 24) — программа, предназначенная для управления структурой сети, свойствами сетевых узлов и пользователей.
- ViPNet Удостоверяющий и ключевой центр (см. глоссарий, стр. 300) — программа, предназначенная для формирования ключей узлов и пользователей ViPNet, а также осуществляющая функции удостоверяющего центра.

Лицензия на сеть ViPNet

Для того чтобы развернуть сеть ViPNet, необходима соответствующая лицензия, которую можно приобрести в ОАО «ИнфоТеКС» (см. «Обратная связь» на стр. 19).

Параметры сети ViPNet, которые определяются приобретенной лицензией, хранятся в лицензионном файле `*.itcslic` или `infotecs.reg`. Этот файл необходимо предоставить при первом запуске программы ViPNet Центр управления сетью, иначе продолжить работу будет невозможно (подробнее см. документ «ViPNet Administrator. Руководство по установке»).

Файл лицензии содержит следующую информацию:

- Номер сети ViPNet и номера подчиненных сетей — в том случае, если лицензия предполагает создание иерархии сетей ViPNet (см. «Иерархическая система сетей ViPNet» на стр. 220).
- Сведения о владельце сети.
- Возможность использования функций удостоверяющего центра и максимальное число сертификатов ключа проверки электронной подписи, которое может быть издано в УКЦ для внешних пользователей и пользователей ViPNet.
- Список ролей, разрешенных для использования в сети ViPNet и ограничения на количество узлов с различными ролями (см. «Роли сетевых узлов» на стр. 31).
- Ограничения на версии и период использования программного обеспечения для ролей.
- Общий срок действия лицензии.

При необходимости расширить сеть ViPNet и ее возможности вы можете обновить лицензию. Подробнее о работе с лицензией см. раздел Работа с лицензией (на стр. 106).

Программа ViPNet Центр управления сетью

Назначение программы ViPNet Центр управления сетью

Программа ViPNet Центр управления сетью является составной частью программного обеспечения ViPNet Administrator, которое также включает программу ViPNet Удостоверяющий и ключевой центр. Программное обеспечение ViPNet Administrator используется для создания и управления наложенными сетями ViPNet (см. «Принцип функционирования сети ViPNet» на стр. 21).

Программа ViPNet Центр управления сетью предназначена для осуществления следующих функций:

- Управление структурой сети ViPNet: создание сетевых узлов и пользователей, а также определение различных связей между ними.
- Настройка свойств объектов сети ViPNet: добавление ролей на сетевые узлы (см. «Роли сетевых узлов» на стр. 31), настройка параметров доступа к сетевым узлам (IP-адреса, DNS-имена и так далее) и способа подключения к внешней сети.
- Управление иерархической системой сетей ViPNet (см. «Иерархическая система сетей ViPNet» на стр. 220): распределение лицензионных ограничений между подчиненными сетями (при наличии специального лицензионного файла).
- Межсетевое взаимодействие (на стр. 232): организация защищенного соединения с другими сетями ViPNet, управление связями между узлами своей сети и узлами доверенных сетей, обмен межсетевой информацией.
- Отправка обновлений на сетевые узлы ViPNet (см. «Отправка обновлений на сетевые узлы» на стр. 87): удаленное обновление на сетевых узлах информации, необходимой для нормального функционирования сети — справочников и ключей (см. «Справочники и ключи ViPNet» на стр. 32), программного обеспечения ViPNet.

Архитектура программы ViPNet Центр управления сетью

Программа ViPNet Центр управления сетью состоит из двух компонентов: серверного приложения и клиентского приложения. Кроме того, в работе программы используется база данных SQL, в которой хранится информация о структуре и объектах сети ViPNet.

Серверное приложение ЦУСа представляет собой набор служб, которые осуществляют чтение и запись информации в базу данных SQL и обеспечивают взаимодействие с клиентским приложением. База данных размещается на SQL-сервере, который может быть установлен на одном компьютере с серверным приложением или на удаленном компьютере. Клиентское приложение обеспечивает удобный графический интерфейс для управления структурой сети ViPNet (см. глоссарий, стр. 307) и свойствами сетевых объектов. Оно может быть установлено на одном компьютере с серверным приложением, на удаленном компьютере или на нескольких компьютерах, если управление сетью ViPNet осуществляется с нескольких рабочих мест. В процессе работы клиентское приложение подключается к серверному приложению локально или через сеть, при этом возможно одновременное подключение к серверному приложению нескольких клиентских приложений. Таким образом, обеспечивается возможность многопользовательской работы в программе ViPNet Центр управления сетью.

Рисунок 4. Компоненты программы ViPNet Центр управления сетью

Взаимодействие с программой ViPNet Удостоверяющий и ключевой центр

Программа ViPNet Удостоверяющий и ключевой центр предназначена для создания ключей сетевых узлов и пользователей сети ViPNet, а также для выполнения функций удостоверяющего центра.

Для создания ключей в программе ViPNet Удостоверяющий и ключевой центр используются данные о структуре и объектах сети ViPNet, которые формируются в программе ViPNet Центр управления сетью. Созданные ключи и сертификаты могут быть переданы в Центр управления сетью для отправки на сетевые узлы.

Программа ViPNet Удостоверяющий и ключевой центр обменивается данными с программой ViPNet Центр управления сетью через ту же базу данных SQL, в которой хранится информация о структуре и объектах сети ViPNet. Таким образом, если программа ViPNet Удостоверяющий и ключевой центр установлена отдельно от серверного приложения ЦУСа, необходимо обеспечить сетевое соединение между компьютерами, на которых установлены эти программы. Кроме того, если SQL-сервер установлен отдельно от серверного приложения ЦУСа, необходимо также обеспечить сетевое соединение с компьютером, на котором установлен SQL-сервер.

Рисунок 5. Взаимодействие компонентов ПО ViPNet Administrator

Если администратор Центра управления сетью вносит в структуру сети какие-либо изменения, информация об изменениях заносится в базу данных. На основании этой информации в программе Удостоверяющий и ключевой центр создаются ключи узлов и пользователей. После того как созданные ключи будут переданы в Центр управления сетью, они могут быть отправлены на сетевые узлы (см. «Отправка справочников и ключей» на стр. 91).

Программы ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр обращаются к общей базе данных, поэтому когда одна из этих программ записывает в базу данных информацию о сети и ее объектах, действия в другой программе могут быть заблокированы. При попытке выполнить заблокированное действие на экране появится соответствующее сообщение. Например, когда администратор ЦУСа вносит в структуру сети какие-либо изменения, формирует справочники или обрабатывает межсетевую информацию, в программе ViPNet Удостоверяющий и ключевой центр блокируются действия по созданию ключей, операции с мастер-ключами и сертификатами администраторов. И наоборот, если администратор Удостоверяющего и ключевого центра формирует ключи для объектов сети, производит смену мастер-ключей или сертификата администратора, в ЦУСе блокируются все операции по добавлению новых объектов в структуру сети и изменению свойств существующих объектов.

Если в ЦУСе создается новая структура сети или конвертируется старая структура, в программе ViPNet Удостоверяющий и ключевой центр блокируются все операции. При этом по завершении работы со структурой сети Удостоверяющий и ключевой центр требуется перезапустить и заново произвести первичную инициализацию, поскольку вместе со структурой сети удаляется текущая ключевая структура. В Центре управления сетью также могут быть заблокированы все операции — при создании или восстановлении в программе ViPNet Удостоверяющий и ключевой центр резервной копии конфигурации.

Взаимодействие с программой ViPNet Registration Point

В программе ViPNet Центр управления сетью предусмотрена автоматическая обработка запросов, поступающих из программы ViPNet Registration Point.

Программа ViPNet Registration Point является частью программного комплекса, включающего программное обеспечение ViPNet Administrator. Она предназначена для выполнения функций

центра регистрации пользователей. Администратор центра регистрации имеет возможность зарегистрировать нового пользователя сети ViPNet и создать для пользователя запрос на получение сертификата электронной подписи или дистрибутива ключей ViPNet (см. глоссарий, стр. 302).

При создании запроса на дистрибутив ключей администратор центра регистрации:

- Указывает, требуется ли добавить пользователя на существующий сетевой узел или создать для пользователя новый сетевой узел.
- Выбирает сетевые узлы, с которыми должен быть связан узел пользователя.

Примечание. Администратор центра регистрации может добавлять связи только с узлами пользователей, зарегистрированных в программе ViPNet Registration Point. Чтобы добавить связь с узлом пользователя, не зарегистрированного в программе ViPNet Registration Point, администратору центра регистрации следует обратиться к администратору Центра управления сетью.

- Выбирает роли, которые должны быть добавлены на узел пользователя.

Для пользователей, зарегистрированных в программе ViPNet Registration Point, администратор может создать запрос на обновление дистрибутива ключей для изменения свойств сетевого узла пользователя, а также запрос на удаление пользователя.

Запросы на создание или обновление дистрибутива ключей, а также запросы на удаление пользователей передаются из программы ViPNet Registration Point в программу ViPNet Центр управления сетью с помощью транспортного модуля ViPNet MFTP.

Внимание! Запросы, размер которых превышает 10 Кбайт, автоматически отклоняются без обработки. Записи об отклоненных запросах заносятся в журнал транспортных конвертов (см. «Журналы транспортных конвертов» на стр. 102).

В программе ViPNet Центр управления сетью поступившие запросы обрабатываются автоматически. В результате создаются новые пользователи и сетевые узлы с заданными свойствами либо изменяются свойства существующих пользователей и узлов. Затем в программе ViPNet Удостоверяющий и ключевой центр для пользователя создается дистрибутив ключей, который автоматически отправляется с помощью транспортного модуля в программу ViPNet Registration Point.

Рисунок 6. Взаимодействие с программой ViPNet Registration Point

Связи между объектами сети ViPNet

В сети ViPNet возможны следующие типы связей между объектами:

- Связь между двумя сетевыми узлами.
- Связь между сетевым узлом и группой сетевых узлов.
- Связь между группами сетевых узлов.
- Связь между двумя пользователями.
- Связь между пользователем и группой пользователей.

Связь между двумя защищенными узлами (см. глоссарий, стр. 302) сети ViPNet обеспечивает возможность соединения между этими узлами. Связи между определенными узлами создаются автоматически и являются обязательными. Такие связи не могут быть удалены. К обязательным связям относятся:

- 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 (см. «Настройка подключения через межсетевой экран с динамической трансляцией адресов» на стр. 182).
- Связи между координаторами, которые образуют межсерверный канал (см. «Настройка межсерверных каналов между координаторами, выполняющими функции VPN-сервера» на стр. 122).
- Связь между узлом с программой ViPNet Policy Manager и подчиненными ему сетевыми узлами.
- Связи шлюзовых координаторов (см. глоссарий, стр. 309) своей сети со шлюзовыми координаторами доверенных сетей (см. глоссарий, стр. 302).
- Связи Центра управления сетью с Центрами управления сетью доверенных сетей.

Также автоматически формируются связи между узлами при создании связей между группами сетевых узлов и связей между узлом и группой узлов. Такие связи между узлами не могут быть удалены, пока существует их связь через группы или пока узлы входят в состав связанных групп.

Использование групп узлов позволяет облегчить создание связей между большим количеством сетевых узлов, а также редактирование данных связей. По умолчанию сетевые узлы, входящие в группу, не связаны между собой. Если требуется связать эти узлы, установите связь данной группы с самой собой.

Также группы узлов могут использоваться для отправки справочников, ключей и обновлений ПО ViPNet целому ряду сетевых узлов (например, удобно отправлять обновления группе координаторов, на которых установлено ПО ViPNet Coordinator for Linux). Подробнее о работе с группами сетевых узлов см. в разделе Работа с группами узлов (на стр. 196).

При создании связи между клиентами должна быть создана связь между координаторами, на которых они зарегистрированы. Также при создании связи между клиентом и другим координатором должна быть установлена связь между связываемым координатором и координатором данного клиента.

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.

Связь между двумя пользователями в программе ViPNet Центр управления сетью позволяет этим пользователям вести конфиденциальную переписку друг с другом в программе ViPNet Деловая почта. Такое сообщение сможет прочесть только тот пользователь, которому оно адресовано. При этом сетевые узлы, на которых зарегистрированы необходимые пользователи, должны также быть связаны между собой. Если пользователь зарегистрирован на нескольких узлах, в программе ViPNet Деловая почта будут отображены пользователи, между сетевыми узлами которых установлена связь.

Если существует связь между двумя сетевыми узлами, но не существует связей между пользователями этих узлов, то в программе ViPNet Деловая почта пользователь одного узла может адресовать зашифрованное сообщение одновременно всем пользователям другого сетевого узла. Каждый пользователь узла, на который адресовано сообщение, сможет его прочесть.

Пользователь может быть связан не только с отдельными пользователями, но и с группами пользователей. При добавлении пользователя в группу (см. «Работа с группами пользователей» на стр. 215) автоматически создается связь между пользователем и этой группой.

Группы пользователей упрощают управление связями между пользователями. Если пользователь связан с группой пользователей, в программе ViPNet Деловая почта он может адресовать зашифрованные сообщения всем пользователям этой группы на определенном сетевом узле или отдельным участникам группы. Это возможно при условии, что связаны сетевые узлы пользователей, которые будут обмениваться сообщениями.

Создание связей между объектами своей сети и объектами доверенных сетей имеет некоторые особенности. Подробнее об этом см. раздел Связи с объектами доверенных сетей (на стр. 242).

Роли сетевых узлов

Роль — это атрибут сетевого узла ViPNet, который определяет возможность использования на сетевом узле какого-либо программного обеспечения или выполнения на узле каких-либо задач.

Роли добавляются на сетевые узлы администратором Центра управления сетью. Список ролей, которые могут быть использованы в конкретной сети ViPNet, и ограничения на количество узлов с различными ролями содержатся в файле лицензии на сеть ViPNet (см. «Просмотр сведений о лицензии для своей сети» на стр. 106).

Каждый сетевой узел может иметь несколько ролей, однако некоторые роли несовместимы друг с другом и не могут быть добавлены на сетевой узел одновременно. Например, роль «Cluster Windows» можно добавить только на координатор с ролью «Программный VPN-координатор». Некоторые роли имеют дополнительные свойства, такие как полномочия пользователя или другие атрибуты (см. «Изменение уровня полномочий пользователя» на стр. 146).

Также в лицензии на сеть ViPNet могут быть предусмотрены дополнительные ограничения на версию и период использования программного обеспечения, соответствующего выбранной роли. Таким образом, на разных узлах, которым назначена одна и та же роль, допускается использование разных версий программного обеспечения. Например, для одного узла с ролью «VPN-клиент» можно выбрать установку программы ViPNet Client последней версии и с индивидуальным периодом использования. На остальных узлах с той же ролью можно использовать программу ViPNet Client предыдущей версии в течение общего срока действия лицензии.

Примечание. Количество версий программного обеспечения, соответствующего одной роли, может варьироваться в зависимости от условий лицензии.

Список ролей, которые могут быть добавлены на сетевые узлы при наличии соответствующих разрешений в лицензии на сеть ViPNet, а также информация о свойствах и совместимости ролей приведены в приложении Роли сетевых узлов (на стр. 266).

Справочники и ключи ViPNet

Справочники и ключи представляют собой набор файлов с данными, которые необходимы для взаимодействия между сетевыми узлами ViPNet.

Справочники формируются в программе ViPNet Центр управления сетью и содержат информацию о сетевых узлах, пользователях и их свойствах: идентификаторах, связях, ролях сетевых узлов, адресах и так далее.

Ключи формируются программе ViPNet Удостоверяющий и ключевой центр (см. глоссарий, стр. 300) на основании информации, которая заносятся в базу данных SQL в результате изменения параметров сети в программе ViPNet Центр управления сетью. В сети ViPNet используются ключи двух типов:

- Симметричные ключи, с помощью которых осуществляется шифрование данных, передаваемых между сетевыми узлами ViPNet. Для шифрования используется российский стандарт симметричного шифрования ГОСТ 28147-89.
- Асимметричные ключи, которые используются для формирования и проверки электронной подписи пользователей ViPNet в соответствии с российскими стандартами ГОСТ 34.10-2001 и ГОСТ 34.10-2012. Асимметричные ключи также могут использоваться для шифрования в сторонних приложениях, например, в программах Microsoft Office.

Для работы программного обеспечения ViPNet на сетевых узлах должны быть установлены справочники и ключи. Первоначальная установка справочников и ключей осуществляется с помощью дистрибутива ключей (см. глоссарий, стр. 302). На действующий сетевой узел новые справочники и ключи можно отправлять из программы ViPNet Центр управления сетью по каналам сети ViPNet (см. «Обновление справочников и ключей» на стр. 87).

Функции координатора в защищенной сети ViPNet

В защищенной сети ViPNet координатор является служебным узлом, который может выполнять функции VPN-сервера, маршрутизацию VPN-трафика, функции VPN-шлюза, межсетевого экрана и обеспечивать другие сетевые сервисы. На таком координаторе может быть установлено программное обеспечение ViPNet Coordinator для Windows или Linux, либо он может быть развернут на специальном программно-аппаратном комплексе.

Координатор выполняет в защищенной сети ViPNet следующие функции:

- **VPN-сервер —** функция, объединяющая в себе следующие подфункции:
    - **Сервер IP-адресов** — функция VPN-сервера, которая в автоматическом режиме обеспечивает взаимодействие защищенных узлов (клиентов и координаторов) как внутри данной виртуальной сети, так и при взаимодействии с другими виртуальными сетями ViPNet. Это возможно благодаря использованию специального протокола динамической маршрутизации VPN-трафика, реализующего обмен информацией о параметрах доступа узлов друг к другу. Данный протокол обеспечивает маршрутизацию VPN-трафика между узлами в сети ViPNet тем методом, который наиболее оптимален для используемого способа подключения узла к сети.
    - **Транспортный сервер** — функция VPN-сервера, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами между узлами (см. глоссарий, стр. 308).

      Маршрутизация прикладных и управляющих конвертов осуществляется с помощью транспортного модуля ViPNet MFTP, работающего на прикладном уровне. Транспортный модуль на координаторе принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения.

      Маршрутизация данных между координаторами выполняется на основании межсерверных каналов, заданных для этих координаторов. Межсерверные каналы могут быть организованы по любой схеме. Если есть несколько маршрутов передачи конвертов между координаторами, передача информации осуществляется по кратчайшему из них. Передача информации из одной сети в другую выполняется через шлюзовые координаторы, с помощью которых происходит взаимодействие двух сетей.

  По умолчанию координатор выступает сервером IP-адресов и транспортным сервером. Администратор ЦУСа может создать координатор без функций VPN-сервера, чтобы уменьшить нагрузку на вычислительные ресурсы координатора.
- **Маршрутизатор VPN-пакетов** — функция VPN-сервера, обеспечивающая маршрутизацию транзитного защищенного трафика, проходящего через координатор, на другие защищенные узлы. Маршрутизация осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании

защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется трансляция адресов (NAT) (см. глоссарий, стр. 308). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора.

- **Сервер соединений** — функция, обеспечивающая соединение между клиентами и координаторами по кратчайшему пути, если они находятся в разных подсетях и не могут соединиться друг с другом напрямую.
- **VPN-шлюз** — стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты (см. «Туннелирование» на стр. 35). VPN-шлюз интегрирован с межсетевым экраном для защищенных и открытых соединений, который осуществляет фильтрацию незашифрованного трафика, а также трафика внутри защищенного соединения.
- **Межсетевой экран** — функция, благодаря которой координатор выполняет фильтрацию открытых, транзитных и локальных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.

  Функция трансляции адресов для открытого трафика позволяет задать правила трансляции адресов для решения двух основных задач:

  - Подключение локальной сети к открытым ресурсам Интернета, когда количество узлов локальной сети превышает количество публичных IP-адресов, выданных поставщиком услуг Интернета.
  - Организация доступа к открытым серверам локальной сети из Интернета.
- **Защищенный интернет-шлюз** (ранее — сервер открытого Интернета) — функция, которая позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации. Защищенные узлы, которые имеют связь с защищенным интернет-шлюзом, могут работать в одном из двух режимов:
  - Доступ к защищенной сети ViPNet при отсутствии подключения к Интернету.
  - Доступ в Интернет при отсутствии соединения с защищенными узлами ViPNet.

На координаторе может быть настроен TCP-туннель, позволяющий обеспечить получение IP-пакетов по протоколу TCP и их дальнейшую передачу по протоколу UDP (см. «Настройка подключения через межсетевой экран со статической трансляцией адресов» на стр. 183).

Туннелирование

Технология туннелирования (см. глоссарий, стр. 309) применяется в том случае, если требуется защитить соединения с участием открытых узлов (см. глоссарий, стр. 305) при передаче данных через Интернет или другие публичные сети.

Туннелирование заключается в шифровании трафика открытых узлов компьютерами с программным обеспечением ViPNet Coordinator или программно-аппаратными комплексами ViPNet Coordinator HW, которые играют роль VPN-шлюзов. С помощью технологии туннелирования можно организовать защищенное соединение между открытым узлом и защищенным узлом ViPNet или между двумя открытыми узлами, которые туннелируются разными координаторами.

Туннелирование позволяет организовать защиту трафика узлов, на которых не может быть установлено программное обеспечение ViPNet Client или ViPNet Coordinator (например, различных серверов, сетевых принтеров, сетевых хранилищ данных и так далее).

Защита трафика открытого узла при туннелировании осуществляется следующим образом:

- Открытые IP-пакеты от туннелируемого узла поступают на координатор.
- На координаторе IP-пакеты обрабатываются сетевыми фильтрами, зашифровываются и передаются на защищенный узел, для которого эти пакеты предназначены, либо на другой координатор.
- Если на координатор поступают зашифрованные IP-пакеты, предназначенные для туннелируемого узла, эти IP-пакеты обрабатываются сетевыми фильтрами, расшифровываются и передаются на узел назначения в открытом виде.

Рисунок 7. Защита соединения на сетевом уровне модели OSI

Для того чтобы обеспечивалось туннелирование открытого узла координатором, должны выполняться следующие условия:

- В программе ViPNet Центр управления сетью на координатор должна быть добавлена роль «Программный VPN-координатор» или «Coordinator HW» (см. «Добавление ролей на сетевые узлы» на стр. 142).
- Также в программе ViPNet Центр управления сетью для координатора должно быть задано максимальное число одновременно туннелируемых соединений и указаны адреса туннелируемых узлов (см. «Настройка туннелирования» на стр. 123).
- Туннелируемые узлы должны находиться в одной маршрутизируемой сети с туннелирующим координатором.
- IP-пакеты, отправляемые с туннелируемого узла на защищенные узлы ViPNet, должны направляться через туннелирующий координатор. Этого можно добиться двумя способами:
  - На туннелируемом узле в качестве шлюза по умолчанию указать туннелирующий координатор.
  - На туннелируемом узле задать статические маршруты для защищенных узлов ViPNet через туннелирующий координатор.

Параметры подключения защищенных узлов к внешней сети

Принципы осуществления соединений в сети ViPNet

Защищенные узлы ViPNet могут быть подключены к внешней сети непосредственно либо взаимодействовать с внешней сетью через различные межсетевые экраны, в том числе ViPNet-координатор.

Каждый защищенный узел получает информацию о других узлах ViPNet, параметрах доступа и их активности в данный момент от своего сервера IP-адресов или от других координаторов (если узел сам является сервером IP-адресов). Таким образом, координатор отвечает за сбор и рассылку информации о сетевых узлах на узлы, для которых он выполняет функции сервера IP-адресов.

Сетевые узлы ViPNet могут располагаться в сетях любого типа, поддерживающих IP-протокол. Способ подключения к сети может быть любой: сеть Ethernet, PPPoE через XDSL-подключение, PPP через подключение Dial-up или ISDN, сеть сотовой связи GPRS или UMTS, устройства Wi-Fi, сети MPLS или VLAN. ПО ViPNet поддерживает разнообразные протоколы канального уровня. Для создания защищенных соединений между сетевыми узлами используются IP-протоколы трех типов (IP/241, UDP и TCP), в которые упаковываются пакеты любых других IP-протоколов.

При взаимодействии любых узлов ViPNet между собой, если они расположены в одном сегменте локальной сети и доступны по широковещательным адресам, используется протокол IP/241 (см. глоссарий, стр. 306). Этот протокол более экономичен, так как не имеет UDP-заголовка размером 8 байт. Исходный пакет после шифрования упаковывается в пакет IP-протокола номер 241.

Рисунок 8. Сетевые узлы расположены в одном сегменте локальной сети

Если узлы ViPNet располагаются в разных сегментах сети, то автоматически используется протокол UDP, который позволяет IP-пакетам проходить через межсетевые экраны. Исходный пакет после шифрования упаковывается в UDP-пакет.

Рисунок 9. Сетевые узлы соединяются через межсетевой экран

Если на пути следования IP-пакета расположено устройство NAT, на этом устройстве должны быть настроены динамические или статические правила трансляции адресов, которые разрешают обмен UDP-трафиком с узлами сети ViPNet. При настройке статических правил должен быть указан порт инкапсуляции UDP-пакетов. По умолчанию используется порт 55777, но при необходимости он может быть изменен на любой другой. Если пакеты проходят напрямую через координатор, то номер порта узлов, расположенных за этим координатором, значения не имеет. После прохождения через координатор пакетам присваиваются IP-адреса соответствующего сетевого интерфейса координатора, то есть осуществляется трансляция адресов.

Бывают случаи, когда взаимодействие защищенных узлов по UDP-протоколу невозможно, передача UDP-пакетов провайдером услуг запрещена. Например, при удаленном подключении к сети ViPNet из гостиниц или других общественных мест. В таком случае весь IP-трафик может передаваться через TCP-туннель, настроенный на сервере соединений узла, являющегося инициатором соединения. При настройке TCP-туннеля на сервере соединений (см. глоссарий, стр. 306) может быть указан произвольный порт. По умолчанию используется порт 443.

Рисунок 10. Сетевые узлы соединяются через межсетевой экран

На сервере соединений полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узел назначения по UDP-протоколу.

Примечание. Установление соединений с помощью серверов соединений и TCP-туннелей возможно только в ПО ViPNet версии не ниже 4.2.x. Более подробную информацию вы найдете в документации к ПО ViPNet Client и ViPNet Coordinator соответствующих версий.

На защищенных узлах ViPNet можно настроить следующие типы подключения к внешней сети:

1. Непосредственное подключение к внешней сети (см. «Подключение без использования межсетевого экрана» на стр. 39). В этом случае следует отключить использование межсетевого экрана.
2. Подключение через координатор, обеспечивающий трансляцию адресов для сетевых узлов ViPNet. Тип межсетевого экрана — **Координатор** (см. «Подключение через координатор» на стр. 40).

3 Подключение через межсетевой экран, на котором настройка статических правил трансляции адресов затруднительна или невозможна. Тип межсетевого экрана — **С динамической трансляцией адресов** (см. «Подключение через межсетевой экран с динамической трансляцией адресов» на стр. 42).

4 Подключение через межсетевой экран, на котором возможна настройка статических правил трансляции адресов. Тип межсетевого экрана — **Со статической трансляцией адресов** (см. «Подключение через межсетевой экран со статической трансляцией адресов» на стр. 44).

Чтобы избежать настройки типа подключения непосредственно на каждом сетевом узле, рекомендуется задать параметры подключения сетевых узлов централизованно в программе ViPNet Центр управления сетью.

Примечание. Настройки подключения через межсетевой экран, заданные в ЦУСе, применяются только на клиентах с версией ПО ViPNet Client ниже 4.2. Клиенты с ПО версии 4.2 и выше всегда используют тип подключения **С динамической трансляцией адресов**.

Подключение без использования межсетевого экрана

Данный тип подключения следует выбирать на защищенном узле, если он имеет хотя бы один IP-адрес, доступный по общим правилам маршрутизации пакетов любым другим узлам, с которыми данный узел должен устанавливать соединения. Например, это может быть публичный IP-адрес.

Защищенные узлы, использующие такой тип подключения, всегда соединяются друг с другом напрямую по протоколу IP/241 (см. глоссарий, стр. 306). При этом шифрованный трафик от таких клиентов к координаторам, а также к клиентам, использующим в качестве межсетевого экрана координаторы, всегда инкапсулируется в UDP-пакеты.

Внимание! Если на сетевом узле, который имеет частный IP-адрес внутри локальной сети и подключен к Интернету через межсетевой экран, настроено подключение без использования межсетевого экрана, то этот узел не сможет устанавливать соединения с сетевыми узлами ViPNet, расположенными вне локальной сети с ее системой частных IP-адресов.

Рисунок 11. Подключение без использования межсетевого экрана на клиентах

Если координатор использует данный тип соединения и находится на границе двух сегментов сети, то он осуществляет трансляцию сетевых адресов (NAT) для всех защищенных соединений в обоих направлениях. Проходящий через координатор зашифрованный трафик, инкапсулированный в UDP-пакеты, пересылается с заменой адреса отправителя пакета на IP-адрес соответствующего сетевого интерфейса координатора. Если координатор выполняет функцию туннелирующего сервера (VPN-шлюза) (см. «Туннелирование» на стр. 35), он также осуществляет трансляцию адресов для туннелируемого трафика.

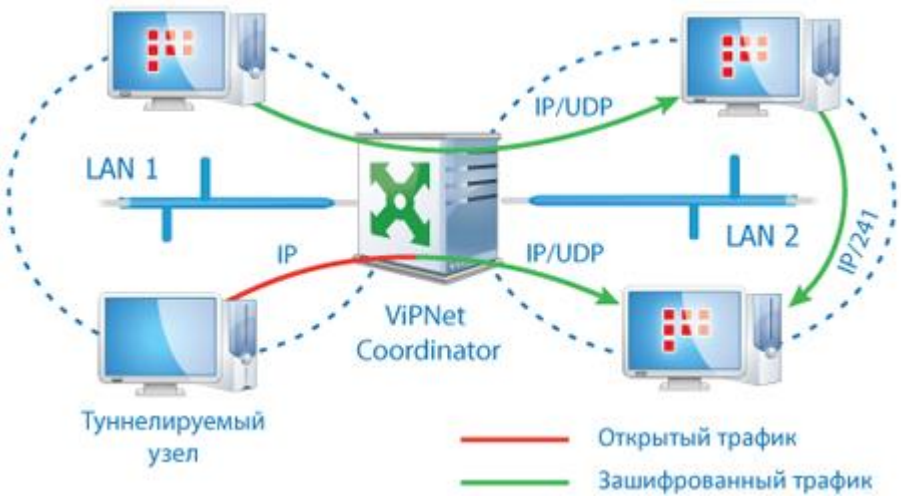

Рисунок 12. Координатор осуществляет туннелирование и трансляцию адресов для ViPNet-соединений

Подключение через координатор

Если на границе локальной сети в качестве шлюза установлен ViPNet-координатор, то для клиентов, находящихся в локальной сети, рекомендуется выбрать этот координатор в качестве межсетевого экрана.

Внимание! Для правильной работы данного типа подключения необходимо, чтобы между клиентом и координатором не было никаких устройств, осуществляющих трансляцию адресов (NAT).

Если клиент использует в качестве межсетевого экрана координатор, то зашифрованный трафик между этим клиентом и узлами, которые недоступны напрямую по их адресам, будет перенаправляться через координатор. В этом случае координатор играет роль маршрутизатора зашифрованных IP-пакетов с функцией трансляции адресов (осуществляется преобразование IP- и MAC-адресов).

Автоматическая маршрутизация зашифрованных IP-пакетов, отправляемых клиентом, через координатор осуществляется без изменения настроек протокола TCP/IP в операционной системе. Настройки сетевого шлюза, используемого по умолчанию, после установки программного обеспечения ViPNet не изменяются. В результате маршрутизация незашифрованных пакетов также остается неизменной, и работа в сети может быть продолжена сразу после установки программного обеспечения ViPNet. Новые маршруты создаются только для зашифрованного IP-трафика.

В качестве межсетевого экрана можно выбрать координатор, не являющийся сервером IP-адресов для данного клиента.

Эта возможность может быть полезна для мобильного пользователя ViPNet, находящегося в чужой локальной сети. Чтобы работать в сети ViPNet в обычном режиме, мобильному пользователю достаточно выбрать в качестве межсетевого экрана координатор, напрямую доступный в этой локальной сети (при наличии связи с этим координатором).

Кроме того, возможность изменить координатор, используемый в качестве межсетевого экрана, обеспечивает своего рода резервирование маршрутизаторов VPN-пакетов. Если заданный координатор недоступен, то можно выбрать в списке другой подходящий координатор и продолжить работу.

Если необходимо защитить трафик отдельного сегмента внутри локальной сети, на границе которой уже установлен координатор, выполняющий функции межсетевого экрана для клиентов этой локальной сети, то на границу такого сегмента может быть установлен второй координатор.

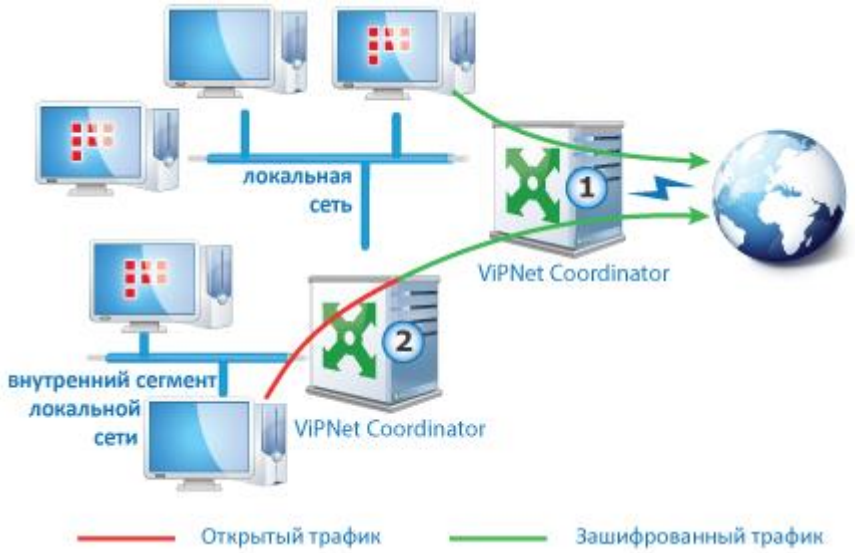

Рисунок 13. Подключение координатора через другой координатор

При этом координатор 1 (см. рисунок выше) должен быть выбран в качестве межсетевого экрана для координатора 2. Между двумя координаторами не должно быть никаких устройств, осуществляющих трансляцию адресов (NAT).

Такое включение координаторов называется каскадным включением. В результате для координаторов будет реализована автоматическая маршрутизация зашифрованного трафика из внутреннего сегмента сети как в локальную, так и в глобальную сеть.

Подключение через межсетевой экран с динамической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT), и на нем затруднительно настроить статические правила трансляции, то для защиты IP-трафика локальной сети, в том числе и при инициативных соединениях снаружи, можно установить координатор с типом межсетевого экрана с динамической трансляцией адресов.

Для клиента данный тип подключения следует выбирать в том случае, если в локальной сети нет координатора, который можно использовать в качестве межсетевого экрана, а соединение с внешней сетью происходит через межсетевой экран, на котором затруднительно настроить статические правила трансляции адресов.

Для правильной работы подключения через межсетевой экран с динамической трансляцией адресов во внешней сети должен существовать координатор, доступный по публичному IP-адресу. Адрес используемого межсетевого экрана должен быть указан в сетевых настройках операционной системы защищенного узла в качестве шлюза по умолчанию.

Подключение через межсетевой экран с динамической трансляцией адресов наиболее универсально и может быть использовано практически в любых ситуациях. Однако основное его

назначение — обеспечить надежное двустороннее соединение с защищенными узлами, подключенными к внешней сети через межсетевые экраны или NAT-устройства, на которых настройка статических правил трансляции адресов затруднена или невозможна (в том числе и просто из-за отсутствия полномочий у пользователя). Такая ситуация типична при использовании простейших сетевых NAT-устройств, например, DSL-модемов, беспроводных точек доступа, а также при использовании общего доступа к подключению Интернет (ICS — Internet Connection Sharing) в операционной системе Windows. Затруднительно также произвести настройку правил трансляции на межсетевых экранах, установленных у провайдера (в домашних сетях, сетях GPRS и других сетях, где провайдер предоставляет частный IP-адрес).

Все NAT-устройства обеспечивают пропускание UDP-трафика благодаря автоматическому созданию так называемых динамических NAT-правил для входящего трафика. Эти правила создаются на основании параметров исходящих пакетов, пропускаемых NAT-устройством.

Например, через NAT-устройство проходит несколько однотипных исходящих пакетов, для них создается динамическое правило. Входящие пакеты, параметры которых соответствуют этому динамическому правилу, пропускаются в течение определенного промежутка времени (таймаута) после прохождения последнего исходящего пакета. По истечении данного промежутка времени динамическое правило удаляется, и NAT-устройство начинает блокировать входящие пакеты.

Это означает, что внешний источник не может инициировать соединение с сетевым узлом, подключенным к внешней сети через NAT-устройство. Внутренний узел должен время от времени передавать исходящий трафик внешнему узлу для сохранения динамического правила в активном состоянии.

Для преодоления этой проблемы на сетевом узле, подключенном к внешней сети через NAT-устройство, нужно настроить подключение через межсетевой экран с динамической трансляцией адресов. Одновременно должен существовать постоянно доступный ViPNet-координатор, расположенный во внешней сети (схема ниже). Назовем его координатором входящих соединений. Координатор входящих соединений должен быть доступен из внешней сети по публичному IP-адресу или через межсетевой экран со статической трансляцией адресов. Координатор входящих соединений не должен работать через тот же межсетевой экран, что и сетевой узел.

Рисунок 14. Подключение через межсетевой экран с динамической трансляцией адресов

Сетевой узел, использующий подключение через межсетевой экран с динамической трансляцией адресов, периодически отправляет на свой координатор входящих соединений UDP-пакеты, чтобы поддерживать динамическое правило в активном состоянии. По умолчанию период отправки — 25 секунд. Это позволяет любому внешнему узлу ViPNet в любое время отправлять IP-пакеты на сетевой узел, работающий через NAT-устройство, через координатор входящих соединений. При этом ответные исходящие пакеты сетевой узел всегда направляет внешнему узлу напрямую, минуя свой координатор входящих соединений (если внешний узел ViPNet не использует межсетевой экран с динамической трансляцией адресов). После получения первого пакета внешний узел, не использующий межсетевой экран с динамической трансляцией адресов, также начинает передавать весь трафик напрямую на сетевой узел, работающий через NAT-устройство. Таким образом, образуется прямой обмен UDP-трафиком между узлами ViPNet.

Такая технология позволяет осуществлять постоянный доступ к ViPNet-узлам, работающим через NAT-устройства (так как динамические правила на NAT-устройстве не удаляются). Кроме того, обеспечивается высокая скорость обмена шифрованным трафиком, так как этот обмен использует координаторы входящих соединений только при инициализации, после чего весь обмен трафиком идет напрямую между узлами (схема выше). Следует учитывать, что исходящий трафик от сетевого узла, использующего подключение через межсетевой экран с динамической трансляцией адресов, на другой такой же узел всегда идет через координатор входящих соединений другого узла.

Подключение через межсетевой экран со статической трансляцией адресов

Если на границе локальной сети с внешней сетью установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT) и позволяющий настроить статические правила трансляции, следует установить координатор между этим межсетевым экраном и узлами локальной сети. На координаторе, который подключен к межсетевому экрану, необходимо настроить параметры подключения через межсетевой экран со статической трансляцией адресов. Для всех ViPNet-клиентов локальной сети необходимо выбрать данный координатор в качестве межсетевого экрана.

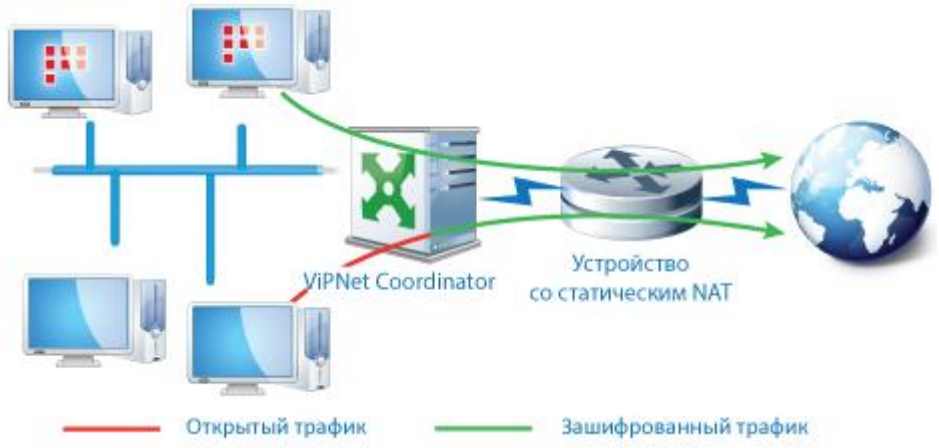

Рисунок 15. Подключение координатора через межсетевой экран со статической трансляцией адресов

На клиенте данный тип подключения следует использовать только в том случае, если в локальной сети нет координатора или невозможно использовать координатор в качестве межсетевого экрана, а соединение с внешней сетью происходит через межсетевой экран, на котором можно настроить статические правила трансляции адресов.

Рисунок 16. Подключение клиента через межсетевой экран со статической трансляцией адресов

Для правильной работы подключения через межсетевой экран **Со статической трансляцией адресов** адрес используемого межсетевого экрана должен быть указан в сетевых настройках операционной системы клиента в качестве шлюза по умолчанию. На межсетевом экране следует настроить статические правила трансляции адресов:

- Пропускать исходящие UDP-пакеты с адресами и портами клиентов, находящихся за межсетевым экраном.
- Пропускать и перенаправлять входящие UDP-пакеты с портом назначения, заданным в настройках клиентов в качестве порта инкапсуляции в UDP-пакеты.

Внимание! Если несколько клиентов используют один и тот же межсетевой экран со статической трансляцией адресов, для каждого клиента должен быть назначен собственный номер порта инкапсуляции в UDP-пакеты. В случае использования

нескольких клиентами одного и того же порта возникают конфликты.

2

Начало работы с программой ViPNet Центр управления сетью

Установка программы ViPNet Центр управления сетью 48

Запуск и завершение работы программы ViPNet Центр управления сетью 49

Интерфейс программы ViPNet Центр управления сетью 54

Создание сети ViPNet: порядок действий 60

Создание структуры сети ViPNet с помощью мастера 62

Загрузка существующей структуры сети из программы версии 3.x 67

Установка программы ViPNet Центр управления сетью

Чтобы развернуть программное обеспечение ViPNet Центр управления сетью, требуется установить два компонента: серверное приложение и клиентское приложение (см. «Архитектура программы ViPNet Центр управления сетью» на стр. 24). Для этого выполните следующие действия:

1. Убедитесь, что вы располагаете установочным комплектом программы ViPNet Центр управления сетью и файлом лицензии на сеть ViPNet (см. «Лицензия на сеть ViPNet» на стр. 23). Выберите схему размещения компонентов программы ViPNet Центр управления сетью.
2. На рабочее место администратора или на специально выделенный сервер установите серверное приложение ViPNet Центр управления сетью. При установке серверного приложения:
   - На компьютер будут автоматически установлены сторонние программы, необходимые для работы серверного приложения (см. «Системные требования» на стр. 15).
   - Будут созданы экземпляр SQL-сервера (если в параметрах подключения не был указан существующий экземпляр) и база данных для хранения структуры и параметров сети ViPNet.

   Также при установке серверного приложения потребуется перезагрузка компьютера.
3. На компьютер, на котором установлено серверное приложение, или на отдельный компьютер установите клиентское приложение ViPNet Центр управления сетью.

   Вместе с клиентским приложением на компьютер будут автоматически установлены сторонние программы, необходимые для его работы (см. «Системные требования» на стр. 15).
4. Если требуется, установите клиентское приложение ViPNet Центр управления сетью на дополнительных рабочих местах администраторов.
5. Установите на компьютер с серверным приложением ViPNet Центр управления сетью программное обеспечение ViPNet Client, которое требуется для отправки обновлений из Центра управления сетью на сетевые узлы ViPNet.

   После создания сети ViPNet (см. «Создание сети ViPNet: порядок действий» на стр. 60) и дистрибутивов ключей для сетевых узлов установите на компьютер с серверным приложением дистрибутив ключей для сетевого узла — Центра управления сетью.
6. При необходимости установите на компьютеры с клиентскими приложениями ViPNet Центр управления сетью программное обеспечение ViPNet Client, настройте подключение клиентских приложений к серверному приложению ЦУСа и создайте дополнительные учетные записи администраторов (см. «Создание учетной записи» на стр. 72).

Подробная информация об установке и первоначальной настройке программы ViPNet Центр управления сетью содержится в документе «ViPNet Administrator. Руководство по установке».

Запуск и завершение работы программы ViPNet Центр управления сетью

Запуск серверного приложения

Серверное приложение ViPNet Центр управления сетью не имеет графического интерфейса и реализовано в виде двух служб:

- `NccService` (процесс `Infotecs.WinNCC.Communication.Hosting.exe`).
- `NccFilewatcherService` (процесс `Infotecs.WinNcc.FileWatcher.Service.exe`).

Службы серверного приложения ViPNet Центр управления сетью запускаются автоматически после загрузки операционной системы. Останавливать эти службы не рекомендуется, иначе управление сетью ViPNet с помощью клиентских приложений будет невозможно.

Если по каким-либо причинам службы серверного приложения были остановлены, запустите их. Для этого выполните следующие действия:

1. Запустите «Диспетчер задач Windows» с помощью сочетания клавиш **Ctrl+Shift+Esc**.
2. В окне **Диспетчер задач Windows** перейдите на вкладку **Службы**.
3. В списке найдите службу `NccService`, щелкните эту службу правой кнопкой мыши и в контекстном меню выберите пункт **Запустить службу**.
4. Таким же образом запустите службу `NccFilewatcherService`.

Запуск и завершение работы клиентского приложения

Чтобы запустить клиентское приложение ViPNet Центр управления сетью:

1. Выполните одно из действий:
   - Если вы используете операционную систему Windows 7 или Windows Server 2008 R2, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Administrator** > **Центр управления сетью**.
   - Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите **ViPNet** > **Центр управления сетью**.

Примечание. Во время установки положение программы в меню **Пуск** или в списке приложений могло быть изменено.

При этом клиентское приложение автоматически подключается к серверному приложению. Если вы запускаете клиентское приложение ViPNet Центр управления сетью впервые, следуйте инструкциям раздела Первый запуск клиентского приложения (на стр. 51).

2 Подключение клиентского приложения к серверному выполняется по адресу, который использовался в предыдущем сеансе работы. Если клиентское и серверное приложения установлены на разных компьютерах, и сервер недоступен по заданному ранее адресу, появится соответствующее сообщение.

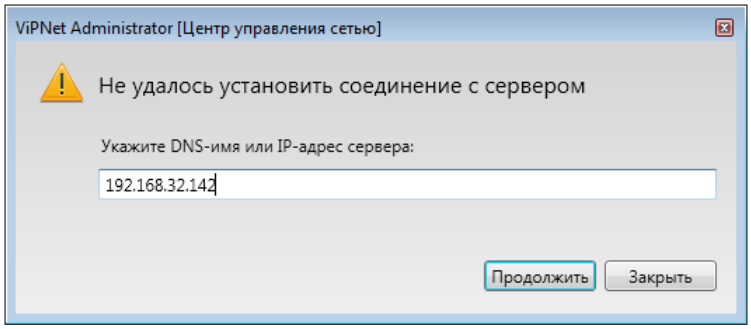

Рисунок 17. Сообщение при отсутствии соединения с SQL-сервером

В окне сообщения введите IP-адрес или DNS-имя компьютера, на котором установлено серверное приложение ViPNet Центр управления сетью, и нажмите кнопку **Продолжить**.

3 В открывшемся окне введите имя и пароль администратора и нажмите кнопку **Продолжить**.

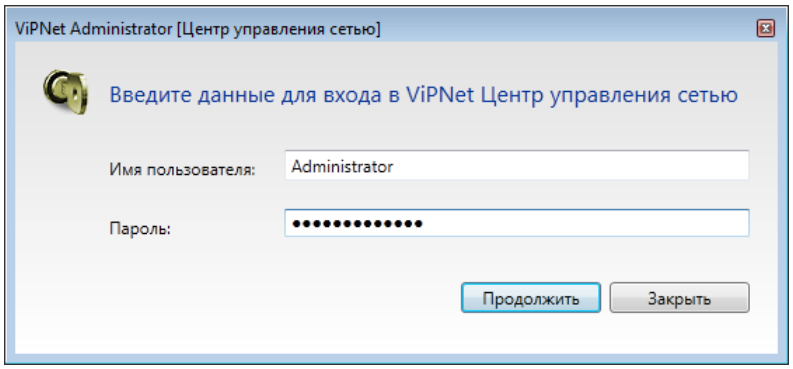

Рисунок 18. Ввод данных администратора для входа в программу ViPNet Центр управления сетью

Откроется главное окно программы (см. «Интерфейс программы ViPNet Центр управления сетью» на стр. 54).

Чтобы завершить работу с клиентским приложением ViPNet Центр управления сетью, выполните одно из действий:

- В меню **Моя сеть** выберите пункт **Выход**.
- Нажмите сочетание клавиш **Alt+F4**.

- Нажмите кнопку **Закрыть** в правом верхнем углу окна **ViPNet Центр управления сетью**.

Первый запуск клиентского приложения

Для управления структурой и параметрами сети ViPNet начните работу с клиентским приложением ViPNet Центр управления сетью:

1 Запустите клиентское приложение (см. «Запуск и завершение работы клиентского приложения» на стр. 49).

2 Для подключения клиентского приложения к серверному по умолчанию используется адрес локального компьютера. Если клиентское и серверное приложения установлены на разных компьютерах, появится сообщение об отсутствии соединения с сервером (см. рисунок на стр. 50). В окне сообщения введите IP-адрес или DNS-имя компьютера, на котором установлено серверное приложение ViPNet Центр управления сетью, и нажмите кнопку **Продолжить**.

3 В окне входа в программу ViPNet Центр управления сетью введите имя пользователя `Administrator` и пароль `Administrator` (см. рисунок на стр. 50). Затем нажмите кнопку **Продолжить**.

4 В целях безопасности требуется сменить пароль выбранной учетной записи. В окне **Начало работы с ViPNet Центр управления сетью** введите текущий пароль, затем задайте новый пароль и подтвердите его.

Пароль должен содержать не менее восьми символов.

Совет. Рекомендуется задавать сложные пароли, содержащие не менее восьми символов, в состав которых входят буквы в разных регистрах, цифры и специальные символы.

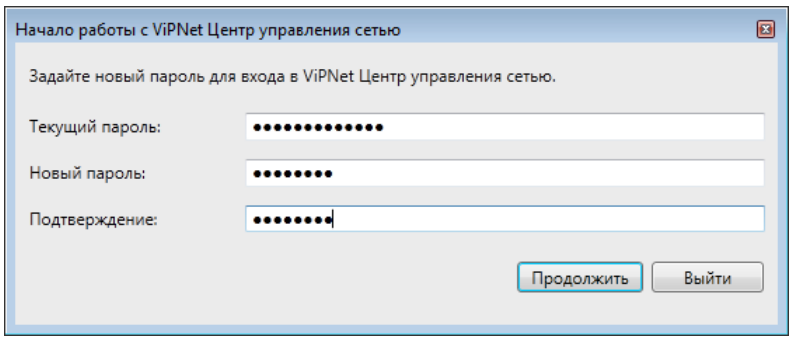

Рисунок 19. Смена пароля администратора ViPNet Центр управления сетью

Чтобы сохранить новый пароль, нажмите кнопку **Продолжить**.

5 В открывшемся окне с помощью кнопки **Обзор** укажите путь к файлу лицензии на сеть ViPNet `*.itcslic` или `infotecs.reg` и нажмите кнопку **Продолжить**.

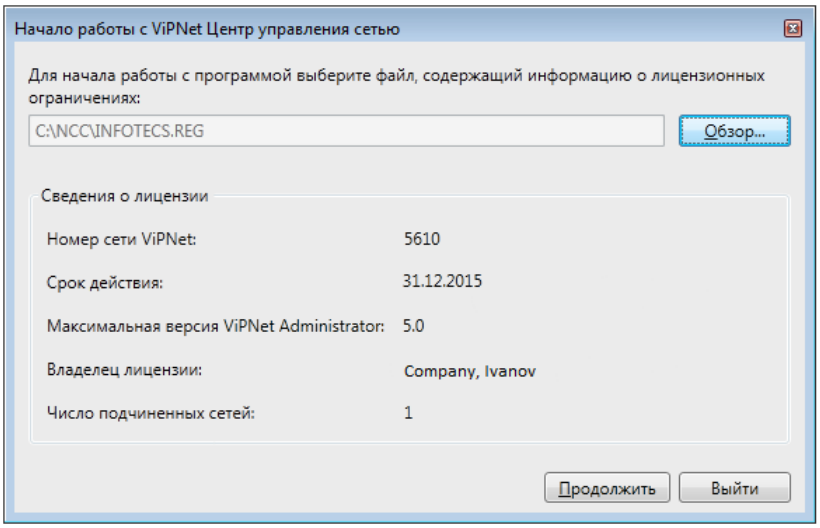

Рисунок 20. Указание пути к файлу лицензии

6 В открывшемся окне выберите один из следующих вариантов:

- **Сформировать структуру защищенной сети автоматически** — для создания сети ViPNet с помощью мастера (см. «Создание структуры сети ViPNet с помощью мастера» на стр. 62).
- **Загрузить структуру существующей сети** — если ранее в вашей сети использовалось программное обеспечение ViPNet Administrator версии 3.x, и вы хотите импортировать данные о существующей сети ViPNet (см. «Загрузка существующей структуры сети из программы версии 3.x» на стр. 67).
- **Настроить структуру защищенной сети самостоятельно** — чтобы создать сетевые объекты и настроить их вручную.

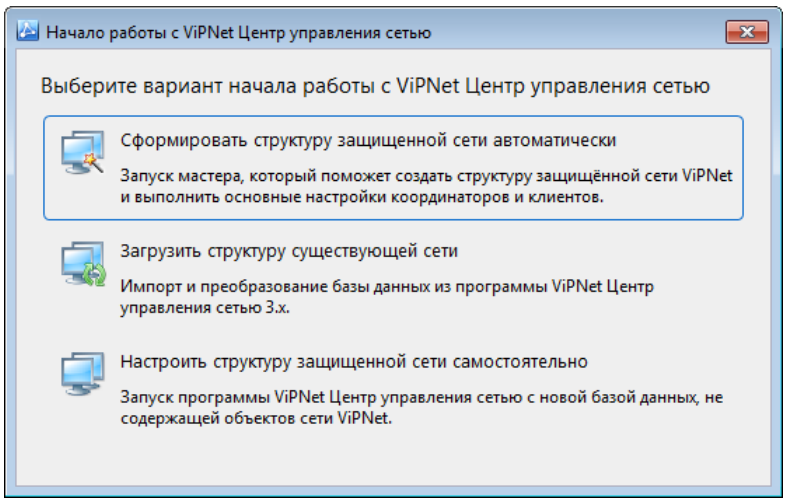

Рисунок 21. Выбор действия для начала работы с программой ViPNet Центр управления сетью

7 Если ваша лицензия на сеть ViPNet предполагает создание иерархии сетей, появится сообщение с предложением распределить лицензионные ограничения между сетями.

В окне сообщения нажмите кнопку **Распределить лицензию** и в окне **Распределение лицензий** задайте лицензионные ограничения для своей сети (см. «Распределение общей лицензии между сетями» на стр. 225).

Примечание. Если вы выбрали загрузку существующей структуры сети, информация о распределении лицензионных ограничений будет загружена автоматически.

Интерфейс программы ViPNet Центр управления сетью

Внешний вид окна программы ViPNet Центр управления сетью представлен на следующем рисунке:

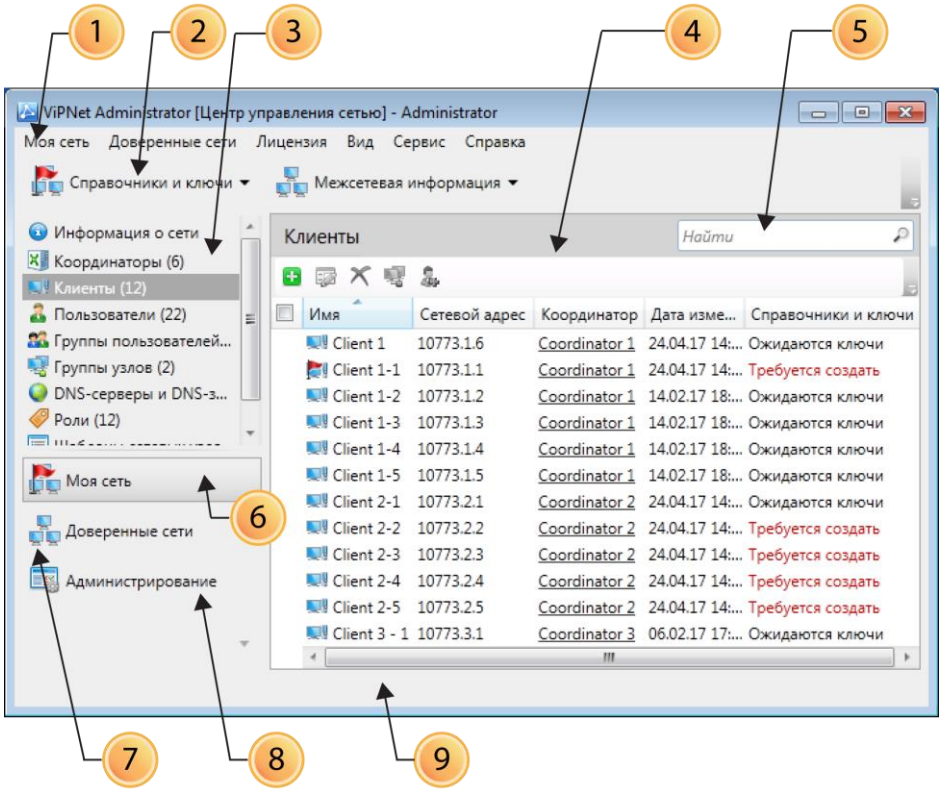

Рисунок 22. Интерфейс программы ViPNet Центр управления сетью

Цифрами на рисунке обозначены:

1. Главное меню программы.
2. Панель инструментов. Чтобы скрыть или отобразить панель инструментов, в меню **Вид** выберите пункт **Панель инструментов**.
3. Панель навигации, на которой отображаются разделы выбранного представления.
4. Панель просмотра, на которой отображается список элементов выбранного раздела и панель инструментов для работы с этими элементами. Флажок, расположенный в заголовке списка, позволяет выбрать или отменить выбор сразу всех элементов списка.
5. Поле поиска, которое позволяет найти объект сети по его имени. Для поиска по маске вы можете использовать следующие специальные символы подстановки:
   - Знак процента % — заменяет любую последовательность символов.

- Квадратные скобки `[<a-z>]` — заменяет любой один символ из указанного диапазона `<a-z>`.
- Знак карета в квадратных скобках перед диапазоном символов `[^<a-z>]` — заменяет любой один символ, который не лежит в указанном диапазоне символов, где `<a-z>` — диапазон символов.

6 Представление **Моя сеть**. При выборе представления **Моя сеть** на панели навигации отображается список объектов своей сети ViPNet (см. «Представление „Моя сеть“» на стр. 55).

7 Представление **Доверенные сети**. При выборе представления **Доверенные сети** на панели навигации отображается список доверенных сетей и их объектов, участвующих в межсетевом взаимодействии (см. «Представление „Доверенные сети“» на стр. 56).

8 Представление **Администрирование**. При выборе представления **Администрирование** на панели навигации отображаются разделы для управления учетными записями администраторов и для просмотра журналов программы (см. «Представление „Администрирование“» на стр. 58).

Примечание. По умолчанию кнопка представления **Администрирование** отображается в виде значка без подписи. Чтобы эта кнопка отображалась также, как кнопки представлений **Моя сеть** и **Доверенные сети**, нажмите кнопку и выберите пункт **Показать дополнительную кнопку**.

---

9 Строка состояния. Чтобы скрыть или отобразить строку состояния, в меню **Вид** выберите пункт **Строка состояния**.

Представление «Моя сеть»

Чтобы получить сведения о вашей сети ViPNet, выберите представление **Моя сеть.** На панели навигации будут отображены разделы, содержащие общую информацию о сети ViPNet, об объектах сети и ролях узлов.

Для просмотра номера и имени вашей сети, данных о количестве созданных объектов и используемых ролях на панели навигации выберите раздел **Информация о сети**.

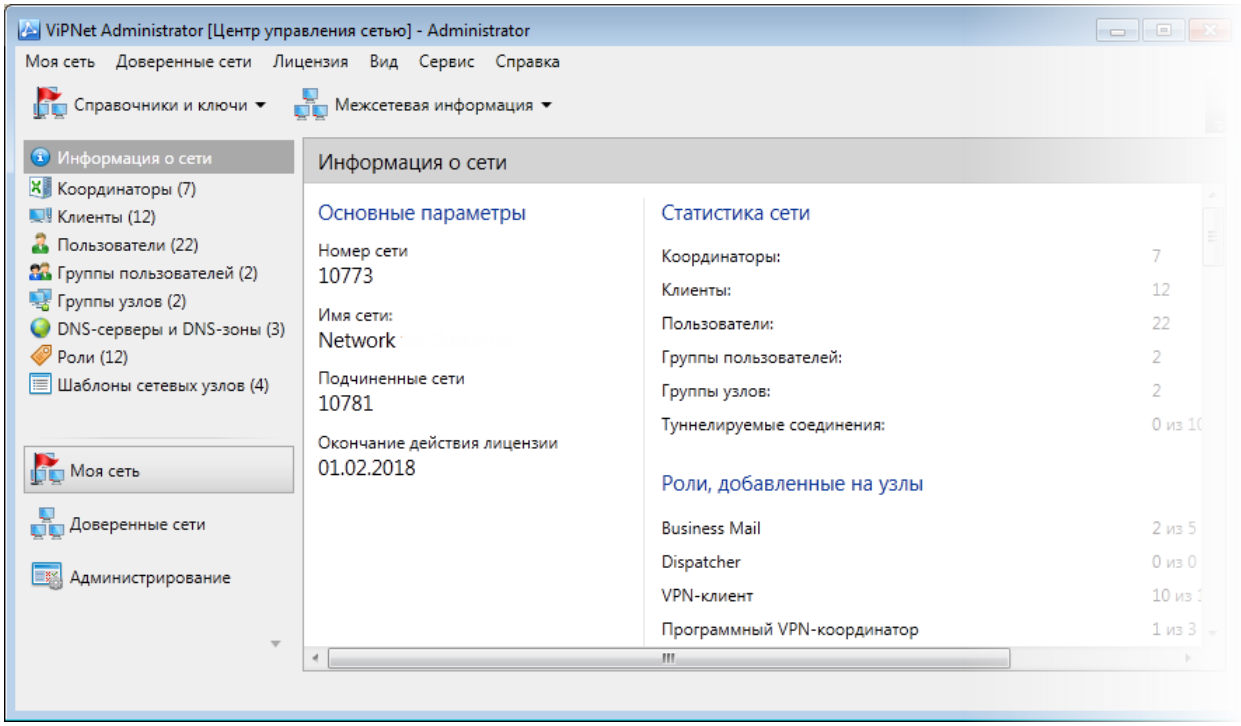

Рисунок 23. Общая информация о своей сети

При выборе на панели навигации одного из разделов, которые соответствуют объектам сети, на панели просмотра будут представлены:

- Панель инструментов для работы с элементами выбранного раздела и строка поиска.
- Список элементов выбранного раздела и их свойств в виде таблицы.

  Для сортировки списка по нужному параметру щелкните заголовок соответствующего столбца.

  Для добавления или удаления столбца щелкните правой кнопкой мыши заголовок любого столбца и в меню выберите нужный параметр.

  Чтобы просмотреть свойства объекта вашей сети ViPNet, щелкните этот объект правой кнопкой мыши и в контекстном меню выберите пункт **Свойства**. Подробное описание свойств объектов сети приведено в разделах Настройка параметров сетевых узлов (на стр. 111) и Настройка параметров пользователей (на стр. 202).

Представление «Доверенные сети»

Чтобы получить сведения о сетях ViPNet, с которыми установлено межсетевое взаимодействие (на стр. 232), выберите представление **Доверенные сети**. На панели навигации будут отображены разделы, содержащие информацию о доверенных сетях и их объектах.

Для просмотра списка всех доверенных сетей и их основных свойств на панели навигации выберите раздел **Свойства сетей**. На панели просмотра будут представлены:

- Панель инструментов для работы с доверенными сетями.

- Список доверенных сетей, с которыми установлено межсетевое взаимодействие, и их параметров в виде таблицы.

  Если ваша сеть является частью иерархической системы сетей ViPNet (см. «Иерархическая система сетей ViPNet» на стр. 220), в списке доверенных сетей всегда присутствуют следующие типы сетей:

  - Главная сеть (обозначается значком) — в Центре управления сетью подчиненной сети.
  - Подчиненные сети (обозначаются значком) — в Центре управления сетью главной сети.

  Для сортировки списка по нужному параметру щелкните заголовок соответствующего столбца.

  Для добавления или удаления столбца щелкните правой кнопкой мыши заголовок любого столбца и в меню выберите нужный параметр.

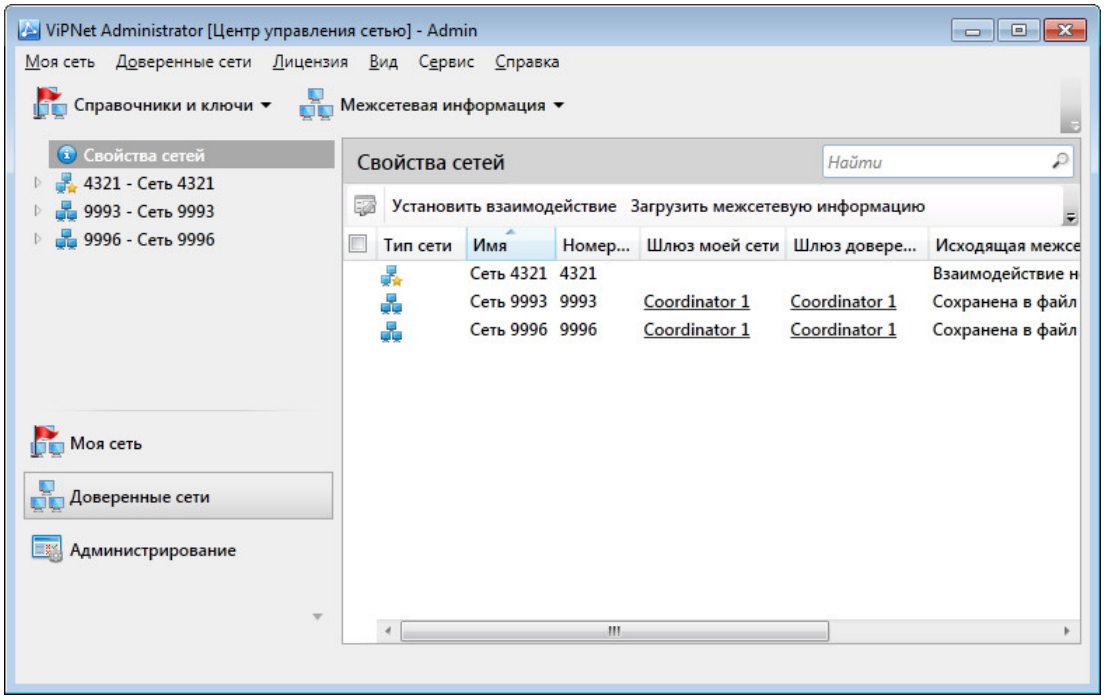

Рисунок 24. Информация о доверенных сетях

При выборе на панели навигации раздела, соответствующего одной из доверенных сетей, на панели просмотра будет представлена следующая информация:

- номер и имя выбранной доверенной сети;
- состояние входящей и исходящей межсетевой информации;
- имена шлюзовых координаторов своей сети и выбранной доверенной сети;
- количество объектов своей сети и выбранной доверенной сети, которые участвуют в межсетевом взаимодействии.

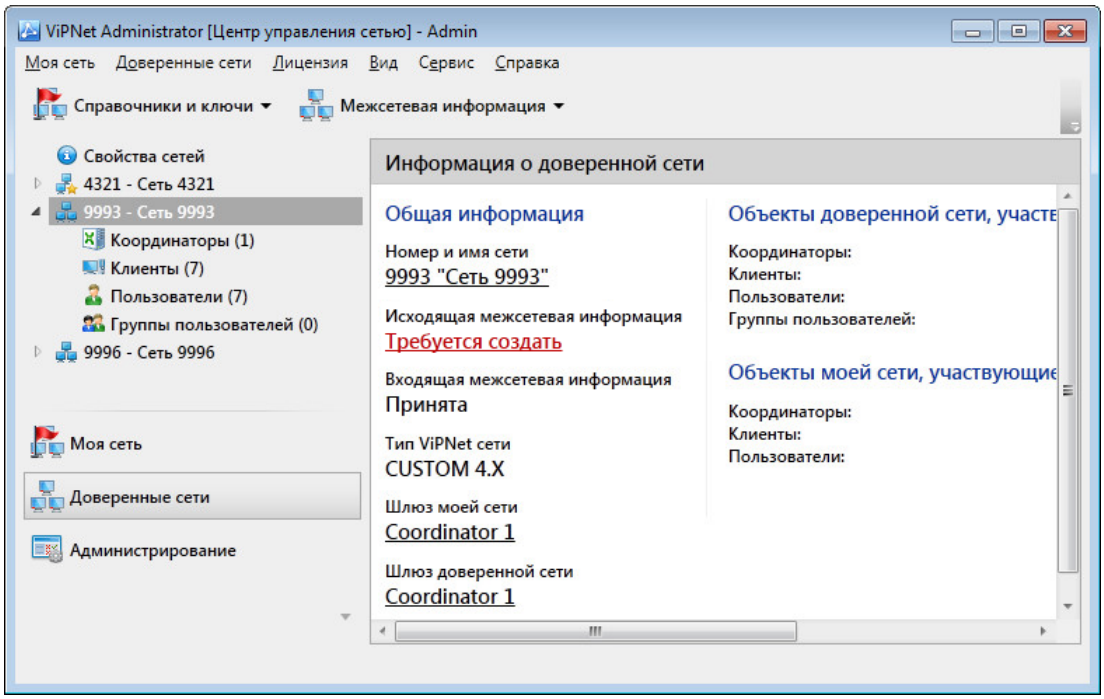

Рисунок 25. Доверенная сеть

С помощью ссылок на панели просмотра вы можете создать или отправить исходящую межсетевую информацию либо обработать входящую межсетевую информацию.

Представление «Администрирование»

Для управления учетными записями администраторов и просмотра журналов программы ViPNet Центр управления сетью выберите представление **Администрирование**.

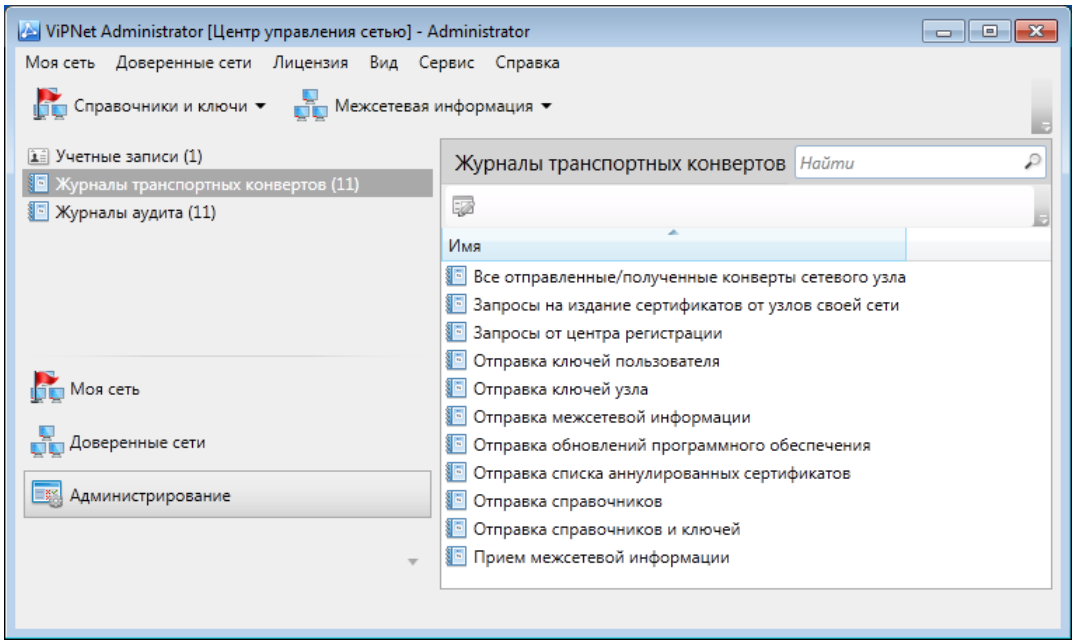

Рисунок 26. Управление учетными записями администраторов

На панели навигации будут отображены следующие разделы:

- **Учетные записи** (см. «Управление учетными записями администраторов» на стр. 72). В этом разделе вы можете создавать и удалять учетные записи администраторов программы ViPNet Центр управления сетью.
- **Журналы транспортных конвертов** (на стр. 102). В этом разделе вы можете просмотреть историю обмена служебными конвертами с сетевыми узлами ViPNet.
- **Журналы аудита** (на стр. 100). В этом разделе вы можете просмотреть журналы системных событий программы ViPNet Центр управления сетью.

Создание сети ViPNet: порядок действий

Чтобы создать и настроить работоспособную сеть ViPNet с помощью программы ViPNet Центр управления сетью, выполните действия из приведенного ниже списка.

Таблица 3. Последовательность действий при создании сети ViPNet

	Действие	Ссылка
☐	Спланируйте структуру будущей сети ViPNet, определите необходимое количество сетевых объектов и связей между ними, выберите программное обеспечение для установки на сетевых узлах.	См. документ «Развертывание сети ViPNet. Руководство администратора»
☐	Убедитесь, что лицензионные ограничения позволяют создать требуемую структуру сети. Если ваша лицензия поддерживает иерархию сетей ViPNet, при необходимости перераспределите лицензионные ограничения.	Просмотр сведений о лицензии для своей сети (на стр. 106) Распределение общей лицензии между сетями (на стр. 225)
☐	Создайте структуру сети ViPNet с помощью мастера	Создание структуры сети ViPNet с помощью мастера (на стр. 62)
☐	При необходимости измените связи между сетевыми узлами и пользователями	Изменение связей между сетевыми узлами (на стр. 138) Изменение связей между пользователями (на стр. 207)
☐	При необходимости добавьте на сетевые узлы роли и задайте свойства ролей	Добавление ролей на сетевые узлы (на стр. 142)
☐	При необходимости настройте туннелирование открытых узлов координаторами	Настройка туннелирования (на стр. 123)
☐	При необходимости добавьте на сетевые узлы дополнительных пользователей	Добавление пользователя (на стр. 204)
☐	Укажите IP-адреса или DNS-имена координаторов	Задание адресов сетевого узла (на стр. 175)
☐	Задайте параметры подключения сетевых узлов к внешней сети	Настройка параметров подключения к внешней сети (на стр. 178)
☐	Создайте справочники, которые необходимы для создания дистрибутивов ключей (см. глоссарий, стр. 302) в программе ViPNet Удостоверяющий и ключевой центр	Создание справочников (на стр. 88)

Примечание. Некоторые действия из списка не являются обязательными. Необходимость выполнения этих действий зависит от требований, которые предъявляются к создаваемой сети ViPNet, и лицензионных ограничений.

После того как в программе ViPNet Центр управления сетью будут созданы справочники, в программе ViPNet Удостоверяющий и ключевой центр создайте дистрибутивы ключей для сетевых узлов. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

На компьютерах, которые должны быть включены в сеть ViPNet, установите выбранное программное обеспечение ViPNet. Затем на эти компьютеры установите созданные в Удостоверяющем и ключевом центре дистрибутивы ключей. При этом дистрибутив ключей для сетевого узла — Центра управления сетью должен быть установлен на компьютер, на который установлено серверное приложение ViPNet Центр управления сетью.

Создание структуры сети ViPNet с помощью мастера

Если при первом запуске программы ViPNet Центр управления сетью в окне **Начало работы с ViPNet Центр управления сетью** (см. рисунок на стр. 52) был выбран вариант **Сформировать структуру защищенной сети автоматически**, будет запущен мастер **Создание сети ViPNet**, с помощью которого можно сформировать структуру сети и настроить ее основные параметры.

В случае необходимости мастер **Создание сети ViPNet** можно запустить из главного окна программы ViPNet Центр управления сетью. Для этого в меню **Моя сеть** выберите пункт **Создать сеть ViPNet**.

Внимание! Если в программе ViPNet Центр управления сетью уже существует структура сети ViPNet, в результате работы мастера она будет удалена и заменена новой структурой.

Для создания сети ViPNet с помощью мастера выполните следующие действия:

1. На первой странице мастера **Создание защищенной сети ViPNet** нажмите кнопку **Далее**.
2. На странице **Координаторы защищенной сети ViPNet** выполните следующие действия:
   - В соответствующем поле укажите желаемое количество координаторов в сети ViPNet.
   - В поле **Формат имени координаторов** введите маску имени для создаваемых координаторов.
   - Задайте роли (см. «Роли сетевых узлов» на стр. 31), которые будут добавлены на координаторы при их создании, установив для этого соответствующие флажки. По умолчанию выбраны роли «Программный VPN-координатор», «Обмен сообщениями и файлами».

Примечание. При добавлении роли с помощью мастера вы не можете выбрать дополнительные ограничения по версии и периоду использования соответствующего программного обеспечения. Версии и период использования устанавливаемых программ в этом случае определяются общими ограничениями, заданными в лицензии для узлов сети ViPNet.

Если вашей лицензией на сеть ViPNet для ролей предусмотрены дополнительные ограничения, вы можете управлять ими после создания структуры сети ViPNet (см. «Изменение списка ролей сетевого узла» на стр. 142).

Если выбрано добавление ролей «Программный VPN-координатор» или «CryptoService», вы можете изменить для этих ролей уровень полномочий пользователя. Для этого щелкните ссылку **параметры** (для роли «Программный VPN-координатор») или **максимальные полномочия** (для роли «CryptoService») и задайте нужный уровень

полномочий пользователей (см. «Изменение уровня полномочий пользователя» на стр. 146).

Если выбрано добавление роли «Обмен сообщениями и файлами», щелкните ссылку **параметры** и задайте параметры этой роли (см. «Настройка параметров роли „Обмен сообщениями и файлами“» на стр. 147). По умолчанию разрешен и файловый обмен, и обмен сообщениями.

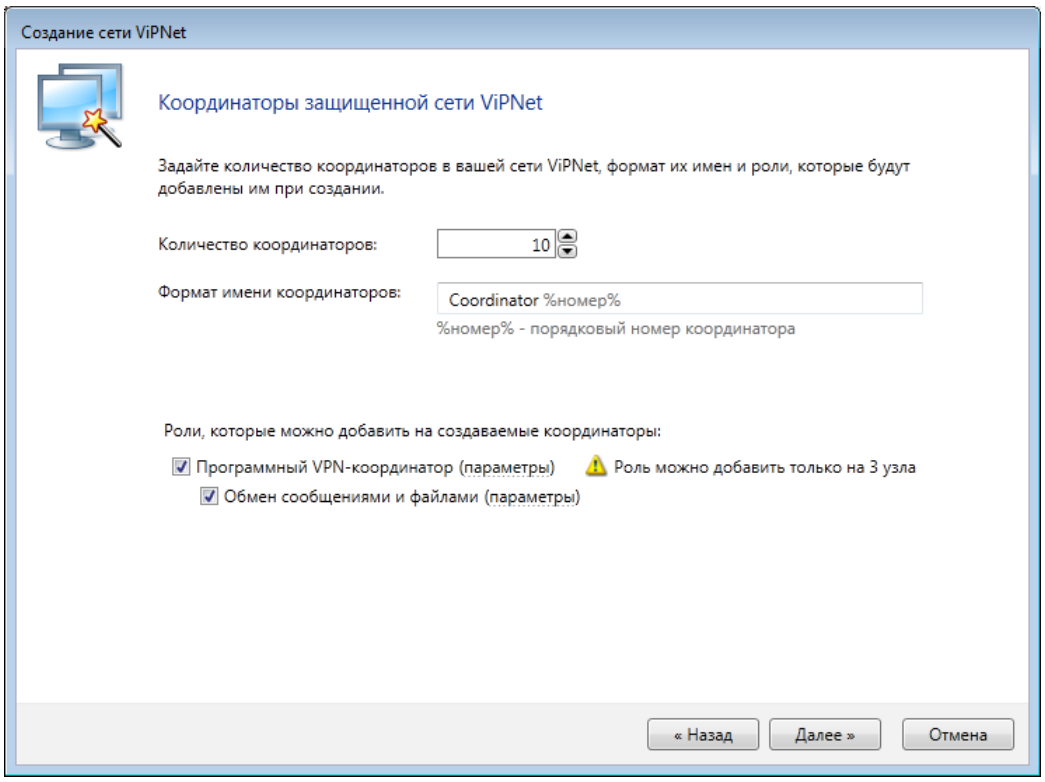

Рисунок 27. Задание координаторов при создании сети ViPNet

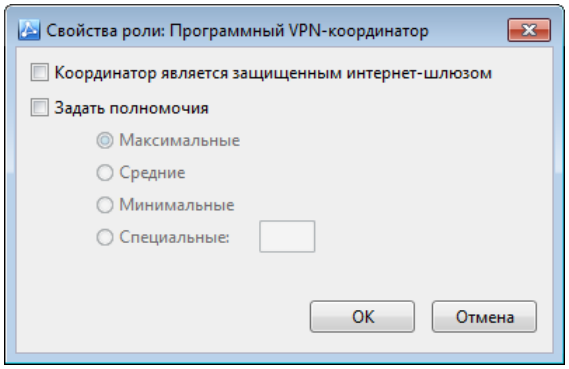

Рисунок 28. Задание параметров роли «Программный VPN-координатор»

После задания количества координаторов и их параметров нажмите кнопку **Далее**.

3 На странице **Клиенты защищенной сети ViPNet** выполните следующие действия:

- В соответствующем поле укажите количество клиентов, которые должны быть зарегистрированы на каждом координаторе.
- В поле **Формат имени клиентов** введите маску имени для создаваемых клиентов.

- Задайте роли (см. «Роли сетевых узлов» на стр. 31), которые будут добавлены на клиенты при их создании, установив для этого соответствующие флажки. По умолчанию выбраны роли «VPN-клиент» и «Business Mail».

  Если выбрано добавление ролей «VPN-клиент», «Business Mail» или «CryptoService», установите для выбранных ролей уровень полномочий пользователей (см. «Изменение уровня полномочий пользователя» на стр. 146). По умолчанию для всех ролей установлены максимальные полномочия.

  Если выбрано добавление роли «Обмен сообщениями и файлами», задайте параметры этой роли (см. «Настройка параметров роли „Обмен сообщениями и файлами“» на стр. 147). По умолчанию разрешен и файловый обмен, и обмен сообщениями.

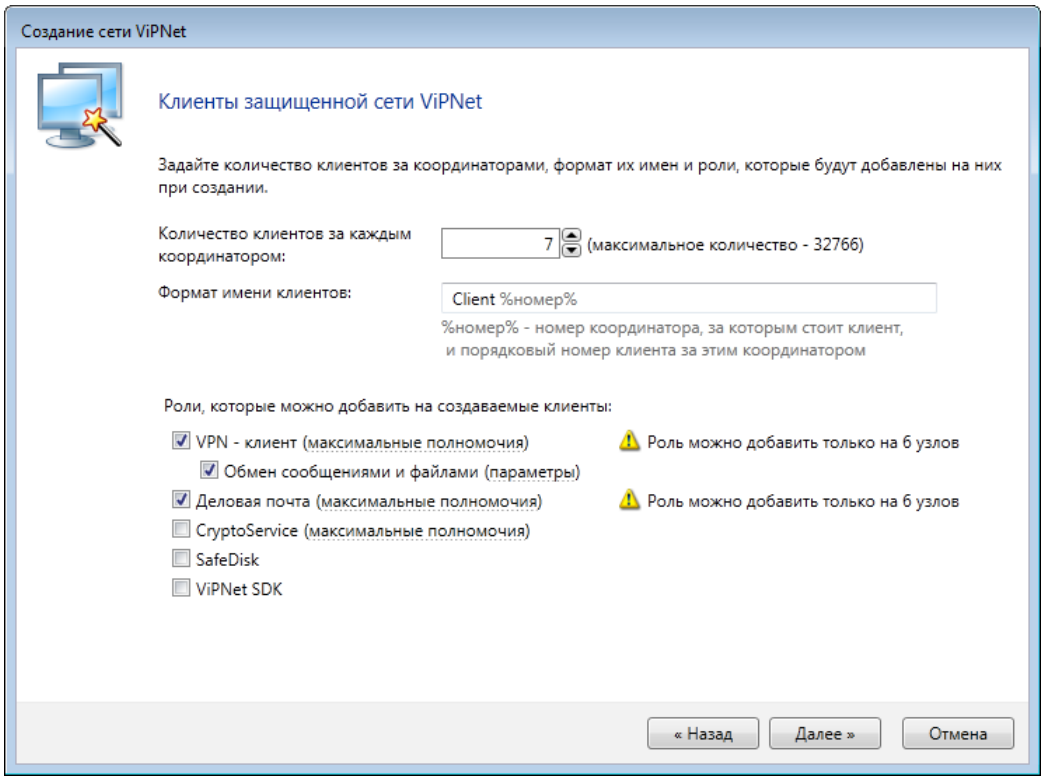

Рисунок 29. Задание клиентов при создании сети ViPNet

После задания количества клиентов и их параметров нажмите кнопку **Далее**.

4 На странице **Связи между объектами защищенной сети ViPNet** с помощью переключателя установите нужный тип связи между защищенными узлами (см. глоссарий, стр. 302). По умолчанию выбран вариант **Связать все сетевые узлы**.

Независимо от выбранного типа связей, между всеми координаторами будут образованы межсерверные каналы. Каждый клиент будет связан со своим координатором, и каждый сетевой узел будет связан с Центром управления сетью. На каждый созданный узел будет добавлен один пользователь, имя которого совпадает с именем сетевого узла.

Рекомендуется задать связи между пользователями связанных сетевых узлов, для этого установите соответствующий флажок. Данная связь необходима, чтобы пользователи могли вести конфиденциальную переписку друг с другом в программе ViPNet Деловая почта.

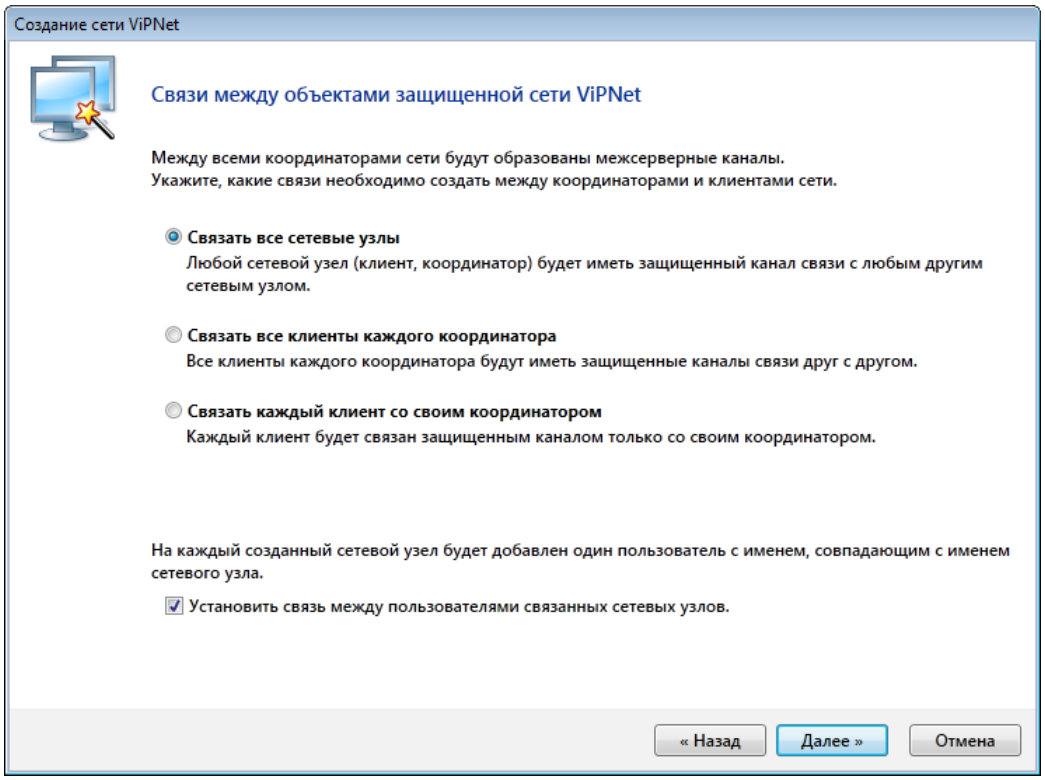

Рисунок 30. Задание связей между объектами создаваемой сети

Нажмите кнопку **Далее**.

5 На странице **Подготовка к созданию сети ViPNet завершена** убедитесь в правильности параметров создаваемой сети, заданных на предыдущих страницах мастера.

Если вы хотите, чтобы по окончании работы мастера были автоматически созданы справочники, установите соответствующий флажок.

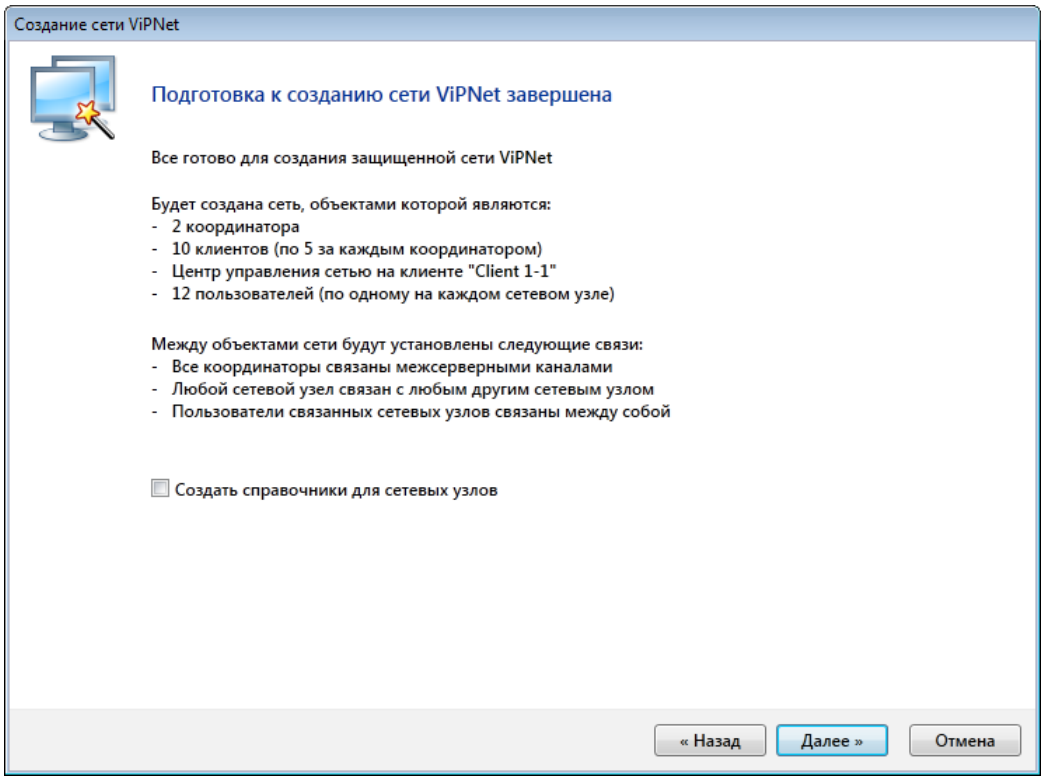

Рисунок 31. Завершение подготовки к созданию сети ViPNet

Нажмите кнопку **Далее**.

6 Появится окно **Создание сети ViPNet** с предупреждением о том, что сеть ViPNet будет создана заново. Установите флажок **Удалить структуру ранее созданной сети** и нажмите кнопку **Создать сеть**.

7 После того как процесс создания сети будет завершен, на странице **Создание защищенной сети ViPNet** нажмите кнопку **Далее**.

8 На странице **Защищенная сеть ViPNet создана** нажмите кнопку **Готово**, чтобы завершить работу мастера.

В результате будет создана следующая структура сети ViPNet:

- На каждом сетевом узле будет создано по одному пользователю.
- Первый созданный клиент будет зарегистрирован как Центр управления сетью.
- Между сетевыми узлами будут образованы связи, тип которых был указан при установке.

После того как в мастере сформирована первичная структура защищенной сети, можно приступать к настройке параметров сетевых узлов и пользователей. Подробнее см. разделы Настройка параметров координатора (на стр. 118), Настройка параметров клиента (на стр. 128), Создание пользователя и настройка его параметров (на стр. 203).

После создания структуры сети в программе ViPNet Центр управления сетью создайте справочники (см. «Создание справочников» на стр. 88). Далее в программе ViPNet Удостоверяющий и ключевой центр создайте дистрибутивы ключей для сетевых узлов и передайте их доверенным способом пользователям для установки на сетевых узлах ViPNet (подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора»).

Загрузка существующей структуры сети из программы версии 3.x

Если ранее для управления вашей сетью ViPNet использовалось программное обеспечение ViPNet Administrator версии 3.x и вы хотите перейти на версию 4.x, то для продолжения работы с существующей структурой сети необходимо загрузить данные из предыдущей версии программы ViPNet Центр управления сетью.

Для загрузки данных о структуре сети из программы ViPNet Administrator версии 3.x выполните следующие действия:

1. Убедитесь, что у вас имеется копия папки `\NCC`, которая находится в папке установки программы ViPNet Administrator 3.x. Эта папка содержит данные о структуре и параметрах сети ViPNet.
2. Запустите мастер конвертации данных Центра управления сетью. Для этого выполните одно из действий:
   - При первом запуске программы ViPNet Центр управления сетью 4.x в окне **Начало работы с ViPNet Центр управления сетью** (см. рисунок на стр. 52) выберите **Загрузить структуру существующей сети**.
   - В окне программы ViPNet Центр управления сетью в меню **Моя сеть** выберите пункт **Загрузить структуру сети ViPNet**.
3. В окне **Конвертация базы данных Центра управления сетью 3.x** в группе **Подключение к базе данных Центра управления сетью 3.x** укажите путь к папке `\NCC`, содержащей данные программы ViPNet Центр управления сетью 3.x.

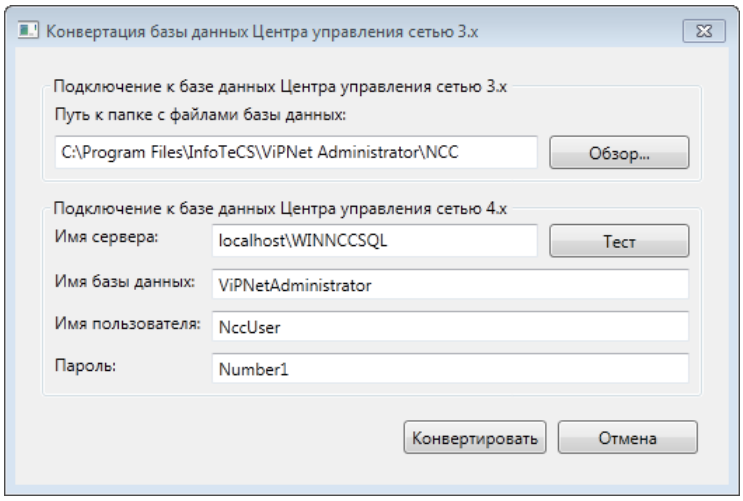

Рисунок 32. Настройка параметров конвертации базы данных программы ViPNet Центр управления сетью 3.2.x

В остальных полях сохраните значения по умолчанию.

4. Нажмите кнопку **Конвертировать**, начнется процесс конвертации данных.

В окне **Конвертация базы данных Центра управления сетью 3.x** будет выводиться отчет о выполняемых операциях.

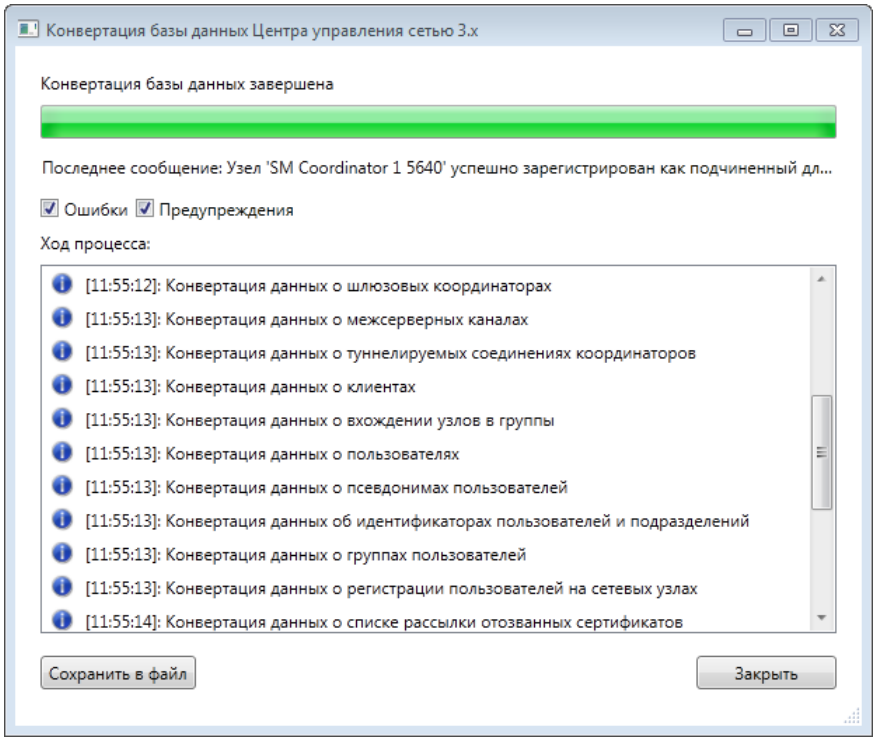

Рисунок 33. Просмотр информации и процессе конвертации

5 По завершении конвертации в окне **Конвертация базы данных Центра управления сетью 3.x** нажмите кнопку **Закрыть**.

В результате данные о структуре сети ViPNet и ее параметрах будут преобразованы и записаны в базу данных SQL. В программе ViPNet Центр управления сетью можно будет продолжить работу с существующей сетью ViPNet.

Подробная информация о конвертации данных программы ViPNet Центр управления сетью 3.x содержится в документе «ViPNet Administrator. Руководство по обновлению с версии 3.2.x на версию 4.x».

3

Управление сетью ViPNet

Основные возможности программы ViPNet Центр управления сетью 70

Управление учетными записями администраторов 72

Настройка параметров программы по умолчанию 75

Проверка конфигурации сети 83

Создание отчета о структуре сети 85

Отправка обновлений на сетевые узлы 87

Резервное копирование и восстановление данных 99

Просмотр журналов 100

Работа с лицензией 106

Основные возможности программы ViPNet Центр управления сетью

Основные функции программы ViPNet Центр управления сетью, которые вы можете использовать для управления вашей сетью, перечислены в следующей таблице. Функции разбиты на три категории: управление своей сетью ViPNet, взаимодействие с другими сетями ViPNet, административные функции программы.

Таблица 4. Основные возможности программы ViPNet Центр управления сетью

Категория	Функция	Ссылка
Управление своей сетью ViPNet	Создание новой сети ViPNet	Создание структуры сети ViPNet с помощью мастера (на стр. 62)
	Добавление и удаление сетевых узлов настройка их свойств	Настройка параметров сетевых узлов (на стр. 111)
	Добавление, удаление и настройка свойств пользователей	Настройка параметров пользователей (на стр. 202)
	Отправка на сетевые узлы обновлений справочников и ключей	Отправка справочников и ключей (на стр. 91)
	Отправка на сетевые узлы обновлений программного обеспечения ViPNet	Обновление программного обеспечения (на стр. 94)
Взаимодействие с другими сетями ViPNet	Организация межсетевого взаимодействия с другими сетями ViPNet	Организация межсетевого взаимодействия (на стр. 233)
	Изменение связей между объектами своей сети и объектами доверенных сетей ViPNet	Изменение связей с объектами доверенной сети (на стр. 245)
	Обмен информацией об изменении параметров межсетевого взаимодействия с администраторами доверенных сетей ViPNet	Отправка межсетевой информации (на стр. 251)
	Распределение лицензионных ограничений для подчиненных сетей при наличии лицензии, которая предполагает создание иерархической системы сетей ViPNet	Распределение общей лицензии между сетями (на стр. 225)
	Создание и удаление учетных записей администраторов программы ViPNet Центр управления сетью	Управление учетными записями администраторов (на стр. 72)

Административные функции	Просмотр журналов аудита системных событий программы ViPNet Центр управления сетью	Журналы аудита (на стр. 100)
	Просмотр журналов обмена транспортными конвертами между Центром управления сетью и сетевыми узлами ViPNet	Журналы транспортных конвертов (на стр. 102)
	Резервное копирование и восстановление данных программы ViPNet Центр управления сетью	Резервное копирование и восстановление данных (на стр. 99)
	Загрузка новой лицензии на сеть ViPNet	Обновление лицензии (на стр. 108)

Управление учетными записями администраторов

Многопользовательская работа в программе

Программа ViPNet Центр управления сетью позволяет создать несколько учетных записей администраторов (см. «Создание учетной записи» на стр. 72). Эта возможность полезна в том случае, если в сети ViPNet несколько администраторов, между которыми распределены обязанности по управлению структурой сети.

Наличие нескольких учетных записей администраторов дает следующие преимущества:

- Несколько администраторов могут работать в многопользовательском режиме, одновременно подключаясь к серверному приложению ViPNet Центр управления сетью со своих рабочих мест.
- Действия каждого администратора регистрируются в журнале аудита системных событий программы ViPNet Центр управления сетью (см. «Журналы аудита» на стр. 100), что обеспечивает прозрачность в управлении сетью.

При работе программы ViPNet Центр управления сетью в многопользовательском режиме действуют следующие ограничения:

- Невозможно одновременное подключение нескольких клиентских приложений от имени одной учетной записи администратора.
- Если в одном из запущенных клиентских приложений выполняется длительная операция, такая как создание справочников для большого количества узлов, в других клиентских приложениях блокируется возможность добавлять и удалять объекты, изменять их свойства. Тем не менее, свойства объектов доступны для просмотра.
- Если в одном из запущенных клиентских приложений выполняется создание структуры сети с помощью мастера или загрузка существующей структуры сети, в других клиентских приложениях все данные будут заблокированы как для изменения, так и для чтения.

Создание учетной записи

Чтобы создать новую учетную запись администратора программы ViPNet Центр управления сетью, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Администрирование**.
2. На панели навигации выберите раздел **Учетные записи**.

3 В разделе **Учетные записи** на панели инструментов нажмите кнопку . Откроется окно **Новая учетная запись**.

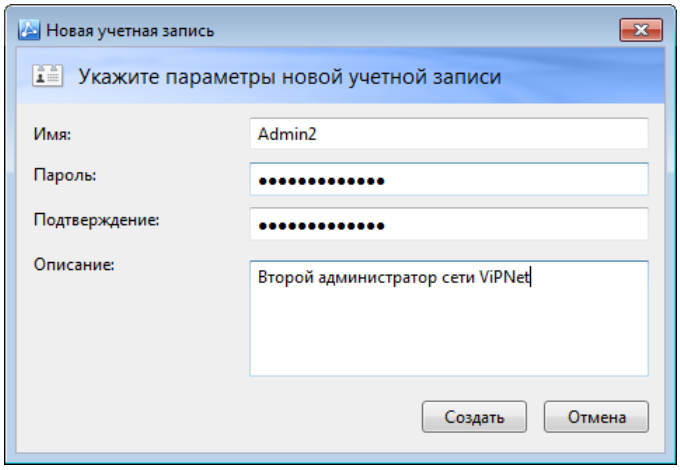

Рисунок 34. Создание новой учетной записи администратора

4 В поле **Имя** задайте имя учетной записи. В дальнейшем имя учетной записи не может быть изменено.

5 В соответствующих полях задайте пароль учетной записи и подтвердите его.

6 Если требуется, в поле **Описание** введите краткое описание учетной записи.

7 Нажмите кнопку **Создать**. Новая учетная запись будет добавлена в список.

8 Сообщите имя и пароль созданной учетной записи администратору, который будет работать от имени этой записи.

В целях обеспечения безопасности после первого входа в программу от имени новой учетной записи появится окно для смены пароля (см. рисунок на стр. 51). Без изменения пароля продолжение работы будет невозможно.

Удаление учетной записи

Если какая-либо учетная запись администратора программы ViPNet Центр управления сетью больше не используется или если требуется запретить обладателю учетной записи вход в программу, вы можете удалить учетную запись. Для этого выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью выберите представление **Администрирование**.

2 На панели навигации выберите раздел **Учетные записи**.

3 В разделе **Учетные записи** выберите в списке одну или несколько учетных записей для удаления и нажмите кнопку на панели инструментов.

Примечание. Невозможно удалить учетную запись, от имени которой вы вошли в программу в текущем сеансе работы.

---

4 В окне подтверждения нажмите кнопку **Удалить записи**. Выбранные учетные записи будут удалены.

Если учетная запись была удалена в то время, как администратор — владелец записи работал в программе ViPNet Центр управления сетью, в клиентском приложении на рабочем месте этого администратора появится сообщение об удалении учетной записи, дальнейшая работа будет заблокирована. После того как в окне сообщения будет нажата кнопка **OK**, клиентское приложение будет закрыто.

Изменение пароля учетной записи

Администратор программы ViPNet Центр управления сетью имеет возможность изменить пароль только той учетной записи, от имени которой он вошел в программу. Изменение паролей других учетных записей невозможно.

Чтобы изменить пароль вашей учетной записи, выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Сервис** выберите пункт **Сменить свой пароль**.

2 В окне **Смена пароля** в соответствующем поле введите текущий пароль вашей учетной записи.

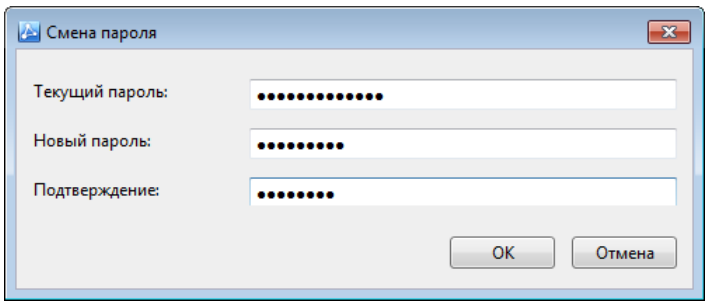

Рисунок 35. Смена пароля текущей учетной записи

3 Задайте новый пароль и введите его снова для подтверждения. Пароль должен содержать не менее восьми символов.

Совет. Рекомендуется задавать сложные пароли, содержащие не менее восьми символов, в состав которых входят буквы в разных регистрах, цифры и специальные символы.

---

4 Нажмите кнопку **OK**. Пароль вашей учетной записи будет изменен.

Настройка параметров программы по умолчанию

Параметры работы с объектами сети

В программе ViPNet Центр управления сетью вы можете задать дополнительные действия, которые будут выполняться по умолчанию при создании или удалении узлов и пользователей сети ViPNet, а также время использования старого адреса клиента после его регистрации на другом координаторе.

Для настройки параметров создания и удаления объектов выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Сервис** выберите пункт **Параметры**.

2 В окне **Параметры ViPNet Центр управления сетью** на левой панели выберите раздел **Работа с объектами**.

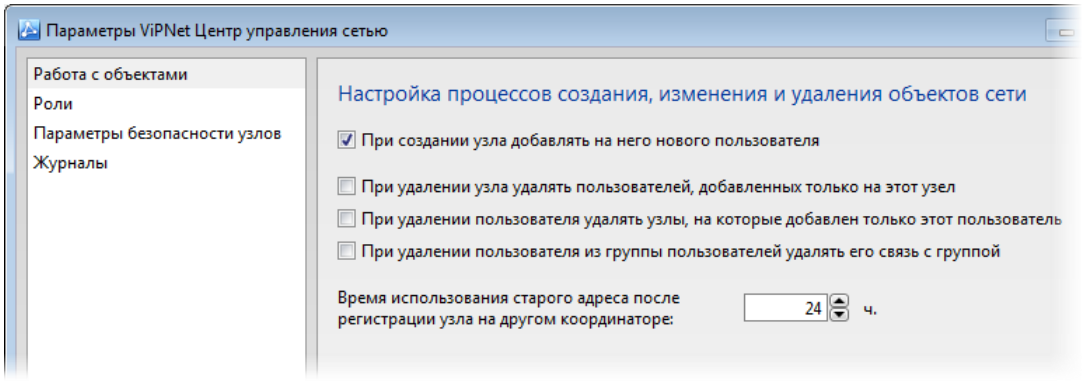

Рисунок 36. Параметры создания и удаления объектов сети ViPNet

3 Если требуется при создании нового узла автоматически создавать для этого узла пользователя, убедитесь, что установлен флажок **При создании узла добавлять на него нового пользователя.**

В этом случае в окне **Новый координатор** (см. «Добавление координатора» на стр. 112) или **Новый клиент** (см. «Добавление клиента» на стр. 113) по умолчанию будет установлен флажок **Создать одноименного пользователя на новом узле автоматически**.

4 Если требуется при удалении узла автоматически удалять пользователей, которые зарегистрированы только на удаляемом узле, установите флажок **При удалении узла удалять пользователей, добавленных только на этот узел**.

В этом случае в окне **Удаление координаторов** (см. «Удаление координатора» на стр. 116) или **Удаление клиентов** (см. «Удаление клиента» на стр. 117) по умолчанию будет установлен флажок **Удалять одиночных пользователей на сетевых узлах**.

5 Если требуется при удалении пользователя автоматически удалять узлы, на которых зарегистрирован только удаляемый пользователь, установите флажок **При удалении пользователя удалять узлы, на которые добавлен только этот пользователь**.

   В этом случае в окне **Удаление пользователей** по умолчанию будет установлен флажок **Удалять сетевые узлы, для которых пользователь является единственным зарегистрированным**.

6 Если требуется при удалении пользователя из группы разрывать его связь с этой группой, установите флажок **При удалении пользователя из группы пользователей удалять его связь с группой**.

   В этом случае при удалении пользователя из группы (см. «Изменение списка участников группы пользователей» на стр. 216) в окне **Пользователи** будет по умолчанию установлен флажок **Удалить связи пользователей с группой пользователей**.

7 Измените, если требуется, время использования старого адреса узла после его регистрации на другом координаторе (см. «Перенос клиента на другой координатор» на стр. 129). По умолчанию время использования 24 часа.

8 Для сохранения настроек нажмите кнопку **ОК**.

Параметры безопасности узлов

С помощью программы ViPNet Центр управления сетью вы можете централизованно настроить параметры безопасности сетевых узлов и передать их на узлы в составе дистрибутива ключей или обновления справочников. Это позволяет избежать необходимости настраивать параметры безопасности для каждого узла вручную и особенно удобно, если узлов много.

Для настройки параметров безопасности узлов защищенной сети ViPNet выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Сервис** выберите пункт **Параметры**.

2 В окне **Параметры ViPNet Центр управления сетью** на левой панели выберите раздел **Параметры безопасности узлов**.

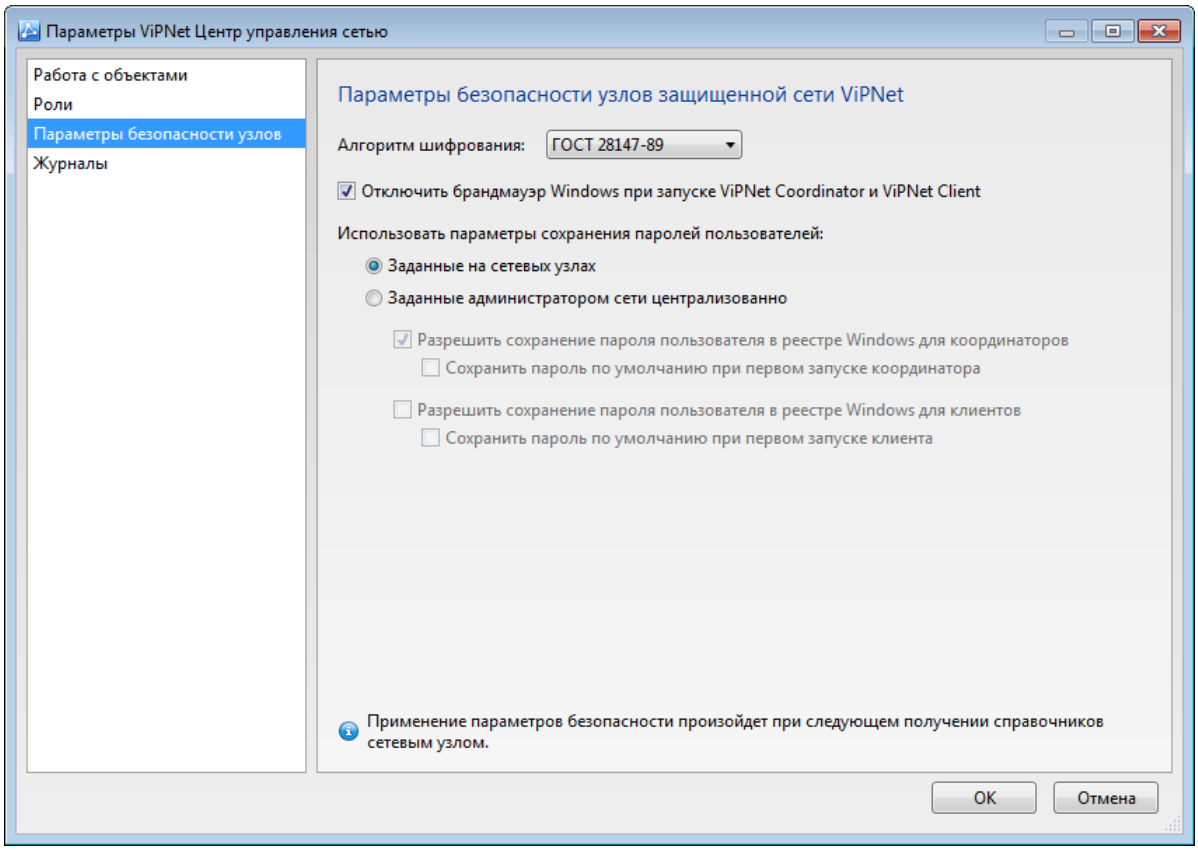

Рисунок 37. Параметры безопасности узлов

3 Чтобы задать алгоритм шифрования исходящего IP-трафика сетевых узлов и писем, отправляемых пользователями сетевых узлов с помощью программы ViPNet Деловая почта, в списке **Алгоритм шифрования** выберите один из стандартов:

- ГОСТ 28147-89 — российский стандарт симметричного шифрования (по умолчанию).
- AES — принятый в США стандарт симметричного шифрования на основе алгоритма Rijndael.

Внимание! В сертифицированной версии программы возможность выбора алгоритма шифрования отсутствует — по умолчанию применяется алгоритм ГОСТ 28147-89.

---

4 Для фильтрации трафика, проходящего через узлы, рекомендуется использовать сетевые экраны, встроенные в программы ViPNet Coordinator или ViPNet Client. При этом на сетевых узлах должен быть отключен брандмауэр Windows, иначе между сетевым экраном и брандмауэром Windows могут возникнуть конфликты, влекущие за собой проблемы с доступом в сеть. Чтобы брандмауэр отключался при запуске программ ViPNet Coordinator и ViPNet Client на всех узлах сети автоматически, по умолчанию установлен флажок **Отключить брандмауэр Windows при запуске ViPNet Coordinator и ViPNet Client**.

При необходимости (например, если встроенный сетевой экран ViPNet по каким-либо причинам не используется для фильтрации IP-трафика на узлах) снимите флажок **Отключить брандмауэр Windows при запуске ViPNet Coordinator и ViPNet Client**.

5 Чтобы централизованно настроить параметры сохранения паролей для всех пользователей программы ViPNet Coordinator или ViPNet Client, щелкните **Заданные администратором сети централизованно** и выполните следующие действия:

- Чтобы разрешить пользователю программы ViPNet Coordinator или ViPNet Client сохранять пароль в реестре Windows (то есть устанавливать флажок **Сохранять пароль** в окне аутентификации программы), установите соответствующий флажок. Это удобно в случае удаленной работы на сетевом узле, но ведет к снижению уровня безопасности узла. По умолчанию сохранять пароль разрешается только пользователям программы ViPNet Coordinator.

  Если флажок **Разрешить сохранение пароля пользователя в реестре Windows для координаторов** или **Разрешить сохранение пароля пользователя в реестре Windows для клиентов** снят, возможность сохранения пароля по умолчанию соответствующей программы недоступна.

- Чтобы по умолчанию при первом запуске программы ViPNet Coordinator или ViPNet Client в окне аутентификации был установлен флажок **Сохранить пароль** (то есть пароль пользователя автоматически подставлялся в поле ввода), установите флажок **Сохранить пароль по умолчанию при первом запуске координатора** или **Сохранить пароль по умолчанию при первом запуске клиента**.

Примечание. При установке соответствующего флажка для сохранения пароля по умолчанию пароль пользователя программы ViPNet Coordinator или ViPNet Client будет автоматически подставляться в поле ввода только в том случае, если данная настройка безопасности передана на узлы в составе дистрибутива ключей. Если вы установите соответствующий флажок для сохранения пароля по умолчанию и отправите настройки безопасности на узлы в составе обновления справочников, в окне аутентификации программы ViPNet Coordinator или ViPNet Client флажок **Сохранить пароль** установлен не будет.

По умолчанию настройка параметров сохранения паролей пользователей программ ViPNet Client и ViPNet Coordinator производится администратором каждого сетевого узла локально (подробнее см. в документе «ViPNet Client for Windows. Руководство пользователя» или «ViPNet Coordinator for Windows. Руководство пользователя», в главе «Административные функции», в разделе «Работа в программе в режиме администратора»).

6 Для сохранения настроек нажмите кнопку **OK**.

7 Если вы изменили настройки параметров сохранения паролей пользователей ViPNet Coordinator и ViPNet Client, в открывшемся окне выполните одно из действий:

- Чтобы применить настройки для всех узлов сети ViPNet, нажмите кнопку **Да, применить**. В результате все параметры безопасности будут переданы на узлы в составе дистрибутива ключей или в составе обновления справочников.

Примечание. Если параметры сохранения паролей пользователей переданы на узлы сети ViPNet в составе дистрибутива ключей или в составе обновления справочников, в программах ViPNet Coordinator и ViPNet Client версий 4.2 и ниже администратор сетевого узла не сможет изменить эти параметры локально, а в программах ViPNet Coordinator и

ViPNet Client версии 4.3 — сможет.

- Чтобы отказаться от изменения настроек параметров сохранения паролей пользователей ViPNet Coordinator и ViPNet Client, нажмите кнопку **Нет**. В этом случае на узлы будут переданы все настройки параметров безопасности, кроме параметров сохранения паролей пользователей.

Роли узлов по умолчанию

При создании новых узлов сети ViPNet на эти узлы могут быть автоматически добавлены определенные роли (см. «Роли сетевых узлов» на стр. 31). Автоматическое добавление часто используемых ролей на сетевые узлы позволяет упростить настройку новых узлов, однако может привести к излишнему расходу лицензионных ограничений (см. «Лицензия на сеть ViPNet» на стр. 23).

Примечание. По умолчанию на узлы могут быть добавлены только роли, для которых не заданы дополнительные ограничения по версиям и периоду использования соответствующего программного обеспечения.

Чтобы указать роли, которые требуется добавлять на создаваемые узлы по умолчанию, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню **Сервис** выберите пункт **Параметры**.
2. В окне **Параметры ViPNet Центр управления сетью** на левой панели выберите раздел **Роли**.

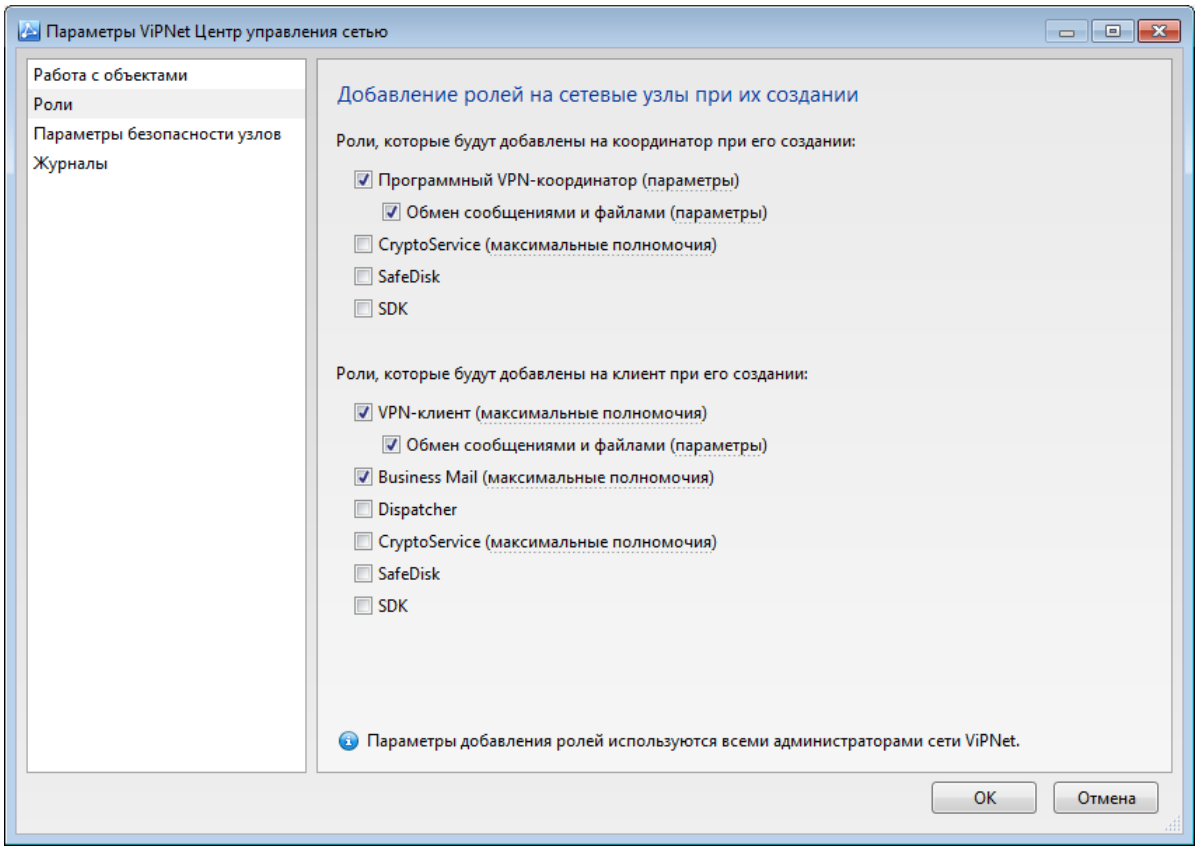

Рисунок 38. Добавление ролей по умолчанию для новых узлов

3 Чтобы задать роли для добавления на новые координаторы (см. «Добавление координатора» на стр. 112), в списке **Роли, которые будут добавлены на координатор при его создании** установите или снимите нужные флажки.

По умолчанию установлены флажки **Программный VPN-координатор** и **Обмен сообщениями и файлами**.

4 Чтобы задать роли для добавления на новые клиенты (см. «Добавление клиента» на стр. 113), в списке **Роли, которые будут добавлены на клиент при его создании** установите или снимите нужные флажки.

По умолчанию установлены флажки **VPN-клиент**, **Обмен сообщениями и файлами** и **Business Mail**.

Примечание. Если в вашей сети отсутствуют лицензии (см. «Лицензия на сеть ViPNet» на стр. 23) на какие-либо из выбранных ролей, эти роли не будут добавляться на создаваемые сетевые узлы.

---

5 Если требуется изменить уровень полномочий, который будет установлен при автоматическом добавлении роли на новые узлы, щелкните ссылку справа от имени роли и в окне **Свойства роли** установите нужный уровень (см. «Изменение уровня полномочий пользователя» на стр. 146).

По умолчанию для всех ролей задан максимальный уровень полномочий.

6 Чтобы обеспечить раздельный доступ узлов в Интернет при отсутствии соединения с узлами ViPNet или к ресурсам сети ViPNet при отсутствии подключения к Интернет, в окне **Свойства роли** установите флажок **Координатор является защищенным интернет-шлюзом**.

Примечание. Настройка доступна для ролей «Программный VPN-координатор» и соответствующих ролей для координаторов на базе модификаций ПАК ViPNet Coordinator HW, ПАК ViPNet Coordinator IG.

---

7 Если требуется изменить права на использование обмена сообщениями и файлами, которые будут установлены при автоматическом добавлении роли **Обмен сообщениями и файлами** на новые узлы, щелкните ссылку справа от этой роли и в окне **Свойства роли** задайте нужные права (см. «Настройка параметров роли „Обмен сообщениями и файлами“» на стр. 147).

По умолчанию для роли **Обмен сообщениями и файлами** разрешены оба вида обмена — обмен сообщениями и файловый обмен.

8 Для сохранения настроек нажмите кнопку **OK**.

Параметры журналов

В программе ViPNet Центр управления сетью вы можете задать время хранения записей в журналах аудита. Для этого выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Сервис** выберите пункт **Параметры**.

2 В окне **Параметры ViPNet Центр управления сетью** на левой панели выберите раздел **Журналы**.

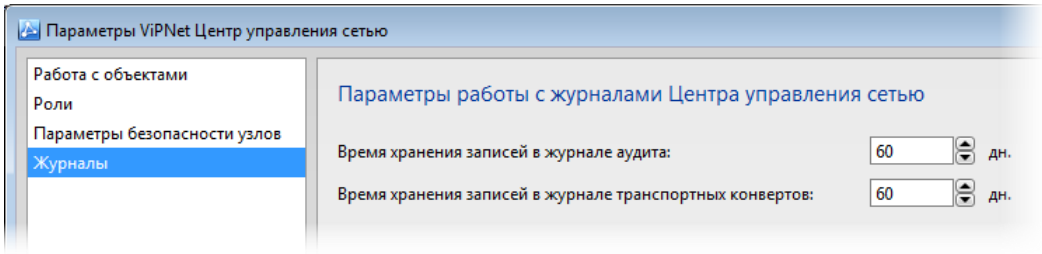

Рисунок 39. Параметры журналов

3 Чтобы задать время хранения записей в журналах аудита, в соответствующем поле установите необходимое число дней. Минимальное время хранения 7 дней, максимальное — 365 дней. По умолчанию записи хранятся 60 дней.

Записи с истекшим временем хранения автоматически удаляются из журналов.

4 Чтобы задать время хранения записей в журнале транспортных конвертов, в соответствующем поле установите необходимое число дней. Минимальное время хранения 1 день, максимальное — 365 дней. По умолчанию записи хранятся 60 дней.

Записи со сроком хранения более установленного значения автоматически удаляются из журналов в 00:00 часов следующего дня.

5 Для сохранения настроек нажмите кнопку **OK**.

Примечание. База данных SQL хранит содержимое отправляемых транспортных конвертов. Размер базы данных SQL будет заметно увеличиваться, если:

- задан длительный срок хранения записей в журналах транспортных конвертов — 30-60 дней;
- существует большое число объектов сети ViPNet и связей между ними;
- происходит частая отправка обновлений на сетевые узлы.

В случае недостаточного места на жестком диске, вы можете задать время хранения записей в журнале транспортных конвертов 1 день. Это позволит освободить дополнительное место на жестком диске.

Проверка конфигурации сети

Чтобы убедиться в том, что структура вашей сети ViPNet не содержит ошибок и заданы основные параметры объектов сети, вы можете выполнить проверку конфигурации сети ViPNet. Кроме того, проверка конфигурации сети выполняется автоматически перед созданием справочников (см. «Создание справочников» на стр. 88).

В результате проверки конфигурации сети могут быть обнаружены ошибки двух типов:

- Конфликтные данные — ошибки, которые препятствуют нормальному функционированию сети ViPNet в целом. В случае обнаружения конфликтных данных будет заблокирована возможность создавать справочники для любых сетевых узлов.

  Например, конфликт может возникнуть, если какие-либо координаторы вашей сети не связаны межсерверными каналами напрямую или через другие координаторы.

- Неполные данные — ошибки, которые препятствуют функционированию отдельных объектов сети ViPNet. Информация об объектах с неполными данными не будет включена в справочники сетевых узлов. Также невозможно создать справочники для узлов с неполными данными.

  Например, неполными данными считается отсутствие ролей или пользователей на сетевом узле.

Чтобы запустить проверку конфигурации сети вручную, выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Моя сеть** выберите пункт **Проверить конфигурацию сети**.

2 Если при проверке не будет обнаружено ошибок, появится соответствующее сообщение.

  Если при проверке будут обнаружены конфликтные или неполные данные, откроется окно **Проверка конфигурации сети** со списком обнаруженных ошибок.

  Конфликтные данные будут отмечены в списке значком  . Неполные данные будут отмечены значком  .

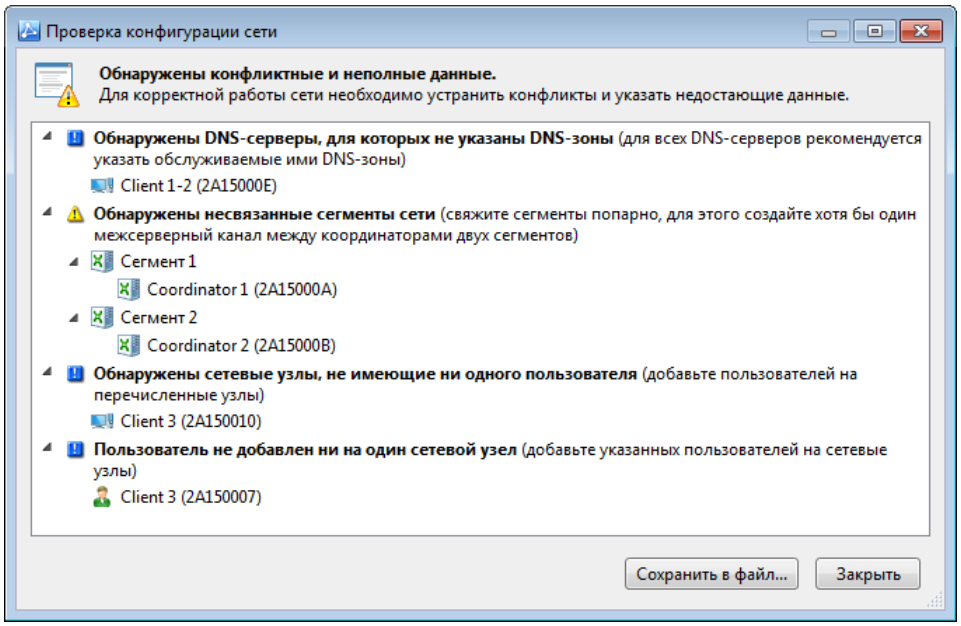

Рисунок 40. Список конфликтных и неполных данных

3 В окне **Проверка конфигурации сети** выполните следующие действия:

- Ознакомьтесь со списком обнаруженных ошибок. Чтобы обеспечить правильное функционирование сети, устраните конфликты и укажите недостающие данные.
- Если требуется сохранить отчет об обнаруженных ошибках в файл, нажмите кнопку **Сохранить в файл**.
- Чтобы закрыть окно **Проверка конфигурации сети**, нажмите соответствующую кнопку.

Создание отчета о структуре сети

С помощью программы ViPNet Центр управления сетью вы можете создавать и сохранять отчеты о структуре развернутой сети ViPNet в файлы формата XML и HTML. В файлах отчетов в иерархическом виде отображаются координаторы и клиенты вашей сети ViPNet, а также содержится информация о пользователях узлов, назначенных ролях, группах узлов, группах пользователей и имеющихся связях между узлами и пользователями.

Чтобы сохранить файл с отчетом о структуре сети ViPNet, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню **Моя сеть** выберите пункт **Сохранить отчет о структуре сети в файл**.
2. В открывшемся окне укажите расположение и имя сохраняемого файла, а также выберите одно из возможных расширений файла: `*.xml` или `*.html`.
3. Нажмите кнопку **Сохранить**.

В результате файл отчета будет сохранен в указанной папке. Теперь вы можете просмотреть его, распечатать на принтере или использовать в другой программе.

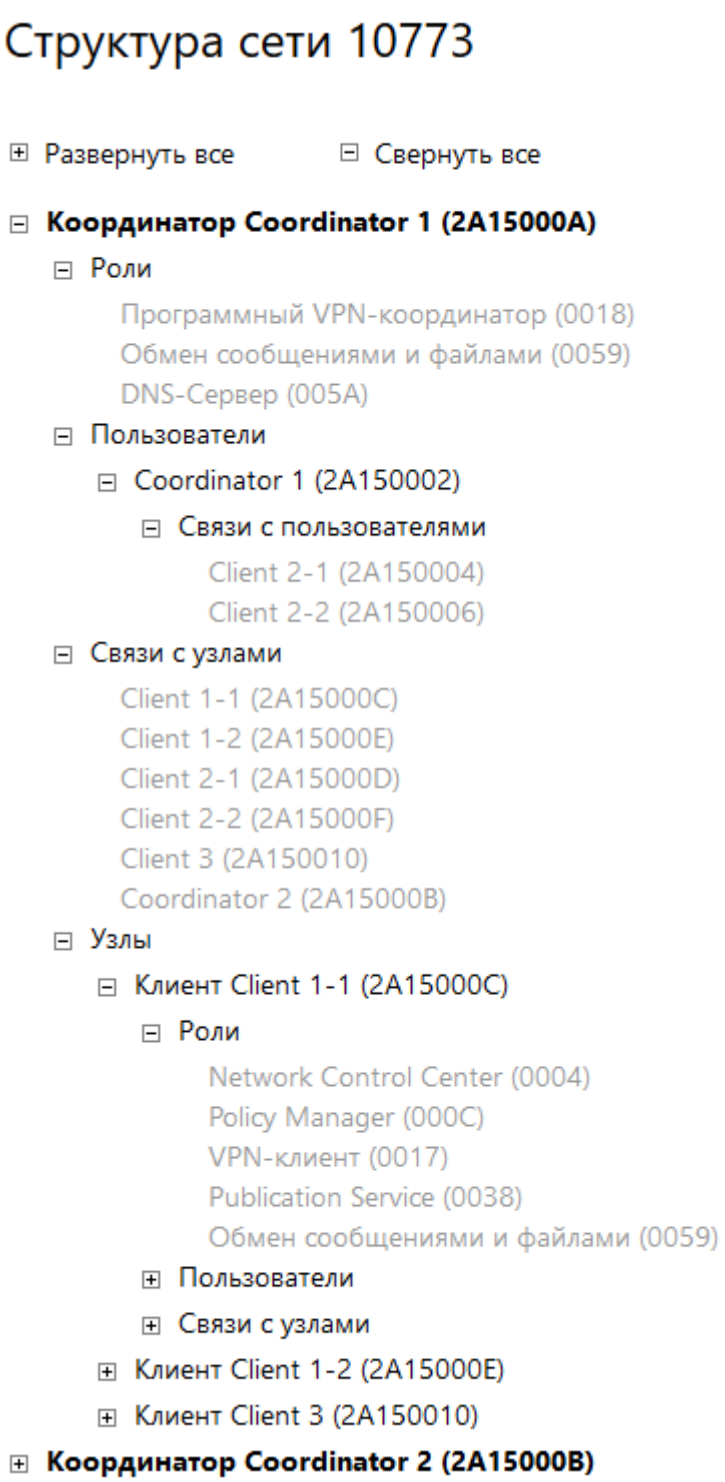

Рисунок 41. Просмотр отчета о структуре сети ViPNet в формате HTML

Отправка обновлений на сетевые узлы

Обновление справочников и ключей

Если в программе ViPNet Центр управления сетью была изменена структура сети ViPNet или свойства сетевых узлов, требуется передать информацию об этих изменениях на сетевые узлы, отправив новые справочники и ключи. Для этого выполните следующие действия:

1. Для сетевых узлов, свойства которых были изменены, создайте справочники (см. «Создание справочников» на стр. 88).
2. Если для сетевых узлов указан статус **Ожидаются ключи** (см. ниже), дождитесь, пока в Удостоверяющем и ключевом центре будут созданы ключи узлов (см. глоссарий, стр. 304).

   Создание ключей узлов требуется в следующих случаях:

   - Если были добавлены или удалены сетевые узлы или пользователи.
   - Если были изменены связи между сетевыми узлами или между пользователями.
   - Если пользователи были добавлены на сетевые узлы или удалены с сетевых узлов.
   - Если пользователи были добавлены в группы или удалены из групп.
   - Если был изменен координатор, на котором зарегистрирован клиент, то есть его транспортный сервер (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).

   В остальных случаях достаточно создать справочники, например:

   - Если на сетевые узлы были добавлены или удалены роли, изменены свойства ролей.
   - Если были изменены адреса сетевых узлов.
   - Если были изменены параметры подключения узлов к внешней сети.
3. Если для сетевых узлов указан статус **Готовы к отправке**, отправьте новые справочники и ключи на сетевые узлы (см. «Отправка справочников и ключей» на стр. 91).

На необходимость обновления справочников и ключей на сетевых узлах указывает их статус, который отображается в списках клиентов и координаторов в столбце **Справочники и ключи**:

- Статус **Требуется создать** указывает, что для сетевого узла необходимо создать справочники.
- Статус **Ожидаются ключи** указывает, что в программе ViPNet Удостоверяющий и ключевой центр необходимо создать ключи узла. Этот статус появляется после создания справочников.
- Статус **Готовы к отправке** указывает, что необходимо отправить справочники и ключи на сетевой узел. Этот статус может появиться в следующих случаях:
  - После создания справочников, если обновление ключей узла не требуется.

- После того как в Удостоверяющем и ключевом центре были созданы и перенесены в Центр управления сетью ключи узла (см. глоссарий, стр. 304), ключи пользователя (см. глоссарий, стр. 303) или обновления ключей узла.

Примечание. Если пользователь зарегистрирован на нескольких сетевых узлах, его ключи пользователя (см. глоссарий, стр. 303) будут отправлены только на первый узел, на который он был добавлен.

- Статус **Отправлены** указывает, что справочники и ключи отправлены на сетевой узел, обновление не требуется.
- Статус **Доставлены** указывает, что отправленные справочники и ключи были доставлены на сетевой узел.
- Статус **Приняты** указывает, что справочники и ключи на сетевом узле были успешно обновлены. Если обновление не удалось, появится статус **Не приняты**.

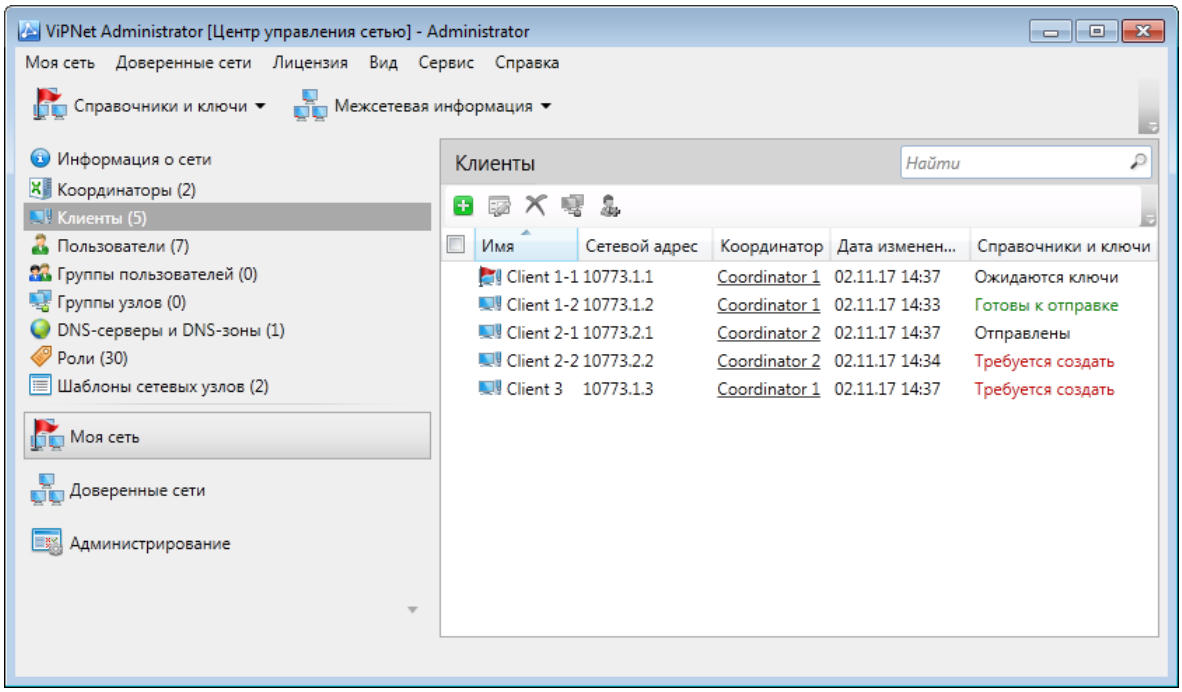

Рисунок 42. Статусы справочников и ключей

Создание справочников

Справочники для сетевых узлов (см. «Справочники и ключи ViPNet» на стр. 32) могут быть созданы в групповом или в индивидуальном режиме.

Для группового создания справочников выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью на панели инструментов нажмите кнопку **Справочники и ключи** и в меню выберите пункт **Создать справочники**.

Если справочники для всех узлов актуальны и не требуют обновления, появится соответствующее сообщение.

2 Если конфигурация вашей сети содержит ошибки, откроется окно **Проверка конфигурации сети**.

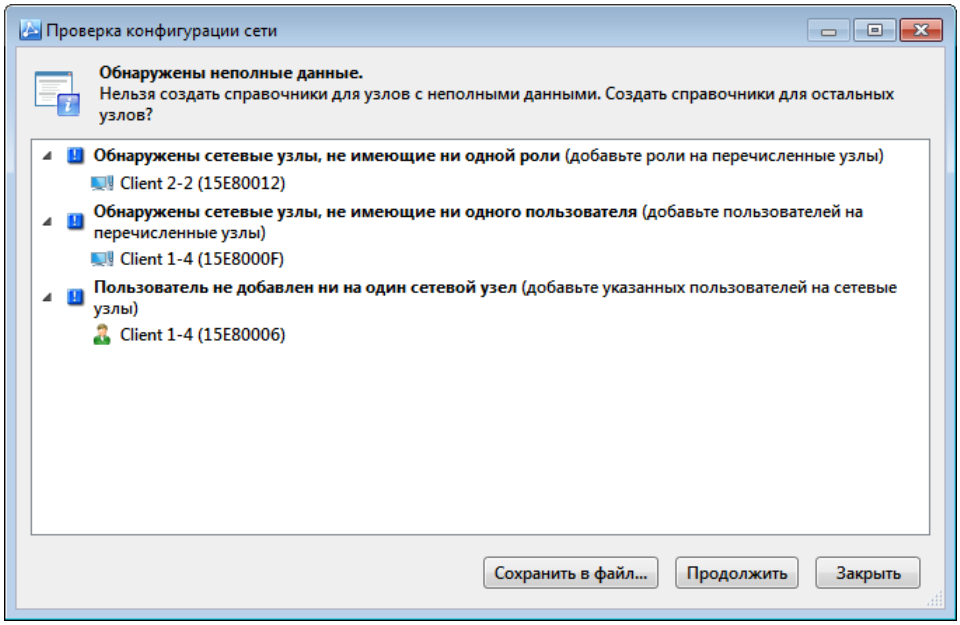

Рисунок 43. Проверка конфигурации сети при создании справочников

В случае обнаружения конфликтных данных (см. «Проверка конфигурации сети» на стр. 83) создание справочников невозможно. Перед созданием справочников устраните конфликты, перечисленные в списке.

Если обнаружены неполные данные, но не обнаружены конфликтные данные, вы можете выбрать одно из действий:

- Чтобы отказаться от создания справочников, нажмите кнопку **Закрыть**.
- Чтобы создать справочники для узлов, которые не имеют неполных данных, нажмите кнопку **Продолжить**. В этом случае информация об узлах с неполными данными не будет включена в справочники других узлов.

3 Если конфигурация вашей сети не содержит ошибок или если вы решили создать справочники при наличии неполных данных, откроется окно **Создание справочников**.

При необходимости в окне **Создание справочников** выберите сетевые узлы, для которых требуется создать справочники. Вы можете выбрать сразу все сетевые узлы с помощью флажка, расположенного в заголовке списка. Для поиска сетевых узлов по именам введите часть имени узла в строку поиска, расположенную внизу окна.

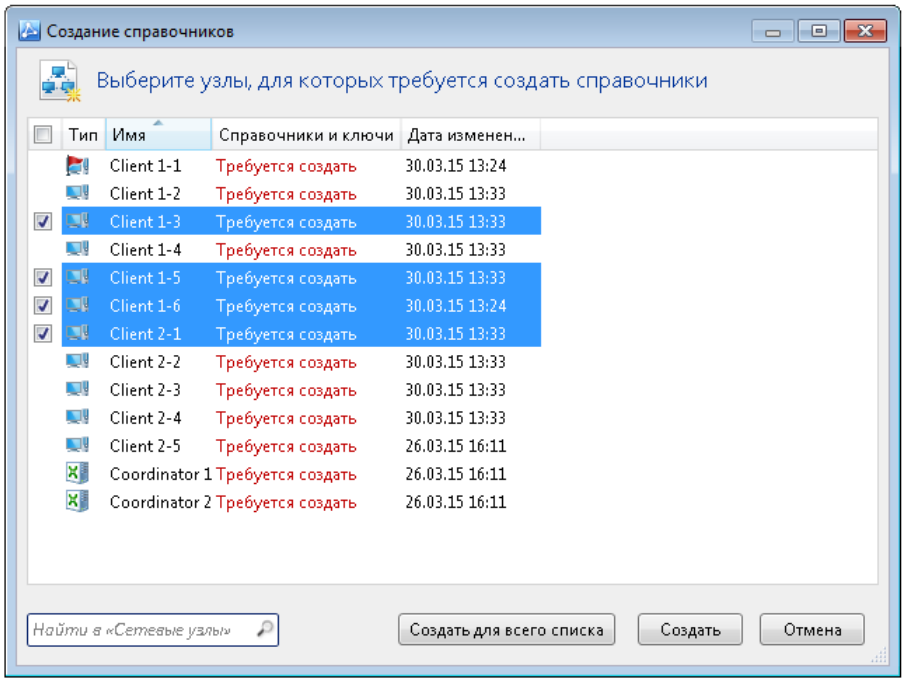

Рисунок 44. Создание справочников

4 Чтобы начать создание справочников, выполните одно из действий:

- Чтобы создать справочники для выбранных сетевых узлов, нажмите кнопку **Создать**.
- Чтобы создать справочники для всех сетевых узлов, отображаемых в списке, нажмите кнопку **Создать для всего списка**. Если вы использовали строку поиска сетевых узлов, справочники будут созданы только для найденных узлов.

5 В результате будут созданы справочники для сетевых узлов. Если создание справочников для сетевых узлов завершено с ошибкой, в открывшемся окне со сведениями о ходе процесса нажмите кнопку **Отчет**, чтобы просмотреть дополнительную информацию об ошибках.

Чтобы создать справочники для одного или нескольких выбранных сетевых узлов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы** или **Клиенты**, в зависимости от типа узлов, для которых требуется создать справочники.

3 На панели просмотра выберите в списке один или несколько сетевых узлов, для которых отображается статус «Требуется создать» (см. «Обновление справочников и ключей» на стр. 87). Для узлов с другим статусом создание справочников невозможно.

4 Щелкните выбранные узлы правой кнопкой мыши и в контекстном меню выберите пункт **Создать справочники**.

5 Если конфигурация вашей сети содержит ошибки, откроется окно **Проверка конфигурации сети** (см. рисунок на стр. 89).

- В случае обнаружения конфликтных данных (см. «Проверка конфигурации сети» на стр. 83) создание справочников будет невозможно.

- Если обнаружены только неполные данные, вы можете продолжить создание справочников, но в справочники не будет включена информация об узлах с неполными данными.

6 Если конфигурация вашей сети не содержит ошибок или если вы решили создать справочники при наличии неполных данных, в окне **Создание справочников** нажмите кнопку **Создать справочники**. Начнется процесс создания справочников для выбранных сетевых узлов.

7 В результате будут созданы справочники для сетевых узлов. В случае если создание справочников для сетевых узлов завершено с ошибкой в открывшемся окне нажмите кнопку **Отчет**, чтобы просмотреть дополнительную информацию об ошибках.

Отправка справочников и ключей

Справочники и ключи могут быть отправлены на сетевые узлы в групповом или в индивидуальном режиме.

Внимание! Если пользователь зарегистрирован на нескольких сетевых узлах, его ключи пользователя (см. глоссарий, стр. 303) будут отправлены только на первый узел, на который он был добавлен.

Узнать первый узел, на который был добавлен пользователь, можно с помощью журнала **Управление конфигурацией своей сети**, указав в параметрах поиска соответствующие событие и имя объекта (см. «Журналы аудита» на стр. 100).

Для групповой отправки справочников и ключей выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью на панели инструментов нажмите кнопку **Справочники и ключи**  и в меню выберите пункт **Отправить справочники и ключи**.

Откроется окно **Отправка справочников и ключей** со списком сетевых узлов, на которые могут быть отправлены справочники и ключи.

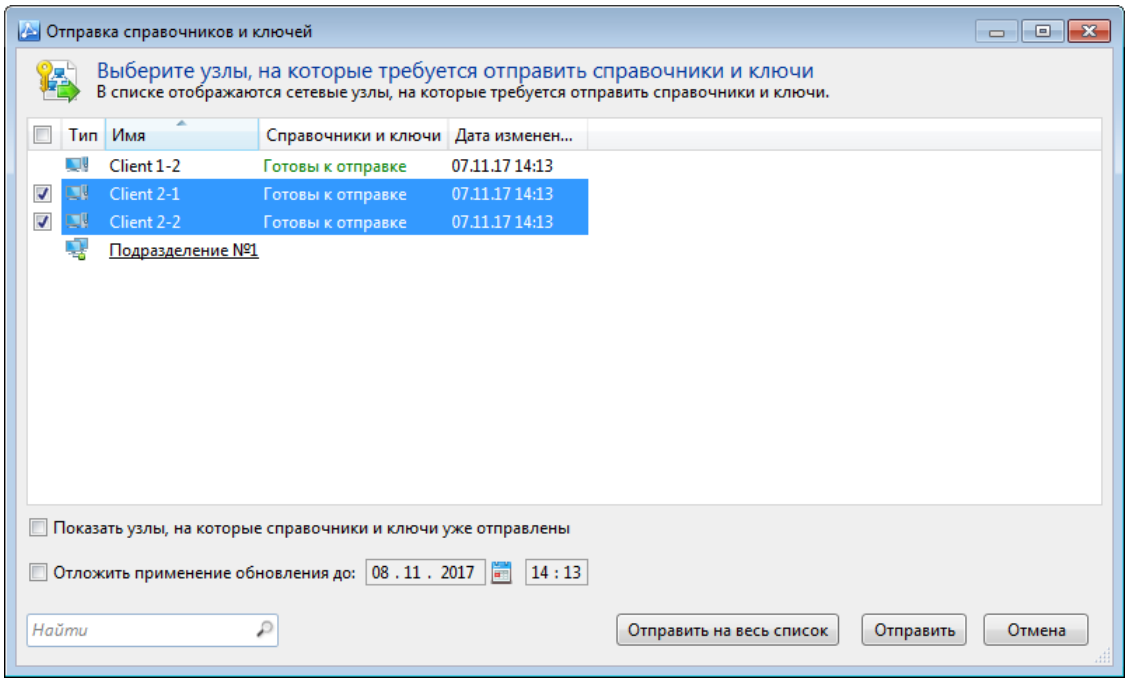

Рисунок 45. Отправка справочников и ключей

2 Если вы хотите повторно отправить справочники и ключи на сетевые узлы, на которые уже были отправлены последние обновления, установите флажок **Показать узлы, на которые справочники и ключи уже отправлены**. Эти узлы будут отображены в списке.

3 При необходимости выберите в списке сетевые узлы или группы узлов, на которые требуется отправить справочники и ключи. Вы можете выбрать сразу все сетевые узлы с помощью флажка, расположенного в заголовке списка.

Выбор группы сетевых узлов удобен, если в списке отображено большое количество узлов. При этом справочники и ключи будут отправлены только тем узлам из группы, для которых это требуется.

Для поиска сетевых узлов или групп по именам введите часть имени в строку поиска, расположенную внизу окна.

4 Если вы хотите, чтобы новые справочники и ключи были применены на сетевых узлах в определенное время, выполните следующие действия:

- Установите флажок **Отложить применение обновления до**.
- В полях справа от флажка задайте дату и время применения обновлений. Дату можно выбрать с помощью календаря, нажав кнопку .

5 Для отправки справочников и ключей выполните одно из действий:

- Чтобы отправить справочники и ключи на выбранные сетевые узлы, нажмите кнопку **Отправить**.
- Чтобы отправить справочники и ключи на все сетевые узлы, отображаемые в списке, нажмите кнопку **Отправить на весь список**. Если вы использовали строку поиска сетевых узлов, обновления будут отправлены только на найденные узлы.

Примечание. Отправка справочников и ключей осуществляется с помощью транспортного модуля ViPNet MFTP, который является частью программы ViPNet Client. Убедитесь, что на компьютере с серверным приложением ViPNet Центр управления сетью запущена эта программа.

6 Если обновления справочников и ключей не отправлены, для просмотра дополнительной информации в окне **Отправка справочников** нажмите кнопку **Отчет**. В случае успешной отправки справочников и ключей окно **Отправка справочников** закроется автоматически.

Чтобы отправить справочники и ключи на один или несколько выбранных сетевых узлов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы** или **Клиенты**, в зависимости от типа узлов, на которые требуется отправить справочники и ключи.

3 На панели просмотра выберите в списке один или несколько сетевых узлов.

Примечание. Нельзя отправить справочники и ключи на сетевые узлы, для которых отображается статус «Требуется создать» или «Ожидаются ключи» (см. «Обновление справочников и ключей» на стр. 87).

4 Щелкните выбранные узлы правой кнопкой мыши и в контекстном меню выберите пункт **Отправить справочники и ключи**.

5 Если вы хотите, чтобы новые справочники и ключи были применены на сетевых узлах в определенное время, в окне **Отправка справочников и ключей**:

- Установите флажок **Отложить применение обновления до**.
- В полях справа от флажка задайте дату и время применения обновлений. Дату можно выбрать с помощью календаря, нажав кнопку  .

6 Нажмите кнопку **Отправить справочники и ключи**, начнется процесс отправки.

7 Если обновления справочников и ключей отправлены с ошибкой, для просмотра дополнительной информации в окне **Отправка справочников** нажмите кнопку **Отчет**. В случае успешной отправки справочников и ключей окно **Отправка справочников** закроется автоматически.

После отправки справочников и ключей вы можете просмотреть их статус в списке координаторов или клиентов в столбце **Справочники и ключи** (см. «Обновление справочников и ключей» на стр. 87). Подробный отчет об отправке обновлений и их статусе можно просмотреть в журнале транспортных конвертов (см. «Журналы транспортных конвертов» на стр. 102).

Обновление программного обеспечения

Если требуется обновить программное обеспечение ViPNet, установленное на сетевых узлах, воспользуйтесь возможностью удаленной отправки программного обеспечения из Центра управления сетью.

Обновление программного обеспечения отправляется на сетевые узлы в виде файлов формата LZH. Для каждого типа программного обеспечения ViPNet существуют соответствующие файлы обновления. По вопросу получения файлов для обновления программного обеспечения ViPNet обратитесь в ОАО «ИнфоТеКС» (см. «Обратная связь» на стр. 19).

Чтобы отправить обновление программного обеспечения на сетевые узлы, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню **Моя сеть** выберите пункт **Обновить программное обеспечение на узлах**. Будет запущен мастер обновления программного обеспечения.
2. На первой странице мастера нажмите кнопку **Далее**.
3. Если файл обновления, который требуется отправить на сетевые узлы, еще не загружен в базу данных, на странице **Выберите обновление для отправки на узлы** загрузите этот файл. Для этого:
   - Нажмите кнопку **Загрузить файл обновления**.
   - В окне **Загрузка файла обновления** выберите в списке нужный тип программного обеспечения и с помощью кнопки **Обзор** укажите путь к файлу обновления (с расширением `.lzh`), который требуется отправить на сетевые узлы. Затем нажмите кнопку **ОК**.

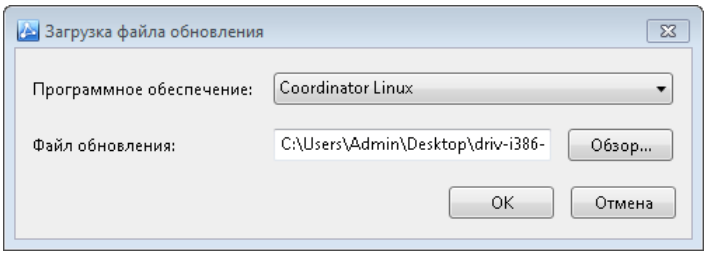

Рисунок 46. Загрузка файла обновления ПО

Таблица 5. Особенности отправки обновлений ПО ViPNet на сетевые узлы

ПО ViPNet на узле	Тип ПО ViPNet в списке	Особенности обновления ПО
ViPNet Деловая почта версии 3.x	**Деловая почта 3.x**	При отправке обновления программного обеспечения на узлы, на которых установлена только программа ViPNet Деловая почта версии 3.x, в окне **Загрузка файла обновления** в качестве типа программного обеспечения укажите **Деловая почта 3.x**.
ViPNet Client или ViPNet Coordinator версии 3.x без компонента «Контроль приложений»	**Client без реверс-firewall** или **Coordinator без реверс-firewall**	• Используйте файлы обновления `driv_fsn.lzh` или `driv_csn.lzh` соответственно. • При отправке обновления ПО ViPNet Client или ViPNet Coordinator версии 4.5 на сетевой узел, на котором установлено ПО ViPNet SafeDisk-V или ОС Windows 10, обновление не будет установлено.
ViPNet Client или ViPNet Coordinator (обновление версии 3.x всех компонентов или версии 4.x)	**Client с реверс-firewall** или **Coordinator с реверс-firewall**	• Используйте файлы `driv_fsa.lzh` или `driv_csa.lzh` соответственно. • При отправке обновления ПО ViPNet Client или ViPNet Coordinator версии 4.5 на сетевой узел, на котором установлено ПО ViPNet SafeDisk-V или ОС Windows 10, обновление не будет установлено.
ПО ViPNet xFirewall	**xF100** **xF1000** **xF2000** **xF5000**	Обновление ПО на узлах ПАК ViPNet xFirewall, включая обновление модуля DPI (см. глоссарий, стр. 305).
Обновление версии только модуля DPI на узлах ПАК ViPNet xFirewall	**xF100 DPI** **xF1000 DPI** **xF2000 DPI** **xF5000 DPI**	• Чтобы поддерживать актуальный набор приложений и протоколов, которые используются при создании фильтров содержимого трафика (см. глоссарий, стр. 309), обновите версию только для модуля DPI. Например, для ПАК ViPNet xFirewall xF100 выберите **xF100 DPI**. • Чтобы в ПО ViPNet Policy Manager иметь возможность создавать фильтры содержимого трафика, необходимо хотя бы один раз отправить обновление версии модуля DPI или ПО ViPNet xFirewall.

Перед загрузкой будет выполнена проверка файла на соответствие выбранному типу программного обеспечения (на основании содержимого файла либо маски его имени, если не удается проверить соответствие по содержимому файла). Если будет обнаружено несоответствие, появится окно с предупреждением. В этом случае рекомендуется отказаться от загрузки файла, нажав в окне предупреждения кнопку **Закрыть**.

Примечание. Убедитесь, что путь к файлу обновления не содержит кириллических символов. В противном случае появится сообщение о повреждении файла обновления.

- Загруженный файл появится в списке. В столбце **Версия обновления** будет отображена версия программного обеспечения, содержащегося в загруженном файле.

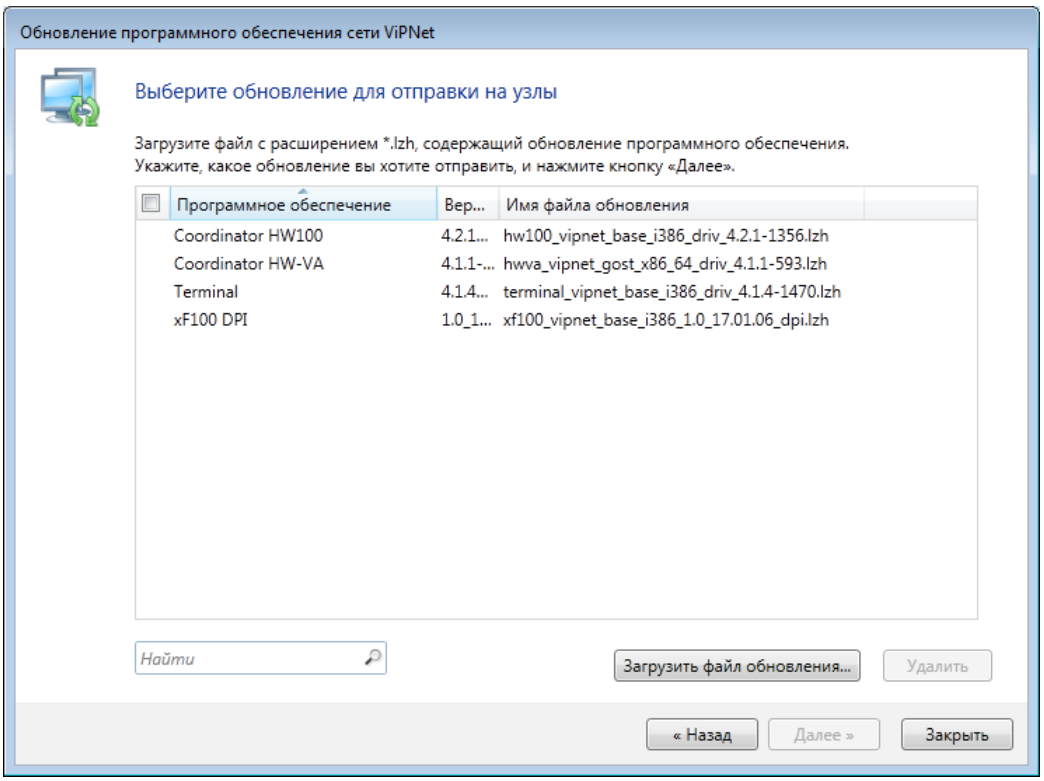

Рисунок 47. Загрузка и выбор обновлений ПО

Примечание. Вы можете удалить из базы данных файлы обновления, которые больше не нужны. Для этого выберите в списке один или несколько файлов и нажмите кнопку **Удалить**.

4 Выберите в списке программное обеспечение, которое требуется обновить, и нажмите кнопку **Далее**.

5 На странице **Укажите сетевые узлы для обновления программного обеспечения** выберите в списке узлы, на которые требуется отправить обновление.

Если обновление выбранного программного обеспечения отправляется впервые, в списке отображаются все клиенты или координаторы, в зависимости от типа обновления. При

последующей отправке обновлений выбранного типа в списке отображаются сетевые узлы, на которые данный тип обновления отправлялся ранее.

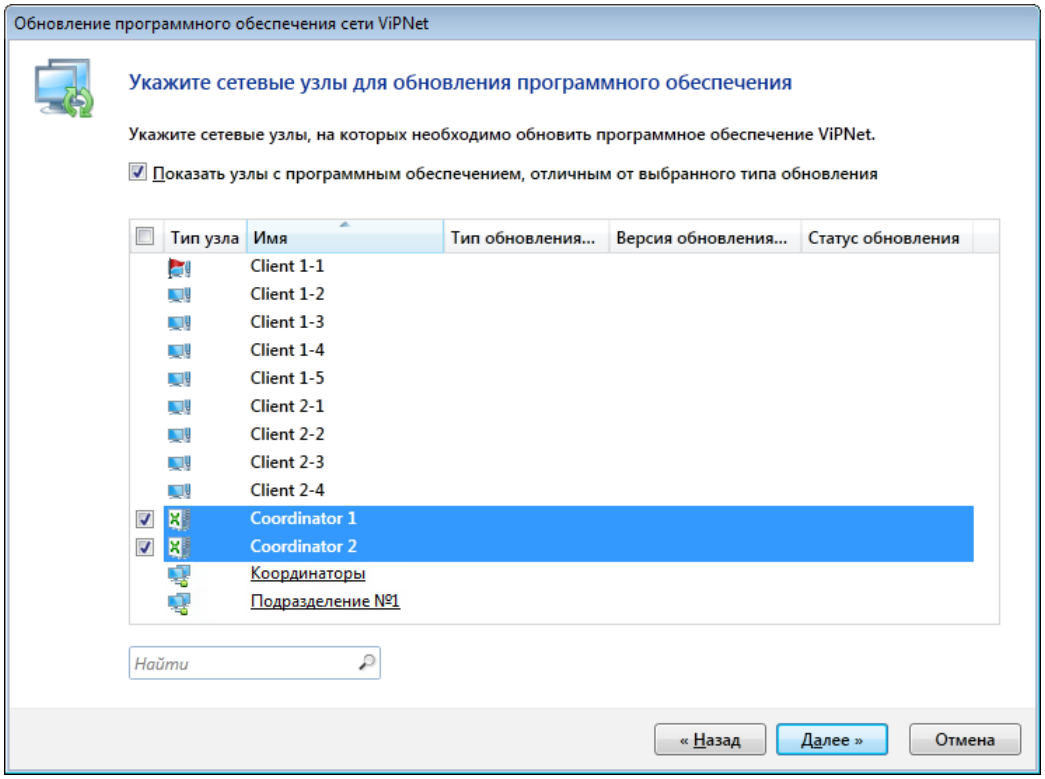

Рисунок 48. Выбор сетевых узлов для обновления ПО

Чтобы указать сетевые узлы для обновления, выполните следующие действия:

- Если вы хотите отправить выбранное обновление программного обеспечения на сетевые узлы, которые не отображены в списке, установите флажок **Показать узлы с программным обеспечением, отличным от выбранного типа обновления** и в окне подтверждения нажмите кнопку **Да**. В списке будут отображены все узлы сети ViPNet.
- Для поиска сетевых узлов по именам введите часть имени узла в строку поиска, расположенную внизу окна.
- Выберите в списке один или несколько сетевых узлов либо группу или несколько групп узлов, на которые требуется отправить обновление. Вы можете выбрать сразу все сетевые узлы с помощью флажка, расположенного в заголовке списка. При выборе группы узлов обновление будет отправлено только тем узлам из группы, которым оно подходит по типу.
- Нажмите кнопку **Далее**.

6 На странице **Вступление обновления в действие** выполните следующие действия:

- Если требуется, измените дату и время применения обновления на сетевых узлах. Дату можно выбрать с помощью календаря, нажав кнопку . По умолчанию заданы текущие дата и время.
- Если вы хотите, чтобы после обновления программного обеспечения была выполнена перезагрузка компьютеров с ОС Windows, установите соответствующий флажок.

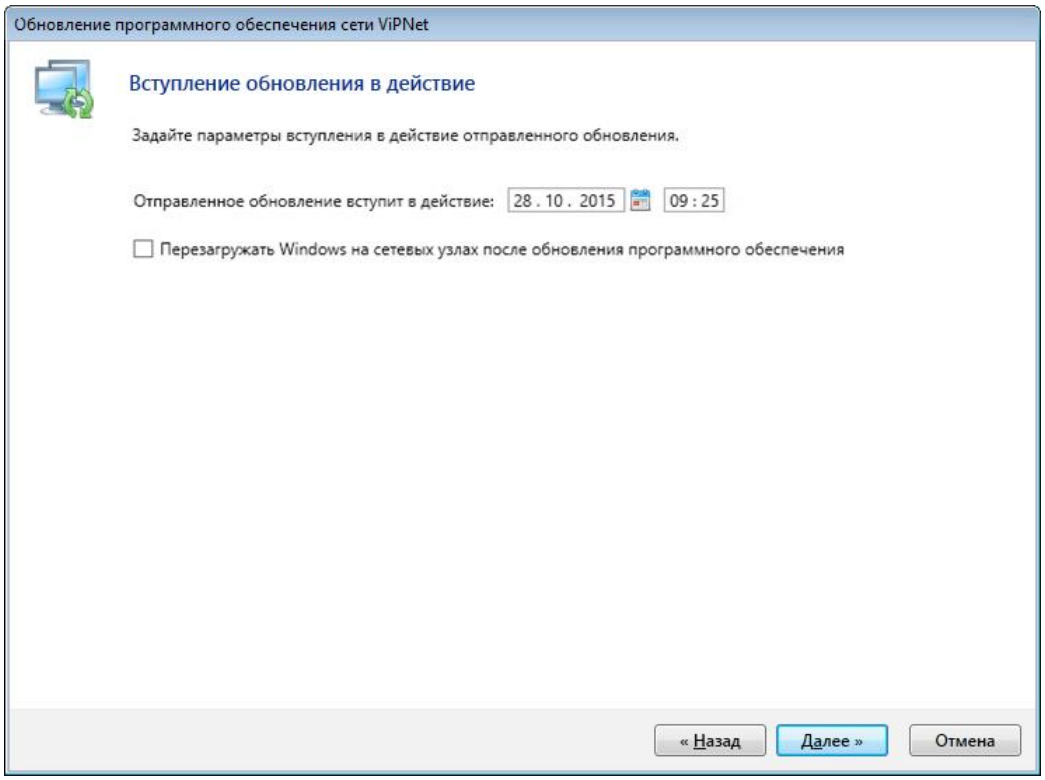

Рисунок 49. Дата и время вступления в действие обновления ПО

Затем нажмите кнопку **Далее**.

7 На странице **Подготовка к обновлению программного обеспечения завершена** нажмите кнопку **Далее**.

8 На странице **Отправка обновления программного обеспечения** с помощью индикатора выполнения будет отображен процесс отправки. Для просмотра подробного отчета щелкните ссылку **Показать информацию о ходе процесса**.

9 По окончании процесса отправки обновления будет отображена информация о результатах отправки программного обеспечения. Для завершения работы мастера нажмите кнопку **Готово**.

Примечание. Процесс обновления программного обеспечения будет полностью завершен после применения обновления на всех выбранных сетевых узлах.

Подробный отчет об отправке обновлений и их статусе можно просмотреть в журнале транспортных конвертов (см. «Журналы транспортных конвертов» на стр. 102).

Информация о приеме обновлений программного обеспечения ViPNet на сетевых узлах содержится в документации соответствующих продуктов.

Резервное копирование и восстановление данных

Данные о структуре сети ViPNet, параметрах сетевых объектов и настройках, сделанных в программе ViPNet Центр управления сетью, а также данные программы ViPNet Удостоверяющий и ключевой центр (см. «Взаимодействие с программой ViPNet Удостоверяющий и ключевой центр» на стр. 25) хранятся в одной базе данных SQL. Вы можете создать резервную копию этой базы данных, чтобы при необходимости вернуться к более ранней конфигурации сети.

Создание резервной копии и восстановление данных ЦУСа и УКЦ осуществляется с помощью программы ViPNet Удостоверяющий и ключевой центр. Во время операций по резервному копированию и восстановлению данных в программе ViPNet Центр управления сетью будут заблокированы любые действия.

Создание резервной копии данных в программе ViPNet Удостоверяющий и ключевой центр может производится автоматически с заданной периодичностью (рекомендуется) либо вручную с использованием мастера. Для восстановления данных из резервной копии в программе ViPNet Удостоверяющий и ключевой мастер в меню **Сервис** выберите пункт **Восстановление конфигурации** и следуйте указаниям мастера. Подробнее создание и восстановлении резервных копий описано в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», в главе «Административные функции».

Внимание! Если выполняется восстановление данных из резервной копии, созданной в программе ViPNet Удостоверяющий и ключевой центр версии 4.3 и ниже, то после завершения процедуры восстановления также необходимо обновить версию базы данных SQL. Для этого запустите установочный файл серверного приложения ViPNet Центр управления сетью и в окне **Изменение установленных компонентов** выберите пункт **Восстановить**.

Просмотр журналов

В программе ViPNet Центр управления сетью в журналах фиксируются два типа событий:

- Изменение администратором параметров программы ViPNet Центр управления сетью, свойств сети ViPNet и ее объектов.
- Обмен управляющими транспортными конвертами с узлами сети ViPNet.

Журналы аудита

В журналы аудита записывается информация о действиях, которые выполняют администраторы в процессе управления сетью ViPNet. В программе ViPNet Центр управления сетью вы можете просматривать несколько журналов, которые содержат информацию о различных группах событий: изменение настроек программы ViPNet Центр управления сетью, изменение свойств объектов сети, вход и выход администраторов из программы и так далее. По умолчанию записи о событиях хранятся в журналах аудита 60 дней, при необходимости вы можете изменить это время в меню **Сервис** > **Параметры** (см. «Параметры журналов» на стр. 81).

Для просмотра журнала аудита выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью выберите представление **Администрирование**.

2 На панели навигации выберите раздел **Журналы аудита**.

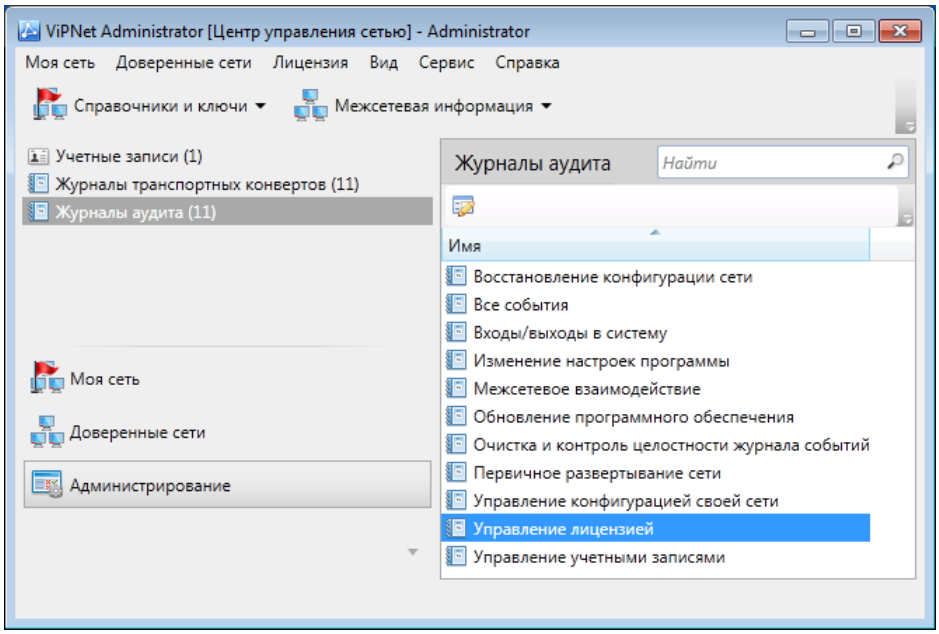

Рисунок 50. Список журналов аудита

3 На панели просмотра двойным щелчком откройте журнал, который соответствует нужной группе событий. Откроется окно просмотра журнала.

По умолчанию в окне просмотра представлены записи обо всех событиях выбранной группы, произошедших за последние сутки.

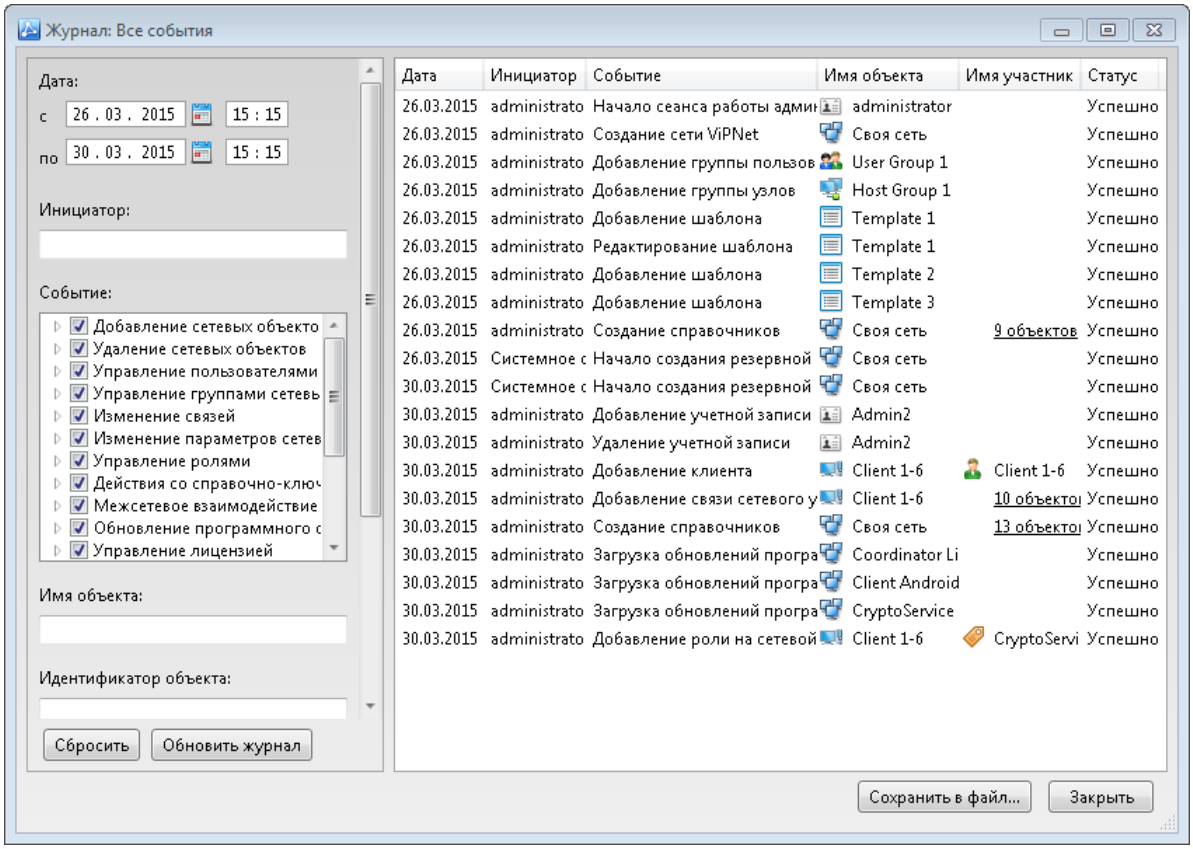

Рисунок 51. Просмотр журнала аудита

4 Задайте параметры поиска записей в журнале:

- Чтобы найти записи о событиях, которые произошли в определенный период времени, под заголовком **Дата** в соответствующих полях укажите начало и конец нужного периода времени.
- Чтобы найти записи о действиях определенного администратора программы ViPNet Центр управления сетью, в поле **Инициатор** введите имя учетной записи администратора.
- Чтобы найти записи о событиях определенного типа, в списке **Событие** разверните нужную группу событий (названия групп соответствуют названиям доступных журналов аудита) и установите или снимите флажки напротив типов событий.
- Чтобы найти записи событиях, в которых был задействован некоторый основной объект сети ViPNet (например, основным объектом может быть сетевой узел, на который добавлена роль), введите имя объекта или его идентификатор (либо часть имени или идентификатора) в соответствующее поле: **Имя объекта** или **Идентификатор объекта**.
- Чтобы найти записи о событиях, в которых был задействован некоторый второстепенный объект (например, второстепенным объектом может быть роль, добавленная на сетевой узел), введите имя или идентификатор второстепенного объекта в соответствующее поле: **Имя участника** или **Идентификатор участника**.

- Чтобы найти записи о событиях, завершившихся успешно либо с ошибкой, в списке **Статус** выберите нужное значение.

5 Чтобы вернуть параметры поиска по умолчанию, нажмите кнопку **Сбросить**.

6 Для поиска в журнале записей в соответствии с заданными параметрами нажмите кнопку **Обновить журнал**. В списке будут представлены записи, которые соответствуют одновременно всем заданным параметрам.

7 Во время просмотра списка событий в журнале вы можете использовать следующие возможности:

- Чтобы сортировать список по какому-либо параметру, щелкните заголовок соответствующего столбца.
- Чтобы скрыть или отобразить столбцы, щелкните правой кнопкой мыши заголовок любого столбца и в меню выберите нужный параметр.
- Если в событии задействованы несколько однотипных объектов, в списке событий будет указано количество этих объектов. Чтобы просмотреть имена объектов, щелкните ссылку **<количество> объектов**.
- Чтобы сохранить отображаемый список записей журнала в файл формата CSV, нажмите кнопку **Сохранить в файл**. Затем в окне **Сохранить как** укажите папку и имя файла для сохранения журнала.

Журналы транспортных конвертов

При осуществлении функций по управлению сетью ViPNet сетевой узел с серверным приложением ViPNet Центр управления сетью обменивается с другими узлами управляющими конвертами (см. глоссарий, стр. 308) с помощью транспортного модуля ViPNet MFTP. Эти конверты могут содержать справочники, ключи и программное обеспечение для сетевых узлов, запросы на издание сертификатов, квитанции, подтверждающие прием обновлений на сетевых узлах, и так далее.

Информация обо всех транспортных конвертах, отправленных и принятых Центром управления сетью, заносится в специальные журналы. Записи в журнале фиксируют изменение статуса конвертов: **Отправлено**, **Доставлено**, **Принят** и так далее.

В программе ViPNet Центр управления сетью вы можете просматривать несколько журналов, которые содержат информацию об отправке и приеме различных типов данных: справочников и ключей, межсетевой информации, запросов на сертификаты и так далее.

Для просмотра журнала транспортных конвертов выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью выберите представление **Администрирование**.

2 На панели навигации выберите раздел **Журналы транспортных конвертов**.

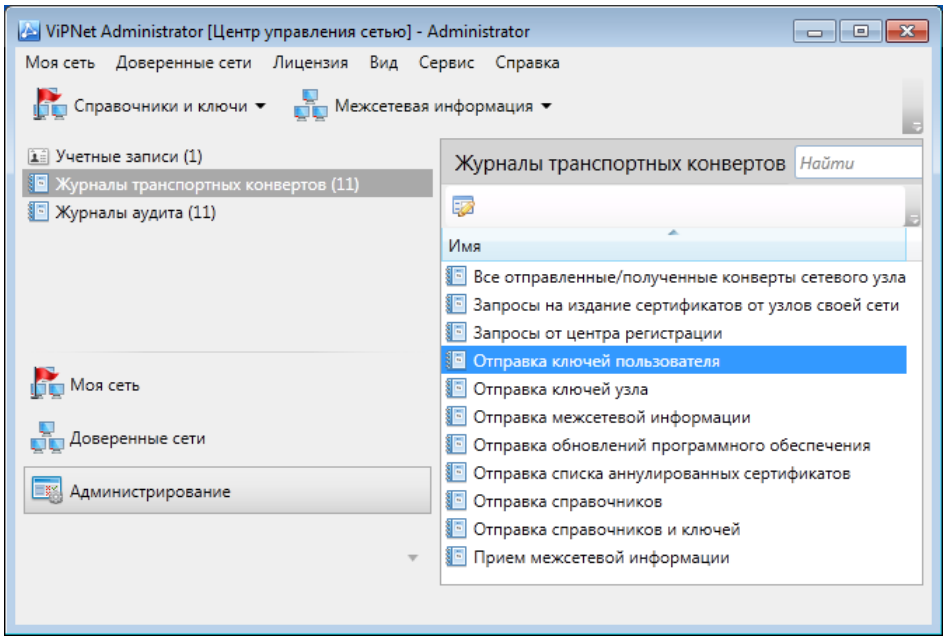

Рисунок 52. Журналы транспортных конвертов

3 На панели просмотра двойным щелчком откройте нужный журнал. Откроется окно просмотра журнала.

По умолчанию в окне просмотра представлены все записи о событиях, произошедших за последние три дня и относящихся к отправке и приему данных выбранного типа.

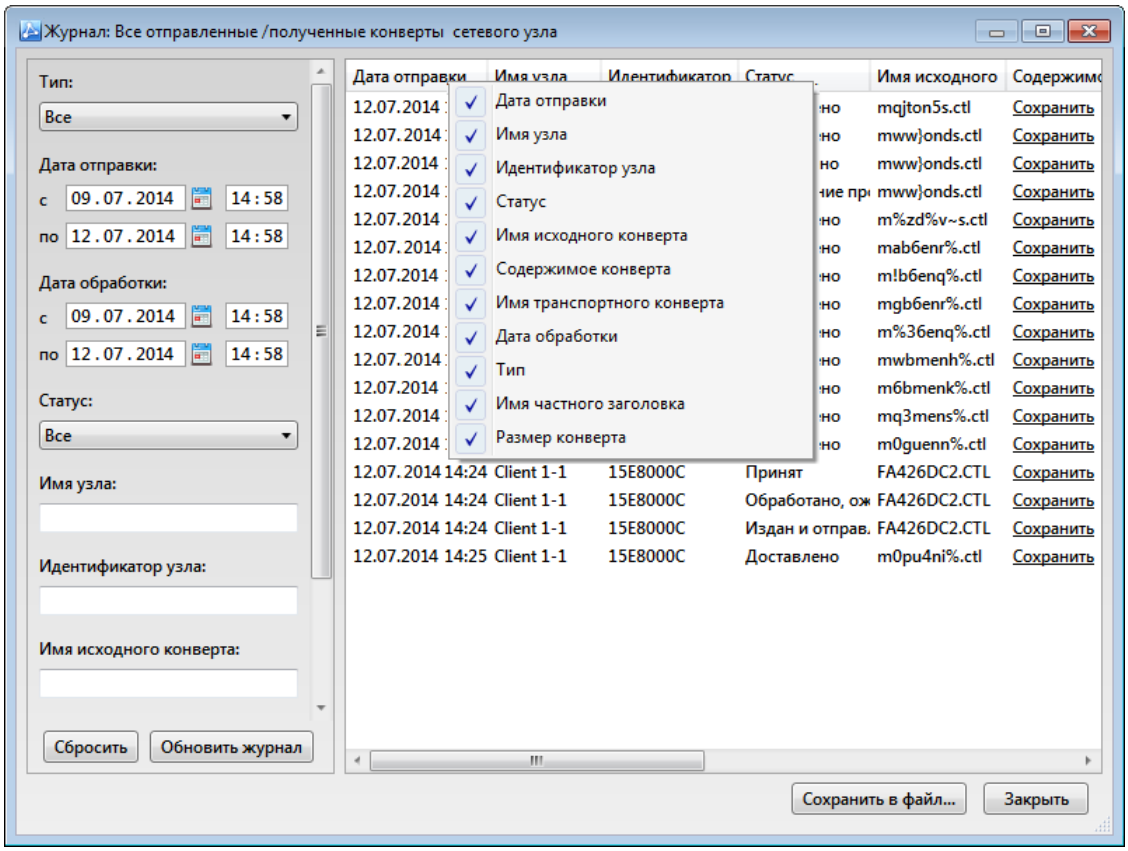

Рисунок 53. Просмотр журнала транспортных конвертов

4 Задайте параметры поиска записей в журнале:

- Чтобы найти записи о конвертах определенного типа, в списке **Тип** выберите нужное значение.

Примечание. Список **Тип** доступен при просмотре журналов **Отправка справочников и ключей**, **Запросы от центра регистрации**, **Все отправленные/полученные конверты сетевого узла**.

- Чтобы найти записи о конвертах, отправленных в определенное время, под заголовком **Дата отправки** в соответствующих полях укажите промежуток времени отправки конвертов. По умолчанию заданы предыдущие два дня.
- Чтобы найти записи о конвертах, которые были обработаны в определенное время, под заголовком **Дата обработки** в соответствующих полях укажите промежуток времени обработки. По умолчанию заданы предыдущие два дня.
- Чтобы найти записи об определенном статусе конвертов, в списке **Статус** выберите нужное значение.
- Чтобы найти записи по имени или идентификатору сетевого узла, с которым Центр управления сетью обменивался конвертами, в соответствующее поле введите имя или идентификатор узла или их часть.
- Чтобы найти записи по имени исходного или транспортного конверта, в соответствующее поле введите имя конверта или часть имени.
- Чтобы найти записи о конвертах, которые содержат какие-либо данные (обновления, запросы), или квитанции (подтверждения доставки, применения обновлений и так далее), в списке **Содержимое конверта** выберите нужное значение.

5 Чтобы вернуть параметры поиска по умолчанию, нажмите кнопку **Сбросить**.

6 Для поиска в журнале записей в соответствии с заданными параметрами нажмите кнопку **Обновить журнал**. В списке будут представлены записи, которые соответствуют одновременно всем заданным параметрам.

7 Во время просмотра списка событий в журнале вы можете использовать следующие возможности:

- Чтобы сортировать список по какому-либо параметру, щелкните заголовок соответствующего столбца.
- Чтобы скрыть или отобразить столбцы, щелкните правой кнопкой мыши заголовок любого столбца и в меню выберите нужный параметр.
- Чтобы сохранить содержимое какого-либо конверта на диск, в столбце **Содержимое конверта** щелкните ссылку **Сохранить**. Затем в окне **Обзор папок** укажите папку для сохранения файлов, содержащихся в конверте.

Внимание! Содержимое конверта может использоваться только для анализа. Использовать содержимое конвертов для других целей, в том числе для загрузки на

сетевой узел, настоятельно не рекомендуется.

- Чтобы сохранить отображаемый список записей журнала в файл формата CSV, нажмите кнопку **Сохранить в файл**. Затем в окне **Сохранить как** укажите папку и имя файла для сохранения журнала.

Работа с лицензией

В данном разделе описываются возможные операции с лицензией для вашей сети ViPNet (см. «Лицензия на сеть ViPNet» на стр. 23). Сведения о работе с общей лицензией для иерархической системы сетей ViPNet содержатся в главе Иерархическая система сетей ViPNet (на стр. 220).

Просмотр сведений о лицензии для своей сети

Для просмотра информации о лицензионных ограничениях на вашу сеть ViPNet и об использовании лицензии выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню **Лицензия** выберите пункт **Сведения о лицензии для своей сети**. Откроется окно **Сведения о лицензии для своей сети**.
2. На вкладке **Общая информация** просмотрите следующие сведения:
   - Номер вашей сети и имя владельца сети.
   - Номер головной сети, номера подчиненных сетей — если ваша сеть является частью иерархической системы сетей ViPNet (см. «Иерархическая система сетей ViPNet» на стр. 220).
   - Срок действия лицензии на вашу сеть и на использование программного комплекса ViPNet StateWatcher.
   - Максимальная версия программного обеспечения ViPNet, которая может использоваться в вашей сети.

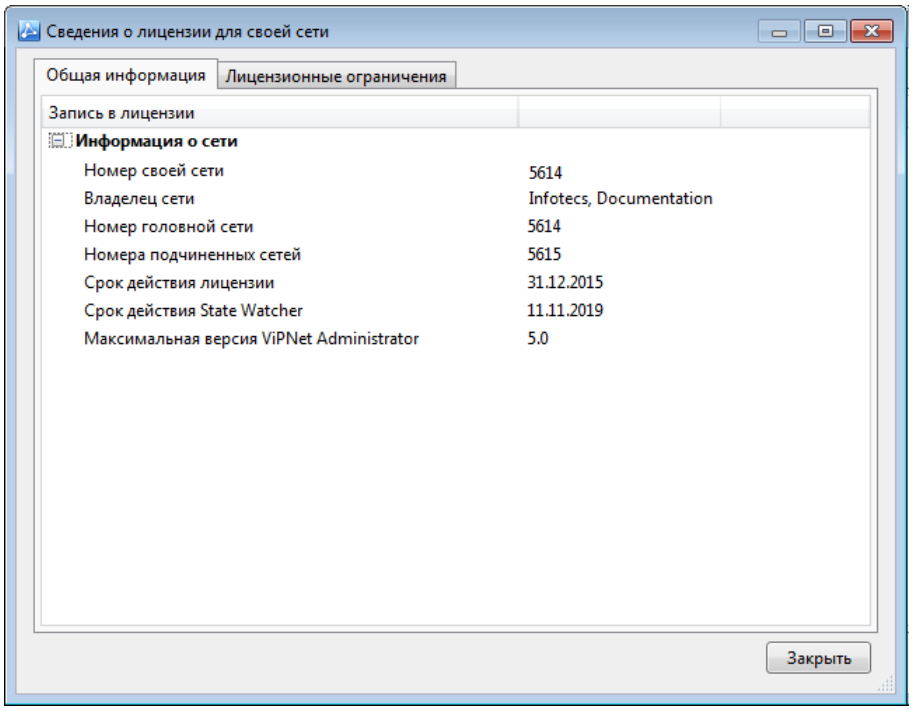

Рисунок 54. Общая информация о лицензии на сеть ViPNet

Примечание. В случае использования файла лицензии `infotecs.reg`, в окне **Сведения об общей лицензии** на вкладке **Общая информация** также можно просмотреть контактные данные поставщика лицензии.

3 На вкладке **Лицензионные ограничения** ознакомьтесь с ограничениями на структуру вашей сети ViPNet. Список ограничений разбит на три части:

- **Параметры удостоверяющего центра**. В столбце **Лицензионное ограничение** указаны возможность использования функциональности удостоверяющего центра и максимальное количество сертификатов внешних пользователей или пользователей ViPNet, которое может быть издано в УКЦ вашей сети, в столбце **Свободно лицензий** — число сертификатов, которое еще разрешает издать ваша лицензия.

  Примечание. Если в столбце **Лицензионное ограничение** для функциональности удостоверяющего центра указано значение 0, это означает, что в программе ViPNet Удостоверяющий и ключевой центр вашей сети функции удостоверяющего центра недоступны.

- **Параметры работы узлов**. Здесь перечислены дополнительные параметры некоторых ролей. Например, число элементов кластера в роли «Cluster Windows». В столбце **Лицензионное ограничение** указано максимальное суммарное значение определенного параметра, в столбце **Свободно лицензий** — число, на которое можно увеличить текущее значение параметра.
- **Максимальное число узлов, на которые могут быть добавлены роли.** Здесь перечислены роли узлов, а также их варианты с дополнительными ограничениями, которые могут быть

использованы в вашей сети ViPNet. В столбце **Лицензионное ограничение** указано максимальное количество узлов в определенной роли, в столбце **Свободно лицензий** — количество узлов, на которые может быть добавлена роль при текущей структуре сети.

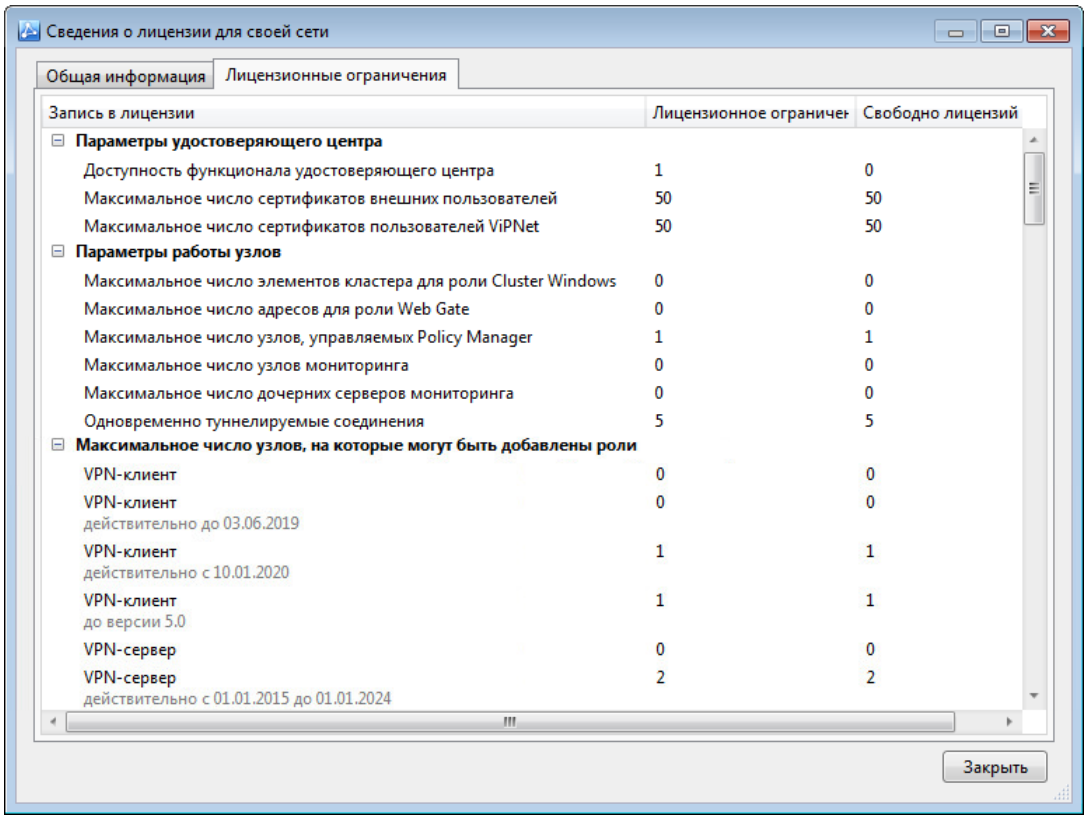

Рисунок 55. Информация о лицензионных ограничениях

4 Получив необходимую информацию, нажмите кнопку **Закрыть**.

Обновление лицензии

Если вам требуется изменить параметры лицензии на вашу сеть ViPNet (например, использовать дополнительные роли), обновите файл лицензии `*.itcslic` или `infotecs.reg` (см. «Лицензия на сеть ViPNet» на стр. 23). Для этого обратитесь за расширением лицензии к представителю ОАО «ИнфоТеКС», сообщив желаемые параметры новой лицензии и номер вашей сети ViPNet.

Примечание. Чтобы узнать номер вашей сети, в программе ViPNet Центр управления сетью в меню **Справка** выберите пункт **О программе**.

После того как ваша заявка на расширение лицензии будет удовлетворена, вы получите новый лицензионный файл `*.itcslic` или `infotecs.reg`. Чтобы загрузить новый лицензионный файл в программу ViPNet Центр управления сетью, выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Лицензия** выберите пункт **Обновить лицензию**.

2 В окне **Обновление лицензии** нажмите кнопку **Обзор** и укажите путь к новому файлу `*.itcslic` или `infotecs.reg`.

Внимание! После того как вы загрузите лицензию из файла `*.itcslic`, загрузить последующие обновления лицензии из файла старого формата `infotecs.reg` будет невозможно.

В группе **Сведения о лицензии** будет отображена общая информация о выбранном файле лицензии.

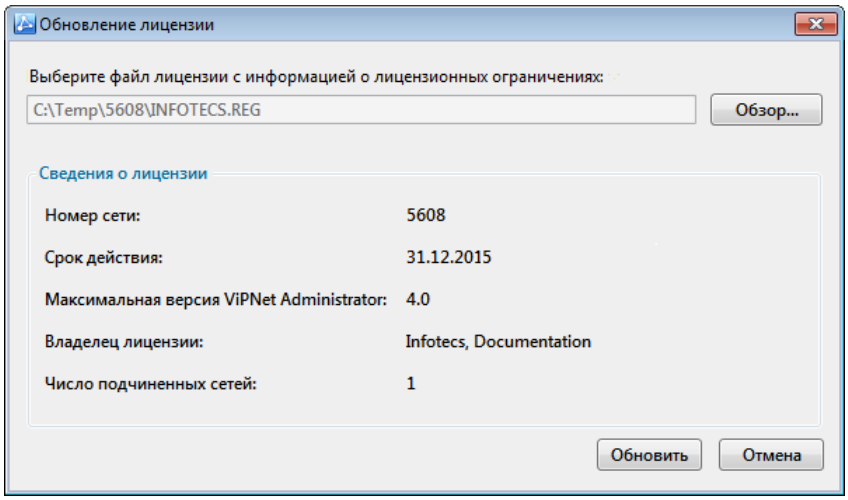

Рисунок 56. Загрузка нового файла лицензии

Если указанный файл лицензии поврежден или предназначен для сети с другим номером, появится соответствующее сообщение. Загрузка такого файла лицензии невозможна.

3 Указав новый файл лицензии, нажмите кнопку **Обновить**. После успешного обновления лицензии появится соответствующее сообщение.

Информация о новой лицензии будет загружена в базу данных SQL, откуда эта информация может быть запрошена программой ViPNet Удостоверяющий и ключевой центр (см. глоссарий, стр. 300).

Примечание. Если обновление лицензии добавляет функциональность удостоверяющего центра, для завершения обновления перезагрузите программу ViPNet Удостоверяющий и ключевой центр.

4 Если вы загрузили лицензию с поддержкой иерархической системы сетей ViPNet в главном Центре управления сетью, распределите лицензионные ограничения для подчиненных сетей (см. «Распределение общей лицензии между сетями» на стр. 225).

5 Сформируйте справочники и отправьте их на все узлы сети. В составе справочников будет передан новый файл лицензии.

Создание отчетов о лицензии на сеть

В программе ViPNet Центр управления сетью вы можете формировать и сохранять в файлы следующие отчеты о лицензии на сеть ViPNet:

- Отчет о лицензионных ограничениях, в котором содержатся сведения об общем количестве лицензий на различные компоненты сети ViPNet, а также о количестве свободных и использованных лицензий на эти компоненты.
- Отчет о распределении лицензионных ограничений, в котором содержатся сведения о том, сколько лицензий на различные компоненты сети используется в главной и подчиненных сетях ViPNet. Создание данного типа отчетов доступно, только если в вашей организации развернута иерархическая система сетей ViPNet (на стр. 220).

Чтобы сохранить файл с отчетом о лицензионных ограничениях или о распределении лицензионных ограничений между своей и подчиненными сетями ViPNet, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью в меню **Лицензия** выберите один из пунктов в зависимости от типа отчета, который вы хотите сохранить:
   - **Сохранить отчет о лицензии своей сети в файл** — для сохранения отчета о лицензионных ограничениях своей сети.
   - **Сохранить отчет о распределении лицензий в файл** — для сохранения отчета о распределении лицензионных ограничений между своей и подчиненными сетями ViPNet. Данный пункт доступен в программе ViPNet Центр управления сетью только на сетевом узле администратора головной сети ViPNet.
2. В открывшемся окне задайте расположение и имя сохраняемого файла.
3. Нажмите кнопку **Сохранить**.

В результате файл отчета выбранного типа в формате CSV будет сохранен в указанной папке. Теперь вы можете просмотреть его, распечатать на принтере или использовать в другой программе.

4

Настройка параметров сетевых узлов

Создание сетевого узла 112

Удаление сетевого узла 116

Настройка параметров координатора 118

Настройка параметров клиента 128

Изменение списка пользователей сетевого узла 136

Изменение связей между сетевыми узлами 138

Добавление ролей на сетевые узлы 142

Настройка защищенных DNS-серверов 168

Задание адресов сетевого узла 175

Настройка параметров подключения к внешней сети 178

Изменение списка групп, в которые входит сетевой узел 189

Работа с шаблонами сетевых узлов 191

Работа с группами узлов 196

Создание сетевого узла

Добавление координатора

Координатор может работать в одном из двух режимов — с включенными или отключенными функциями VPN-сервера. Координатор, не выполняющий функций VPN-сервера, не имеет клиентов и не участвует в рассылке служебной информации о сетевых узлах и транспортных конвертов, поэтому он создает меньшую нагрузку на вычислительные ресурсы по сравнению с координатором, который выполняет функции VPN-сервера. Координатор без функций VPN-сервера вы можете использовать в качестве межсетевого экрана, защищенного интернет-шлюза и туннелирующего сервера (VPN-шлюза).

Если вам нужен координатор, на котором вы сможете регистрировать клиенты, создайте координатор с функциями VPN-сервера.

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 .

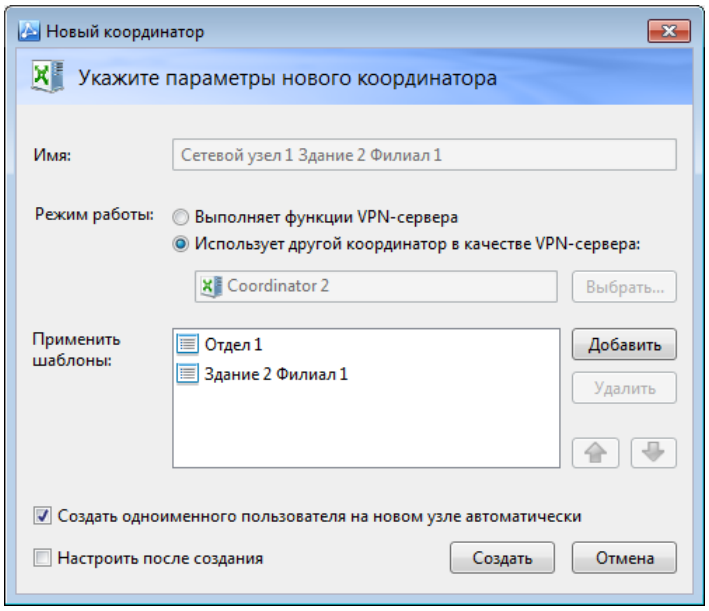

Рисунок 57. Добавление нового координатора

4 В окне **Новый координатор** выполните следующие действия:

4.1 В соответствующее поле введите имя создаваемого координатора.

4.2 Установите переключатель **Режим работы** в одно из положений:

4.2.1 Чтобы создать координатор, на котором можно регистрировать клиенты (или координаторы без функций VPN-сервера), установите переключатель в положение **Выполняет функции VPN-сервера**.

4.2.2 Чтобы уменьшить нагрузку на вычислительные ресурсы координатора, установите переключатель в положение **Использует другой координатор в качестве VPN-сервера**. Выберите координатор, который будет выполнять функции VPN-сервера, для этого нажмите соответствующую кнопку и в появившемся окне выберите координатор.

4.3 При необходимости добавьте один или несколько шаблонов, на основе которых будут заданы свойства координатора. Для этого нажмите кнопку **Добавить** и в открывшемся окне выберите нужные шаблоны.

Если в шаблоне были указаны имя или координатор узла (см. «Настройка шаблона сетевых узлов» на стр. 192), то соответствующие поля будут неактивными для изменения.

4.4 Если в шаблонах указаны пересекающиеся настройки, задайте приоритет шаблонов, установив их положение в списке с помощью стрелок  и  .

4.5 Чтобы одновременно с координатором создать для него пользователя, установите флажок **Создать одноименного пользователя на новом узле автоматически**.

Если в настройках программы были заданы соответствующие параметры создания узлов (см. «Параметры работы с объектами сети» на стр. 75), этот флажок установлен по умолчанию.

4.6 Чтобы после создания координатора открыть окно для его настройки, установите флажок **Настроить после создания** (по умолчанию снят).

4.7 Нажмите кнопку **Создать**.

В списке **Координаторы** появится новый координатор. Если было выбрано автоматическое создание пользователя, в список **Пользователи** будет добавлен одноименный пользователь.

5 Если требуется, настройте параметры созданного координатора (см. «Настройка параметров координатора» на стр. 118).

6 После создания координатора и других объектов, а также выполнения необходимых настроек сформируйте справочники. Для этого на панели инструментов нажмите кнопку **Справочники и ключи**  и выберите пункт **Создать справочники**.

В программе ViPNet Удостоверяющий и ключевой центр для нового координатора и связанных с ним объектов создайте дистрибутивы ключей, которые затем следует установить на сетевых узлах. Информация о работе в Удостоверяющем и ключевом центре содержится в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Добавление клиента

Чтобы добавить в сеть ViPNet новый клиент, 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 .

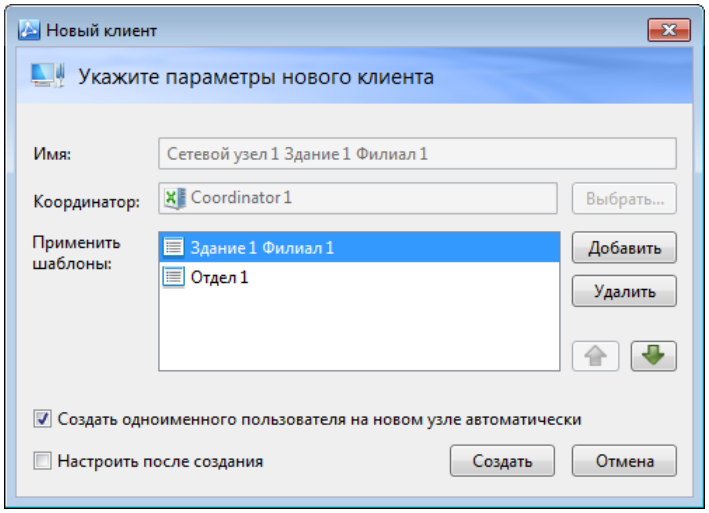

Рисунок 58. Добавление нового клиента

4 В окне **Новый клиент** выполните следующие действия:

4.1 В соответствующее поле введите имя создаваемого клиента.

4.2 В поле **Координатор** с помощью кнопки **Выбрать** укажите координатор, на котором требуется зарегистрировать новый клиент.

Примечание. Выбранный координатор будет выполнять функцию транспортного сервера для клиента.

4.3 При необходимости добавьте один или несколько шаблонов, на основе которых будут заданы свойства клиента (см. «Работа с шаблонами сетевых узлов» на стр. 191). Для этого нажмите кнопку **Добавить** и в открывшемся окне выберите нужные шаблоны.

Если в шаблоне были указаны имя или координатор узла (см. «Настройка шаблона сетевых узлов» на стр. 192), то соответствующие поля будут неактивными для изменения.

4.4 Если в шаблонах указаны пересекающиеся настройки, задайте приоритет шаблонов, установив их положение в списке с помощью стрелок и .

4.5 Чтобы одновременно с клиентом создать для него пользователя, установите флажок **Создать одноименного пользователя на новом узле автоматически**.

Если в настройках программы были заданы соответствующие параметры создания узлов (см. «Параметры работы с объектами сети» на стр. 75), этот флажок установлен по умолчанию.

4.6 Чтобы после создания клиента открыть окно для его настройки, установите флажок **Настроить после создания** (по умолчанию снят).

4.7 Нажмите кнопку **Создать**. В списке **Клиенты** появится новый клиент. Если было выбрано автоматическое создание пользователя, в список **Пользователи** будет добавлен одноименный пользователь.

Примечание. При создании самого первого клиента в сети он автоматически назначается Центром управления сетью. В списке **Клиенты** такой узел помечается значком .

На этом узле должно быть установлено серверное приложение ViPNet Центр управления сетью. Предупреждение об этом будет отображено в нижней части окна **Новый клиент**.

---

5 Если требуется, настройте параметры созданного клиента (см. «Настройка параметров клиента» на стр. 128).

6 После создания клиента и других объектов, а также выполнения необходимых настроек сформируйте справочники. Для этого на панели инструментов нажмите кнопку **Справочники и ключи** и выберите пункт **Создать справочники**.

В программе ViPNet Удостоверяющий и ключевой центр для нового клиента и связанных с ним объектов создайте дистрибутивы ключей, который затем следует установить на сетевых узлах. Информация о работе в Удостоверяющем и ключевом центре содержится в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Удаление сетевого узла

Удаление координатора

Чтобы удалить координатор из сети ViPNet, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы**.

3 На панели просмотра выберите в списке один или несколько сетевых узлов и выполните одно из следующих действий:

- Нажмите кнопку  на панели инструментов.
- В контекстном меню узлов выберите пункт **Удалить**.

Внимание! Вместе с координатором будут удалены все клиенты, зарегистрированные на данном координаторе.

Невозможно удалить координатор, на котором зарегистрирован узел Центра управления сетью, отмеченный значком  , шлюзовой координатор (см. глоссарий, стр. 309) и сам Центр управления сетью. При попытке удалить такой координатор будут удалены все зарегистрированные на нем клиенты, кроме ЦУСа.

---

4 Если какие-либо из выбранных координаторов и их клиентов имеют по одному пользователю и этих пользователей требуется удалить вместе с сетевыми узлами, в окне **Удаление координаторов** установите флажок **Удалить пользователей, зарегистрированных только на удаляемых сетевых узлах**.

Этот флажок установлен по умолчанию, если были заданы соответствующие параметры для удаляемых узлов (см. «Параметры работы с объектами сети» на стр. 75).

5 В окне **Удаление координаторов** нажмите кнопку **Удалить координаторы**. Выбранные координаторы и зарегистрированные на них клиенты будут удалены из сети ViPNet.

6 Если удаляемый координатор используется в качестве сервера IP-адресов или межсетевого экрана, появится соответствующее предупреждение.

Для удаления координатора в окне предупреждения нажмите кнопку **Да**. В этом случае параметры сетевых узлов, использовавших удаленный координатор, будут автоматически изменены следующим образом:

- В настройках адресации клиента во внешних сетях удаленный координатор будет заменен координатором, на котором зарегистрирован данный клиент.
- В настройках подключения защищенных узлов к внешней сети не будет задан координатор, выполняющий функцию межсетевого экрана.

7 После удаления координаторов создайте справочники и ключи и отправьте их на узлы своей сети (см. «Отправка справочников и ключей» на стр. 91). Если требуется, отправьте

межсетевую информацию в доверенные сети (см. «Отправка межсетевой информации» на стр. 251).

Удаление клиента

Чтобы удалить клиент из сети ViPNet, выполните следующие действия:

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

2 На панели навигации выберите раздел **Клиенты**.

3 На панели просмотра выберите в списке один или несколько сетевых узлов и выполните одно из действий:

- Нажмите кнопку  на панели инструментов.
- В контекстном меню узлов выберите пункт **Удалить**.

Примечание. Центр управления сетью, то есть клиент, на котором установлено серверное приложение ViPNet Центр управления сетью, удалить нельзя. Этот клиент помечен в списке значком  . При попытке удалить Центр управления сетью появится соответствующее сообщение.

---

4 Если какие-либо из выбранных клиентов имеют по одному пользователю и этих пользователей требуется удалить вместе с клиентами, в окне **Удаление клиентов** установите флажок **Удалить пользователей, зарегистрированных только на удаляемых сетевых узлах**.

Этот флажок установлен по умолчанию, если были заданы соответствующие параметры для удаляемых узлов (см. «Параметры работы с объектами сети» на стр. 75).

5 В окне **Удаление клиентов** нажмите кнопку **Удалить клиенты**. Выбранные клиенты будут удалены из сети ViPNet.

6 После удаления клиентов создайте справочники и ключи и отправьте их на узлы своей сети (см. «Отправка справочников и ключей» на стр. 91). Если требуется, отправьте межсетевую информацию в доверенные сети (см. «Отправка межсетевой информации» на стр. 251).

Примечание. Чтобы удалить все клиенты, зарегистрированные на определенном координаторе, удалите этот координатор (см. «Удаление координатора» на стр. 116). Также клиент можно удалить в окне свойств координатора (см. «Изменение списка узлов, зарегистрированных на координаторе» на стр. 120).

Настройка параметров координатора

На каждый координатор необходимо добавить, по крайней мере, одного пользователя и создать связи координатора с другими сетевыми узлами. В зависимости от требуемой функциональности и типа координатора, требуется добавить для него нужные роли.

Основные функции координатора в сети ViPNet — транспортный сервер и сервер IP-адресов (см. «Функции координатора в защищенной сети ViPNet» на стр. 33). Для обмена служебной информацией между координаторами требуется связать их межсерверными каналами. Для того чтобы клиенты могли получить доступ к своим транспортным серверам и серверам IP-адресов, требуется задать адреса и другие параметры доступа к координаторам.

В зависимости от типа подключения координатора к внешней сети, нужно настроить параметры межсетевого экрана координатора. Также рекомендуется выполнить групповую настройку межсетевого экрана клиентов, для которых координатор назначен сервером IP-адресов.

Основные параметры координаторов рекомендуется настроить в программе ViPNet Центр управления сетью, в этом случае не потребуется задавать нужные параметры непосредственно на сетевых узлах.

Для настройки параметров координатора рекомендуется выполнить следующие шаги:

Таблица 6. Последовательность настройки параметров координатора

	Действие	Ссылка
☐	Добавление пользователей на координатор	См. раздел Изменение списка пользователей сетевого узла (на стр. 136).
☐	Создание межсерверных каналов для обмена служебной информацией с другими координаторами	См. раздел Настройка межсерверных каналов (см. «Настройка межсерверных каналов между координаторами, выполняющими функции VPN-сервера» на стр. 122).
☐	Создание связей с другими сетевыми узлами	См. раздел Изменение связей между сетевыми узлами (на стр. 138).
☐	Добавление ролей на координатор	См. раздел Изменение списка ролей сетевого узла (на стр. 142).
☐	Добавление клиентов на координатор	См. раздел Изменение списка клиентов, зарегистрированных на координаторе (см. «Изменение списка узлов, зарегистрированных на координаторе» на стр. 120).

	Действие	Ссылка
☐	Настройка межсетевого экрана координатора	См. раздел Параметры межсетевого экрана координатора (на стр. 178).
☐	Настройка межсетевого экрана клиентов	См. раздел Настройка параметров межсетевого экрана клиентов на сервере IP-адресов (на стр. 186).
☐	Задание адресов координатора	См. раздел Задание IP-адресов сетевого узла (на стр. 175).
☐	Задание адресов туннелируемых соединений	См. раздел Настройка туннелирования (на стр. 123).

Просмотр и изменение основных параметров координатора

Для просмотра и изменения таких параметров координатора, как имя или описание, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Координаторы**.
3. На панели просмотра дважды щелкните координатор, параметры которого нужно просмотреть.
4. В окне свойств координатора на левой панели выберите пункт **Основные параметры**.

   В разделе **Основные параметры координатора** будут отображены:

   - имя и описание координатора;
   - шестнадцатеричный идентификатор сетевого узла;
   - сетевой адрес, состоящий из номера сети ViPNet и номера координатора;
   - информация о последнем обновлении программного обеспечения, отправленном на сетевой узел: имя файла, версия и статус обновления.

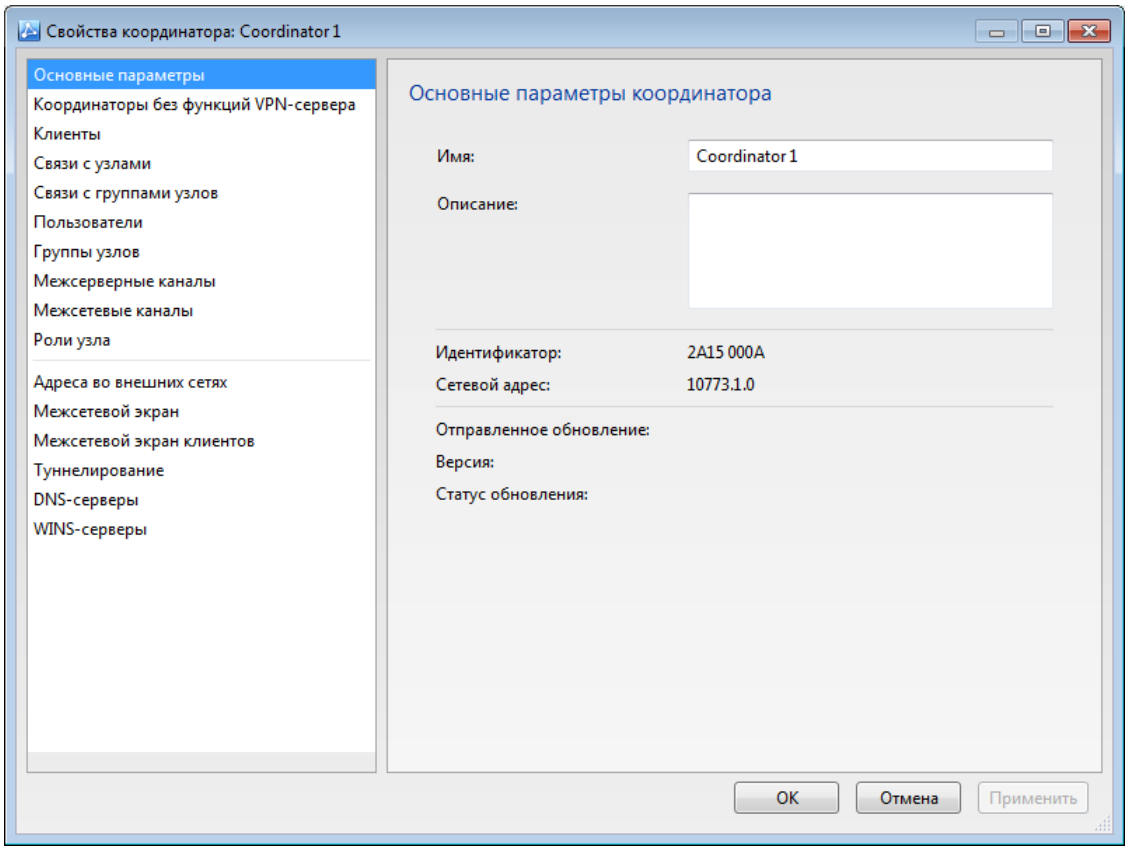

Рисунок 59. Просмотр основных параметров координатора

5 Если требуется, в соответствующих полях измените имя и описание координатора. Остальная информация недоступна для редактирования.

6 Чтобы сохранить изменения, нажмите кнопку **OK**.

Изменение списка узлов, зарегистрированных на координаторе

Каждый клиент сети ViPNet и координатор без функций VPN-сервера (см. «Функции координатора в защищенной сети ViPNet» на стр. 33) зарегистрированы на каком-либо одном координаторе, который работает в режиме VPN-сервера. Этот координатор обеспечивает доставку на узлы ключей и справочников, служебных и почтовых конвертов, то есть выполняет функцию транспортного сервера (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).

Для просмотра и изменения списка узлов, зарегистрированных на координаторе, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы**.

3 На панели просмотра дважды щелкните координатор, список узлов которого нужно просмотреть.

4 В окне свойств координатора на левой панели выберите пункт **Клиенты** или **Координаторы без функций VPN-сервера**.

В соответствующем разделе будет отображен список узлов, зарегистрированных на координаторе.

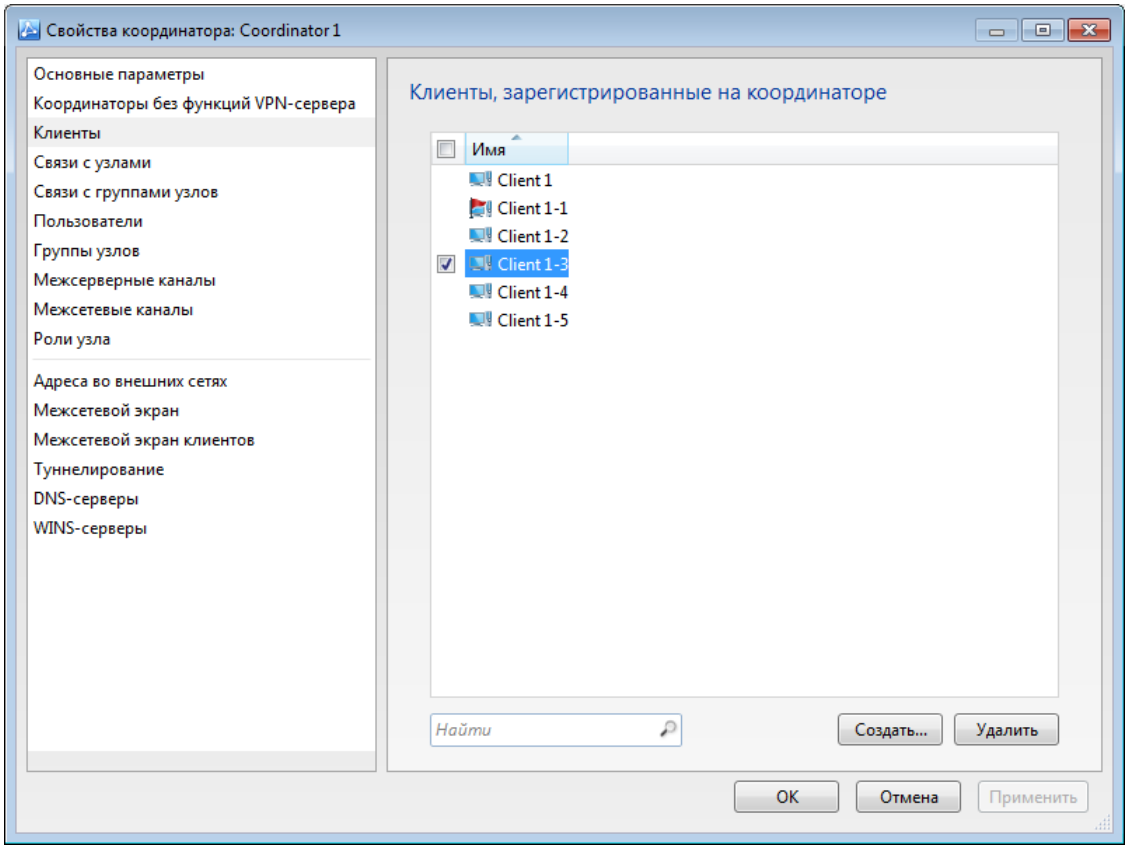

Рисунок 60. Список клиентов, зарегистрированных на координаторе

5 Чтобы создать координатор без функций VPN-сервера (см. «Добавление координатора» на стр. 112) или клиент (см. «Добавление клиента» на стр. 113) и добавить его на выбранный координатор, нажмите кнопку **Создать**.

6 Чтобы удалить узел, зарегистрированный на данном координаторе, выберите узел в списке и нажмите соответствующую кнопку.

7 Выполнив необходимые изменения, нажмите кнопку **OK**.

Настройка межсерверных каналов между координаторами, выполняющими функции VPN-сервера

Межсерверный канал можно создать между координаторами, выполняющими функции VPN-сервера. Межсерверный канал связывает два координатора и позволяет им выполнять функцию транспортного сервера — обмениваться управляющими и прикладными транспортными конвертами (см. глоссарий, стр. 308). Необходимо, чтобы все координаторы были связаны между собой напрямую или через другие такие же координаторы, то есть должен существовать хотя бы один путь передачи служебной информации между двумя любыми координаторами. Можно связать все координаторы с одним центральным (схема «звезда»), все координаторы между собой или использовать другие схемы.

Чтобы убедиться в наличии маршрутов между всеми координаторами сети, выполните проверку конфигурации сети (см. «Проверка конфигурации сети» на стр. 83).

Чтобы просмотреть или изменить список межсерверных каналов с участием координатора, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Координаторы**.
3. На панели просмотра дважды щелкните координатор, список межсерверных каналов которого нужно изменить.
4. В окне свойств координатора на левой панели выберите пункт **Межсерверные каналы**.

   В разделе **Координаторы, с которыми образованы межсерверные каналы** будет отображен список координаторов, с которыми текущий координатор связан межсерверными каналами.

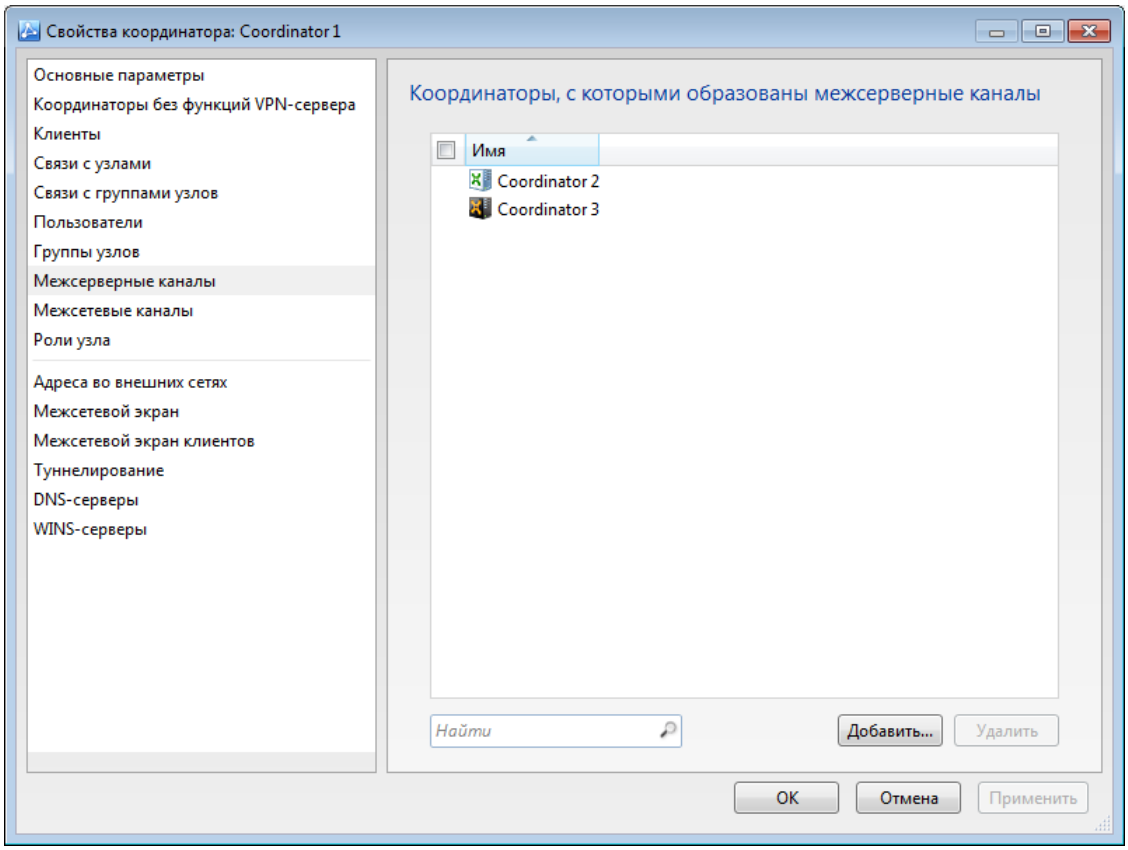

Рисунок 61. Список межсерверных каналов

5 Чтобы создать межсерверные каналы между текущим координатором и другими координаторами:

- Нажмите кнопку **Добавить**.
- В открывшемся окне из списка координаторов, с которыми не образованы межсерверные каналы, выберите один или несколько координаторов и нажмите кнопку **Добавить**.

6 Чтобы удалить межсерверные каналы текущего координатора, выберите в списке нужные координаторы и нажмите кнопку **Удалить**.

7 Чтобы сохранить изменения, нажмите кнопку **OK**.

Настройка туннелирования

Координаторы могут выполнять туннелирование соединений открытых узлов (то есть узлов, на которых не установлено программное обеспечение ViPNet) для защиты трафика этих узлов при передаче через публичные сети (см. «Туннелирование» на стр. 35).

Чтобы настроить туннелирование на координаторе, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы**.

3 На панели просмотра дважды щелкните координатор, который требуется настроить.

4 В окне свойств координатора на левой панели выберите раздел **Туннелирование**.

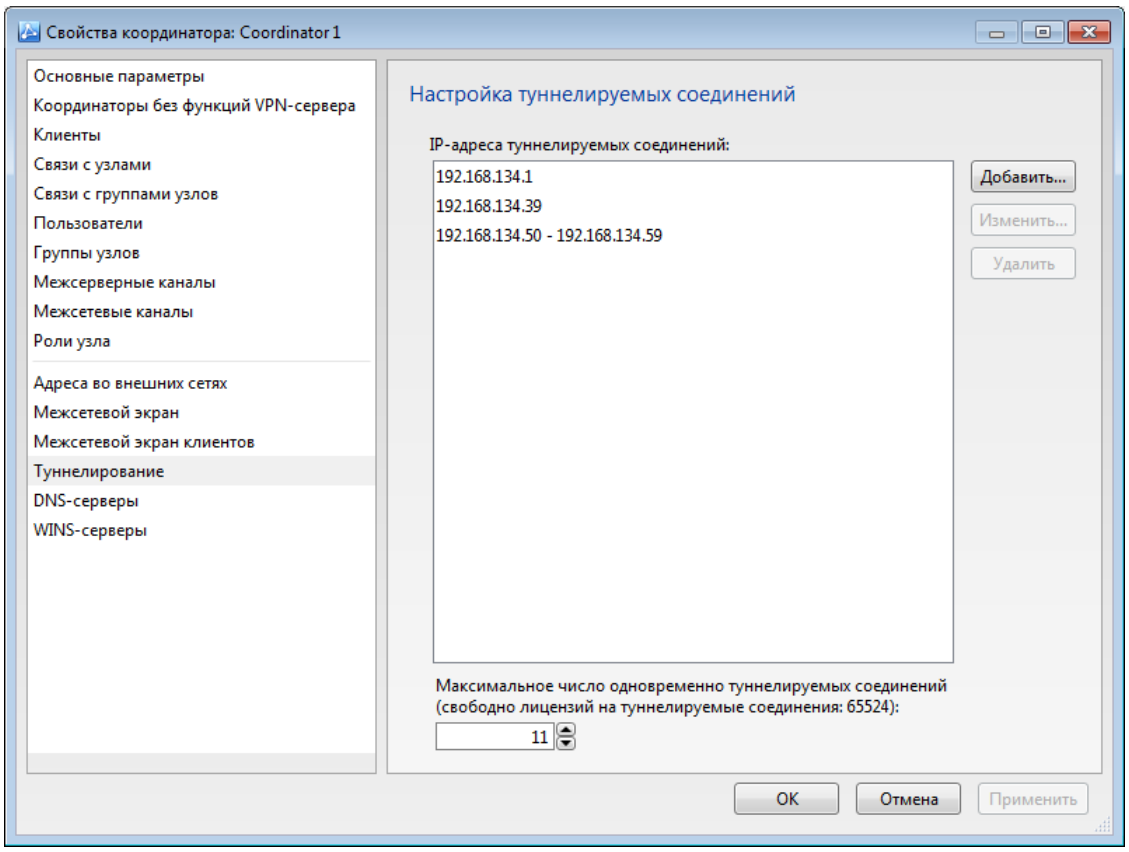

Рисунок 62. Настройка туннелирования

5 Добавьте IP-адреса открытых узлов для туннелирования в список **IP-адреса туннелируемых соединений**:

- Чтобы добавить IP-адрес или диапазон адресов, нажмите кнопку **Добавить**. В окне **IP-адрес или диапазон**:
  - Для добавления одиночного IP-адреса выберите **IP-адрес** и введите адрес туннелируемого узла. Затем нажмите кнопку **OK**.
  - Для добавления диапазона IP-адресов выберите **Диапазон**, в поле **от** введите начальный адрес диапазона, в поле **до** — конечный адрес. Затем нажмите кнопку **OK**.
- Чтобы изменить заданный IP-адрес или диапазон, выберите его в списке и нажмите кнопку **Изменить**, затем отредактируйте адрес.
- Чтобы удалить заданные IP-адреса или диапазоны, выберите их в списке и нажмите кнопку **Удалить**, затем в окне подтверждения нажмите кнопку **Да**.

6 Для координатора с ролями «Программный VPN-координатор» и «Coordinator HW-VA» вы можете изменить максимальное число одновременно туннелируемых соединений, для этого в соответствующем поле задайте число соединений, которые координатор сможет туннелировать одновременно.

Заданное число может быть меньше числа заданных туннелируемых IP-адресов и не может превышать число туннелируемых соединений, которое указано над полем. Для всех ролей координатора, кроме ролей «Программный VPN-координатор» и «Coordinator HW-VA» (см.

«Роли сетевых узлов» на стр. 266) максимальное число одновременно туннелируемых соединений задано по умолчанию и не может быть изменено.

Внимание! На координаторах, на которые добавлены роли «Программный VPN-координатор» и «Coordinator HW-VA», максимальное число одновременно туннелируемых соединений равное 65535 интерпретируется такими координаторами как отсутствие ограничения на число одновременно туннелируемых соединений.

7 Чтобы сохранить настройки, нажмите кнопку **OK**.

Перенос координатора без функций VPN-сервера на другой координатор

При необходимости вы можете зарегистрировать координатор без функций VPN-сервера на другом координаторе, то есть изменить транспортный сервер (см. «Функции координатора в защищенной сети ViPNet» на стр. 33) координатора без функций VPN-сервера. Чтобы координатор без функций VPN-сервера получил информацию о смене транспортного сервера, на него необходимо отправить обновление справочников и ключей.

Чтобы изменить транспортный сервер координатора без функций VPN-сервера, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы**.

3 На правой панели дважды щелкните нужный координатор без функций VPN-сервера.

4 В окне свойств сетевого узла нажмите кнопку **Выбрать**, расположенную справа от поля **Координатор**. В появившемся окне подтвердите изменение транспортного сервера, нажав кнопку **Сменить координатор**.

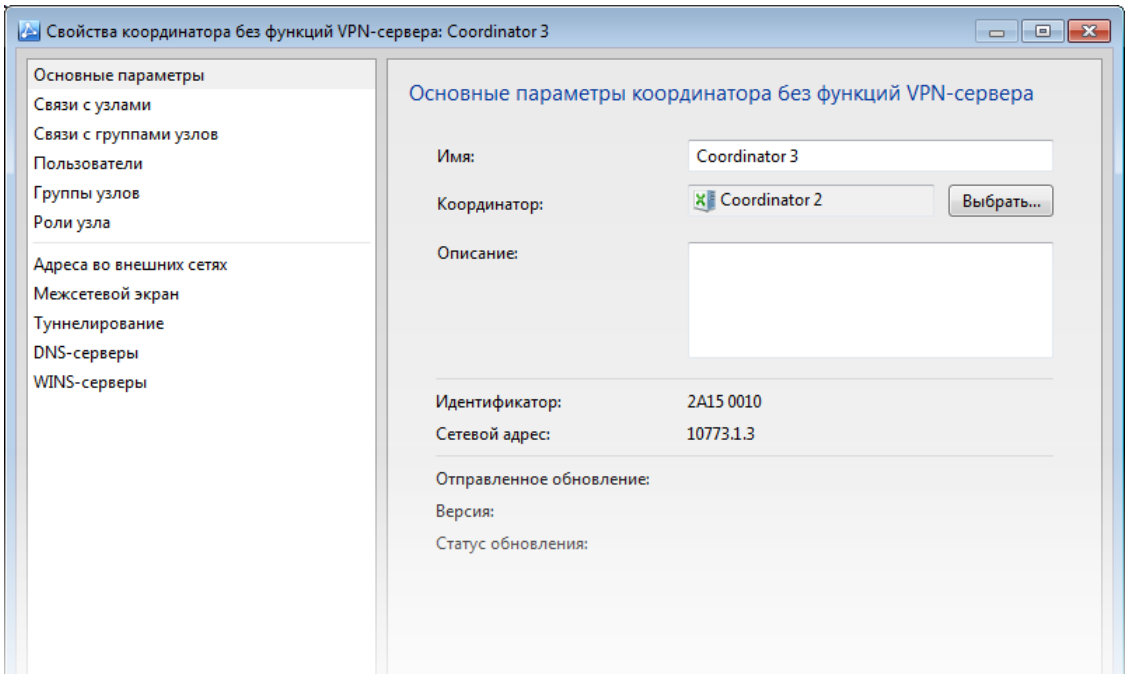

Рисунок 63. Изменение координатора, на котором зарегистрирован координатор без функций VPN-сервера

5 В открывшемся окне выберите в списке нужный координатор и нажмите соответствующую кнопку.

Примечание. В списке будут присутствовать все координаторы, кроме того, на котором зарегистрирован выбранный узел.

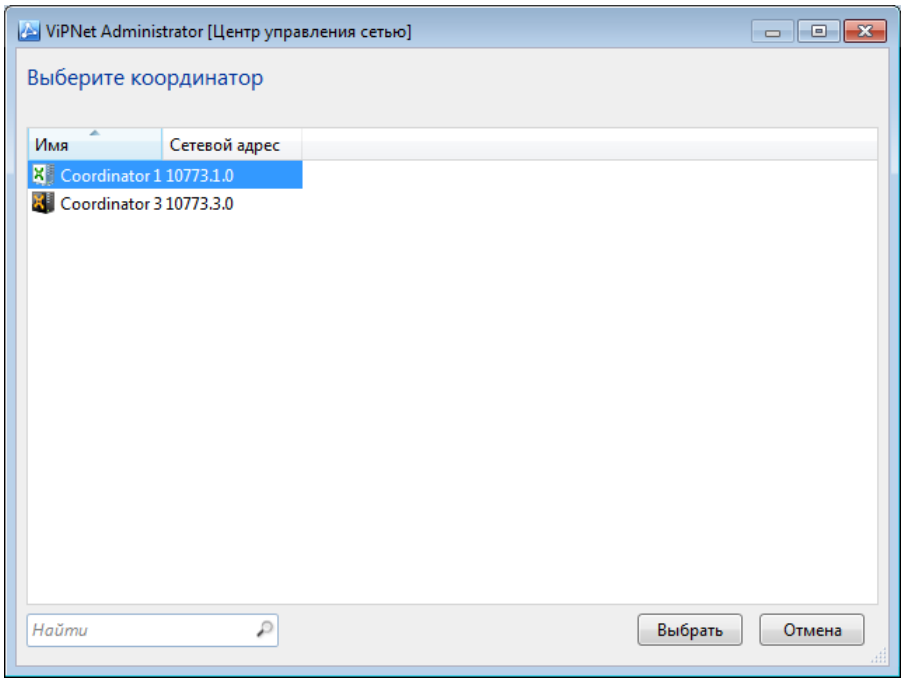

Рисунок 64. Выбор координатора

6 Чтобы сохранить изменения, нажмите кнопку **OK**.

Узел будет зарегистрирован на выбранном координаторе, при этом автоматически изменится сетевой адрес координатора без функций VPN-сервера, содержащий номер координатора и номер узла на координаторе. Если выбранный координатор не был связан с координатором без функций VPN-сервера, такая связь будет создана автоматически.

Для всех узлов, для которых это требуется, создайте и отправьте справочники и ключи (см. «Обновление справочников и ключей» на стр. 87).

Внимание! Если выполняется перенос узла, который участвует в межсетевом взаимодействии с узлами какой-либо доверенной сети, после завершения процедуры переноса узла необходимо отправить новую межсетевую информацию для этой доверенной сети (см. «Отправка межсетевой информации» на стр. 251).

Настройка параметров клиента

На каждый клиент необходимо добавить, по крайней мере, одного пользователя и создать связи клиента с другими сетевыми узлами. В зависимости от программного обеспечения ViPNet, которое планируется установить на клиенте, и его функций, требуется добавить для него нужные роли.

В защищенной сети клиент получает информацию о параметрах доступа к сетевым узлам, с которыми он связан, от своего сервера IP-адресов (см. «Функции координатора в защищенной сети ViPNet» на стр. 33). Поэтому адреса клиентов задавать необязательно, достаточно задать адреса и другие параметры доступа к координаторам. В зависимости от типа подключения клиента к внешней сети, нужно настроить параметры межсетевого экрана клиента.

Основные параметры клиентов рекомендуется настроить в программе ViPNet Центр управления сетью, в этом случае не потребуется задавать нужные параметры непосредственно на сетевых узлах.

Для настройки параметров клиента рекомендуется выполнить следующие шаги:

Таблица 7. Последовательность настройки параметров клиента

	Действие	Ссылка
☐	Добавление пользователей на клиент	См. раздел Изменение списка пользователей сетевого узла (на стр. 136).
☐	Создание связей с другими сетевыми узлами	См. раздел Изменение связей между сетевыми узлами (на стр. 138).
☐	Добавление ролей на клиент	См. раздел Изменение списка ролей сетевого узла (на стр. 142).
☐	Настройка межсетевого экрана клиента	См. раздел Параметры межсетевого экрана клиента (на стр. 180).
☐	Выбор сервера IP-адресов и задание адресов клиента (при необходимости)	См. раздел Смена сервера IP-адресов (на стр. 134).

Просмотр и изменение основных параметров клиента

Для просмотра и изменения таких параметров клиента, как имя или описание, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты**.
3. На панели просмотра дважды щелкните клиент, параметры которого нужно просмотреть.

4 В окне свойств клиента на левой панели выберите пункт **Основные параметры**.

В разделе **Основные параметры клиента** будут отображены:

- имя и описание клиента;
- координатор, на котором зарегистрирован клиент, то есть его транспортный сервер (см. «Функции координатора в защищенной сети ViPNet» на стр. 33);
- шестнадцатеричный идентификатор сетевого узла;
- сетевой адрес, состоящий из номера сети ViPNet, номера координатора и номера клиента на координаторе;
- информация о последнем обновлении программного обеспечения, отправленном на сетевой узел: имя файла, версия и статус обновления.

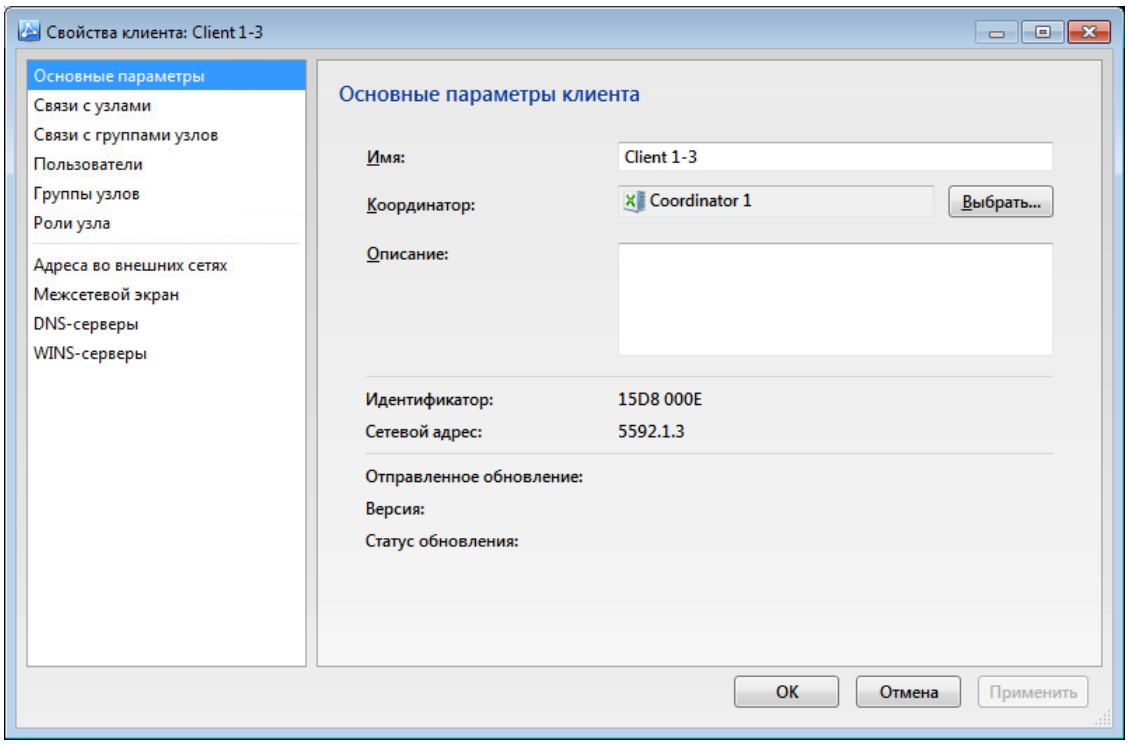

Рисунок 65. Основные параметры клиента

5 Чтобы изменить транспортный сервер клиента, следуйте указаниям раздела Перенос клиента на другой координатор (на стр. 129).

6 Если требуется, в соответствующих полях измените имя и описание клиента.

Редактировать идентификатор узла и сетевой адрес нельзя.

7 Чтобы сохранить изменения, нажмите кнопку **Применить**.

Перенос клиента на другой координатор

При необходимости вы можете зарегистрировать клиент на другом координаторе, то есть изменить транспортный сервер клиента (см. «Функции координатора в защищенной сети ViPNet»

на стр. 33). Чтобы клиент получил информацию о смене транспортного сервера, на него необходимо отправить обновление справочников и ключей. Доставку обновления обеспечивает транспортный сервер, причем до получения информации о смене клиент не может принимать обновления от нового транспортного сервера. Поэтому в течение некоторого времени обновления будут отправляться на клиент через старый транспортный сервер. Время использования старого транспортного сервера задается в настройках программы (см. «Параметры работы с объектами сети» на стр. 75).

Примечание. Если возникла необходимость сменить транспортный сервер для клиента, который является Центром управления сетью, следуйте инструкциям раздела Перенос клиента, являющегося Центром управления сетью, на другой координатор (на стр. 132).

Чтобы изменить транспортный сервер клиента, выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты**.
3. На правой панели дважды щелкните нужный сетевой узел.
4. В окне свойств сетевого узла нажмите кнопку **Выбрать**, расположенную справа от поля **Координатор** (см. рисунок на стр. 129). В появившемся окне подтвердите смену координатора, нажав соответствующую кнопку.
5. В открывшемся окне выберите в списке нужный координатор и нажмите кнопку **Выбрать**.

Примечание. В списке будут присутствовать все координаторы, кроме того, на котором зарегистрирован выбранный клиент.

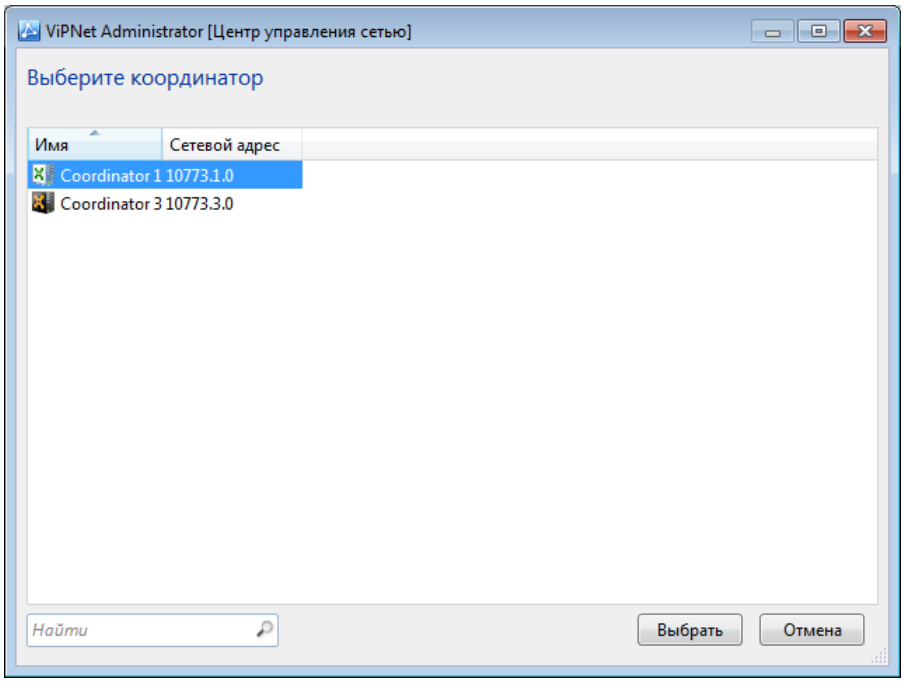

Рисунок 66. Выбор координатора

6 Чтобы сохранить изменения, нажмите кнопку **OK**.

Клиент будет зарегистрирован на выбранном координаторе, при этом автоматически изменится сетевой адрес клиента, содержащий номер координатора и номер клиента на координаторе. Если выбранный координатор не был связан с клиентом, такая связь будет создана автоматически. Сервер IP-адресов клиента также изменится. Он останется прежним, если был изменен вручную ранее (см. «Смена сервера IP-адресов» на стр. 134).

7 Для всех узлов, для которых это требуется, создайте и отправьте справочники и ключи (см. «Обновление справочников и ключей» на стр. 87). Для старого координатора, на котором клиент был зарегистрирован до изменения, автоматически будет сформировано отложенное обновление с временем применения, заданным в настройках программы.

Если вы хотите отложить применение обновления на старом координаторе на более поздний срок, при отправке задайте время вручную. Заданное вручную время должно быть больше времени, заданного в настройках, иначе для отложенного обновления будет использоваться время из настроек.

Внимание! Если выполняется перенос клиента, который участвует в межсетевом взаимодействии с клиентами какой-либо доверенной сети, после завершения процедуры переноса клиента необходимо отправить новую межсетевую информацию для этой доверенной сети (см. «Отправка межсетевой информации» на стр. 251).

---

8 После того, как обновление будет принято на клиенте, для которого был изменен координатор, и на новом координаторе клиента, смена транспортного сервера для этого клиента завершена. При этом для старого координатора автоматически будет сформировано повторное обновление для немедленного применения, статус ключей координатора изменится на **Готовы к отправке**. Вы можете отправить на старый координатор повторное обновление, чтобы не дожидаться применения первого отправленного обновления.

Примечание. Смена транспортного сервера клиента произойдет также в случае, если на новом координаторе клиента обновление не будет принято в течение времени, заданного в настройках программы (см. «Параметры работы с объектами сети» на стр. 75).

Перенос клиента, являющегося Центром управления сетью, на другой координатор

Клиент, являющийся Центром управления сетью, при необходимости может быть перенесен на другой координатор (например, если вы хотите включить данный сетевой узел в подсеть, относящуюся к другому координатору). В отличие от переноса обычных клиентов, на ЦУСе и его координаторе при этом необходимо установить новые дистрибутивы ключей.

Чтобы сменить транспортный сервер для Центра управления сетью, выполните следующие действия:

1. В главном окне программы ViPNet Центр управления сетью в меню **Сервис** выберите **Параметры**.
2. В окне **Параметры ViPNet Центр управления сетью** в разделе **Работа с объектами** установите время использования старого адреса клиента равным одному часу и нажмите кнопку **OK**.

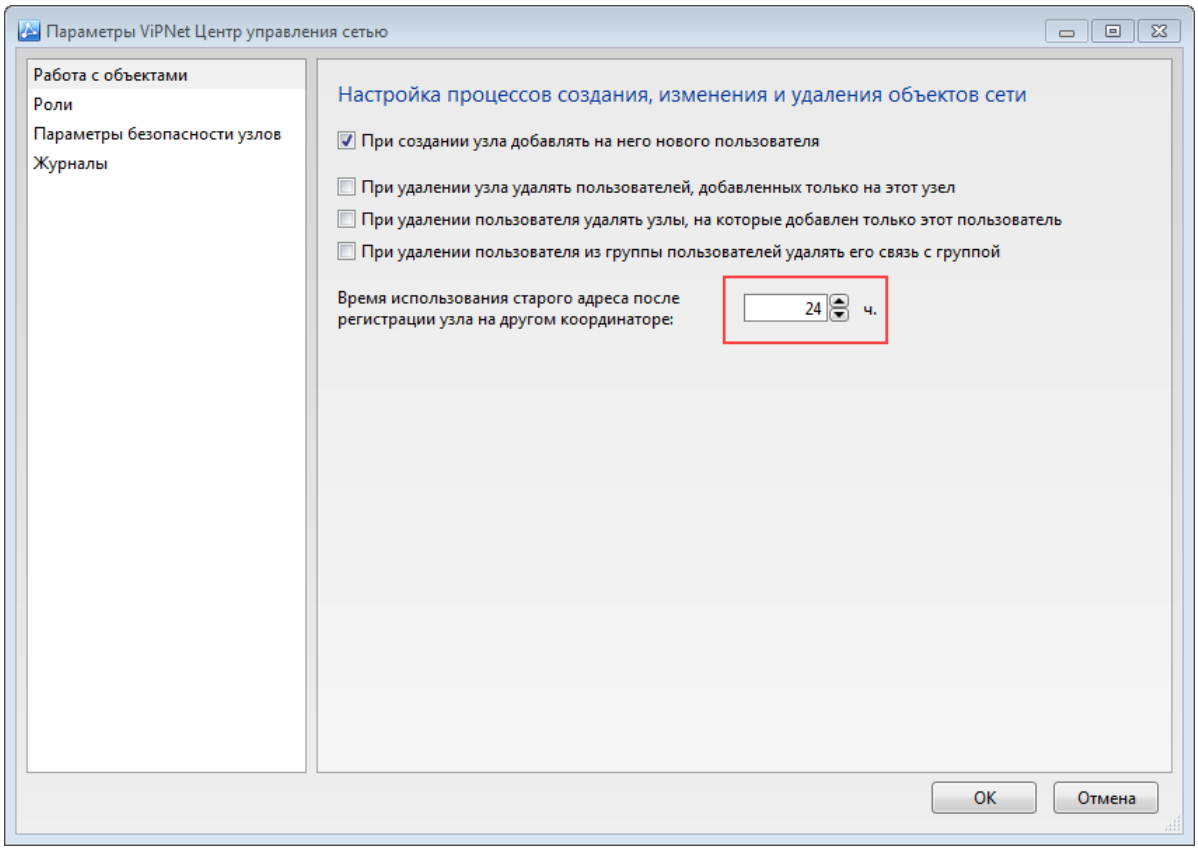

Рисунок 67. Задание времени использования старого адреса

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

4 На панели навигации выберите раздел **Клиенты**.

5 На панели просмотра дважды щелкните клиент, который является Центром управления сетью.

6 В окне свойств клиента (см. рисунок на стр. 129) рядом с полем **Координатор** нажмите кнопку **Выбрать**.

7 В появившемся окне с сообщением подтвердите смену координатора, для этого нажмите кнопку **Сменить координатор**.

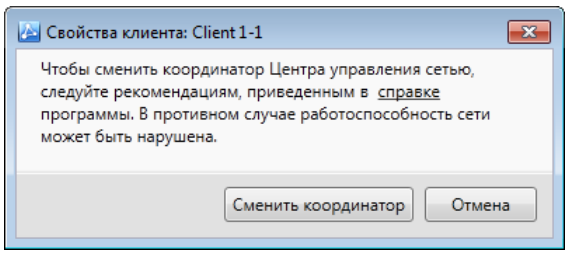

Рисунок 68. Подтверждение смены координатора

8 В появившемся окне (см. рисунок на стр. 131) выберите координатор, на котором будет зарегистрирован ЦУС, и нажмите кнопку **Выбрать**.

В результате ЦУС будет зарегистрирован на выбранном координаторе, и его адрес в сети ViPNet изменится.

9 Создайте справочники для клиента, который является ЦУСом, и координатора, на котором он теперь зарегистрирован (см. «Создание справочников» на стр. 88).

10 В программе ViPNet Удостоверяющий и ключевой центр создайте дистрибутивы ключей для клиента, который является ЦУСом, и для его координатора.

11 На клиенте, являющемся ЦУСом, установите новый дистрибутив ключей. Во время установки обязательно снимите флажок **Не обновлять справочники (рекомендуется)**. Если данный флажок будет установлен, связь ЦУСа с координатором и другими узлами будет нарушена.

12 На координаторе, на котором зарегистрирован ЦУС, установите новый дистрибутив ключей.

13 В программе ViPNet Центр управления сетью отправьте справочники на клиент, являющийся ЦУСом, и на его координатор (см. «Отправка справочников и ключей» на стр. 91).

14 В течение двух часов не производите в ЦУСе рассылку справочников и ключей, а также обновлений ПО. При этом координатор, на котором был раньше зарегистрирован ЦУС, должен быть постоянно включен. Это время необходимо, чтобы убедиться, что ЦУС и его новый координатор функционируют корректно.

15 В программе ViPNet Центр управления сетью сформируйте и отправьте на узлы все необходимые справочники.

Смена сервера IP-адресов

Чтобы изменить для клиента сервер IP-адресов (см. «Функции координатора в защищенной сети ViPNet» на стр. 33), выполните следующие действия:

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

2 На панели навигации выберите раздел **Клиенты**.

3 На панели просмотра дважды щелкните клиент, который требуется настроить.

4 В окне свойств клиента на левой панели выберите раздел **Адреса во внешних сетях**.

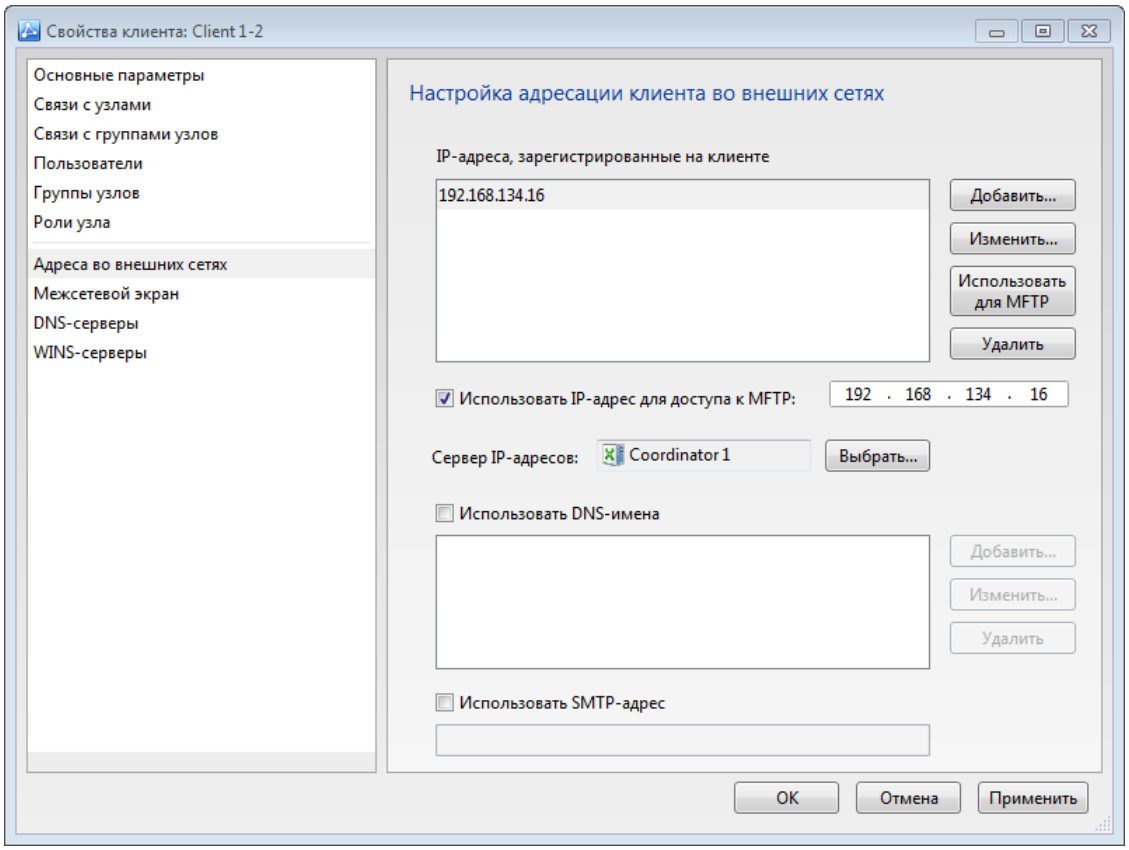

Рисунок 69. Смена сервера IP-адресов

5 По умолчанию сервером IP-адресов назначен координатор, на котором зарегистрирован клиент. Чтобы изменить сервер IP-адресов:

- Нажмите кнопку **Выбрать** рядом с полем **Сервер IP-адресов**.
- В открывшемся окне выберите из списка координатор, который требуется назначить сервером IP-адресов для текущего клиента. Сервером IP-адресов может быть любой координатор своей сети ViPNet.
- Нажмите кнопку **Выбрать**.

  Сервер IP-адресов клиента будет изменен. Если выбранный координатор не был связан с клиентом, такая связь будет создана автоматически.

6 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Изменение списка пользователей сетевого узла

Чтобы просмотреть или изменить список пользователей, добавленных на сетевой узел, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы** или **Клиенты**, в зависимости от типа узла, который требуется настроить.

3 На панели просмотра дважды щелкните сетевой узел, список пользователей которого нужно изменить.

4 В окне свойств сетевого узла на левой панели выберите пункт **Пользователи**.

В разделе **Пользователи клиента (координатора)** будет отображен список пользователей выбранного сетевого узла.

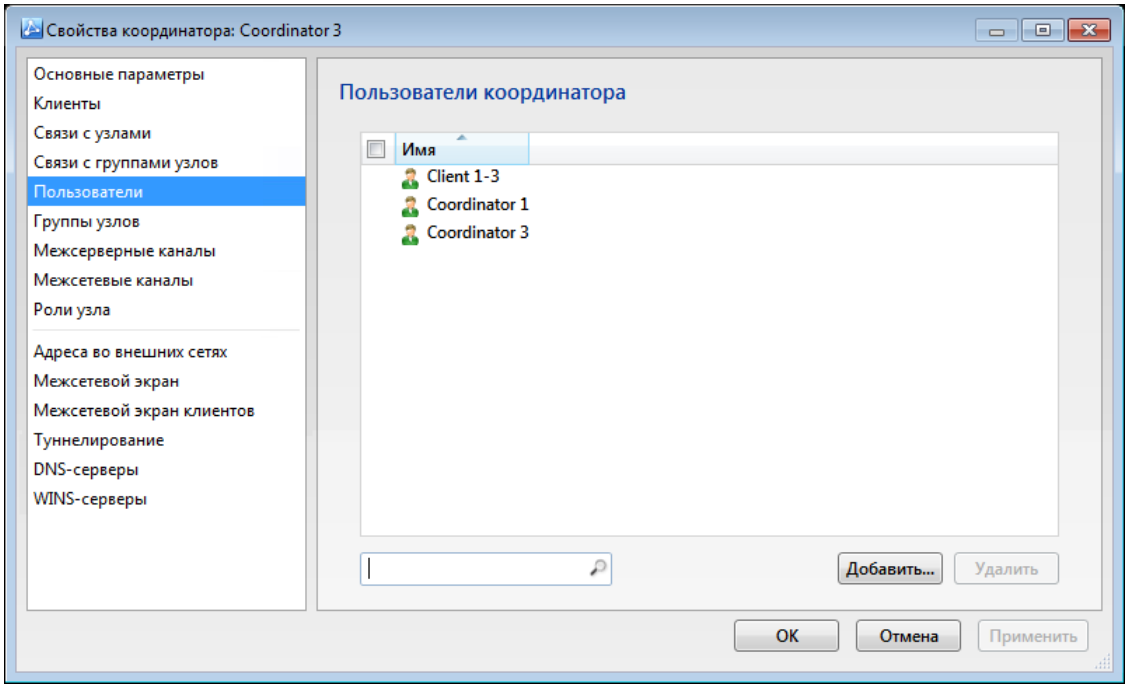

Рисунок 70. Список пользователей координатора

5 Чтобы добавить существующих пользователей в список пользователей сетевого узла нажмите кнопку **Добавить** и в открывшемся окне выберите из списка одного или несколько пользователей.

Внимание! Если пользователь зарегистрирован на нескольких сетевых узлах, его ключи пользователя (см. глоссарий, стр. 303) могут быть отправлены только на первый узел, на который он был добавлен.

---

6 Чтобы удалить пользователей из списка пользователей сетевого узла, выберите в списке одного или несколько пользователей и нажмите кнопку **Удалить**.

Примечание. Не рекомендуется удалять из списка всех пользователей сетевого узла, так как в результате создание справочников для этого узла будет невозможно.

7 Чтобы сохранить изменения, нажмите кнопку **ОК**.

Добавить пользователя на сетевой узел или удалить пользователя с сетевого узла можно также в окне свойств пользователя (см. «Изменение списка сетевых узлов пользователя» на стр. 206).

Изменение связей между сетевыми узлами

Каждый сетевой узел может быть связан с другими сетевыми узлами и с группами сетевых узлов. Оба вида связей обеспечивают возможность соединений между узлами сети ViPNet. Связь с группой сетевых узлов означает, что текущий узел связан со всеми узлами, входящими в группу. При создании связи сетевого узла с группой автоматически создаются связи этого узла с каждым узлом из группы. Такие связи отображаются вместе с остальными связями с сетевыми узлами в окне свойств узла в разделе **Связи с узлами**.

Примечание. При создании связи между клиентами следует установить связь между координаторами, на которых зарегистрированы связываемые узлы. Также при создании связи между клиентом и координатором установите связь между этим координатором и координатором, на котором зарегистрирован клиент.

Связи с сетевыми узлами

Для просмотра и изменения списка сетевых узлов, с которыми связан клиент или координатор, выполните следующие действия:

1. В окне **ViPNet Центр управления сетью** на панели навигации нажмите кнопку **Моя сеть**.
2. На панели навигации в списке **Моя сеть** выберите пункт **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.
3. На панели просмотра дважды щелкните сетевой узел, связи которого требуется изменить.
4. В окне свойств сетевого узла на левой панели выберите пункт **Связи с узлами**.

   В разделе **Сетевые узлы, с которыми установлена связь** будет отображен список узлов своей сети, с которыми связан данный сетевой узел. Связи с узлами, имена которых выделены серым цветом, созданы автоматически и не могут быть изменены в окне свойств сетевого узла. Для каждой связи в столбце **Статус связи** отображается:

   - Информация о связи.
   - Причина, по которой нельзя удалить связь (например, **Связь между узлом и ЦУСом**).
   - Информация о связях с группами узлов, на основе которых созданы связи с узлами.

Примечание. Связи, сформированные автоматически при создании связи с группой узлов, также выделены серым цветом. Если вы хотите удалить такую связь с каким-либо узлом, то предварительно необходимо удалить связь с соответствующей группой (см. «Связи с группами узлов» на стр. 140) или удалить узел из группы (см. «Изменение списка сетевых узлов в группе» на стр. 197).

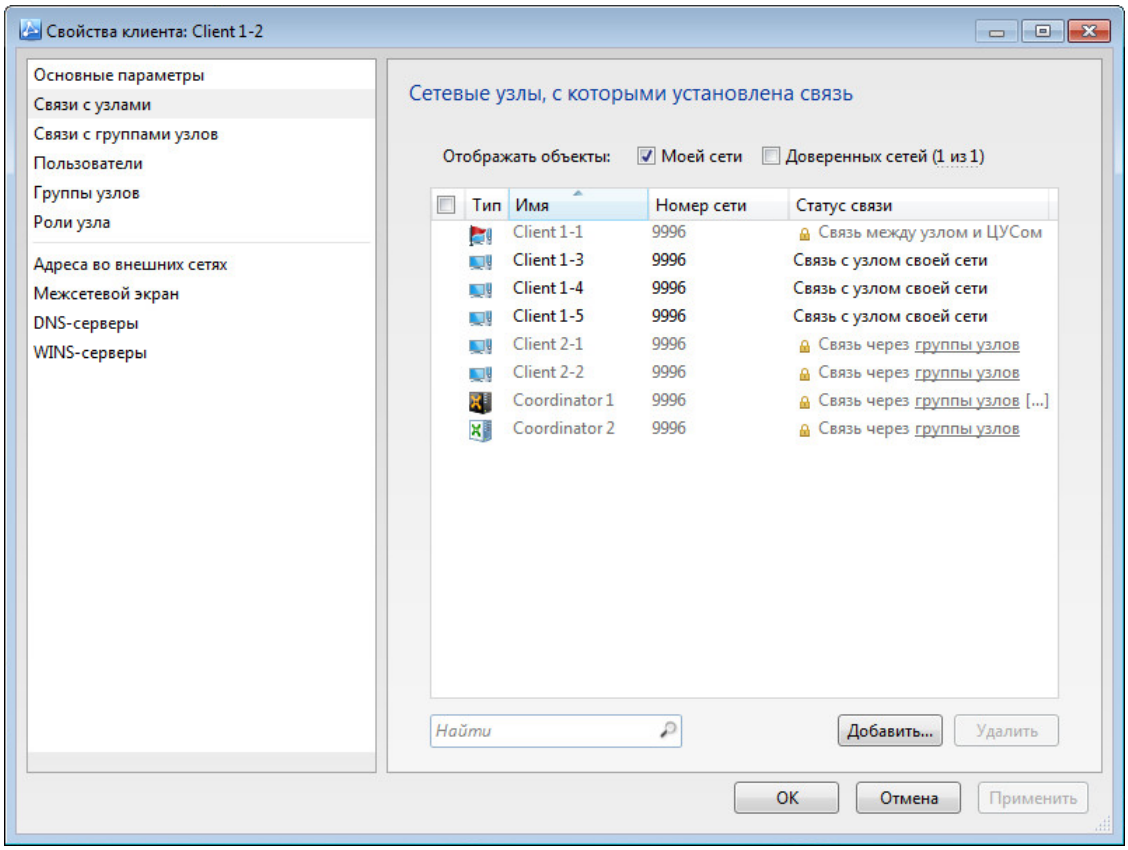

Рисунок 71. Список связей координатора

5 Чтобы просмотреть связи сетевого узла с узлами доверенных сетей, установите флажок **Доверенных сетей** или нажмите ссылку справа от флажка, чтобы выбрать нужные доверенные сети.

6 Для добавления связей нажмите кнопку **Добавить** в окне со списком доступных для связывания узлов выберите один или несколько сетевых узлов.

7 Чтобы удалить связи, выберите в списке связей один или несколько сетевых узлов и нажмите кнопку **Удалить**.

Примечание. Связи с узлами, созданные автоматически и выделенные серым цветом, невозможно удалить.

Чтобы изменить связи между узлами вашей сети и узлами доверенных сетей, измените связи между пользователями этих узлов (см. «Изменение связей с объектами доверенной сети» на стр. 245).

---

8 Чтобы сохранить изменения, нажмите кнопку **OK**.

Связи с группами узлов

Для просмотра и изменения списка групп узлов, с которыми связан клиент или координатор, выполните следующие действия:

1 В окне **ViPNet Центр управления сетью** на панели навигации нажмите кнопку **Моя сеть**.

2 На панели навигации в списке **Моя сеть** выберите пункт **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.

3 На панели просмотра дважды щелкните сетевой узел, связи которого требуется изменить.

4 В окне свойств сетевого узла на левой панели выберите пункт **Связи с группами узлов**.

В разделе **Группы узлов, с которыми установлена связь** будет отображен список групп узлов своей сети, с которыми связан данный сетевой узел.

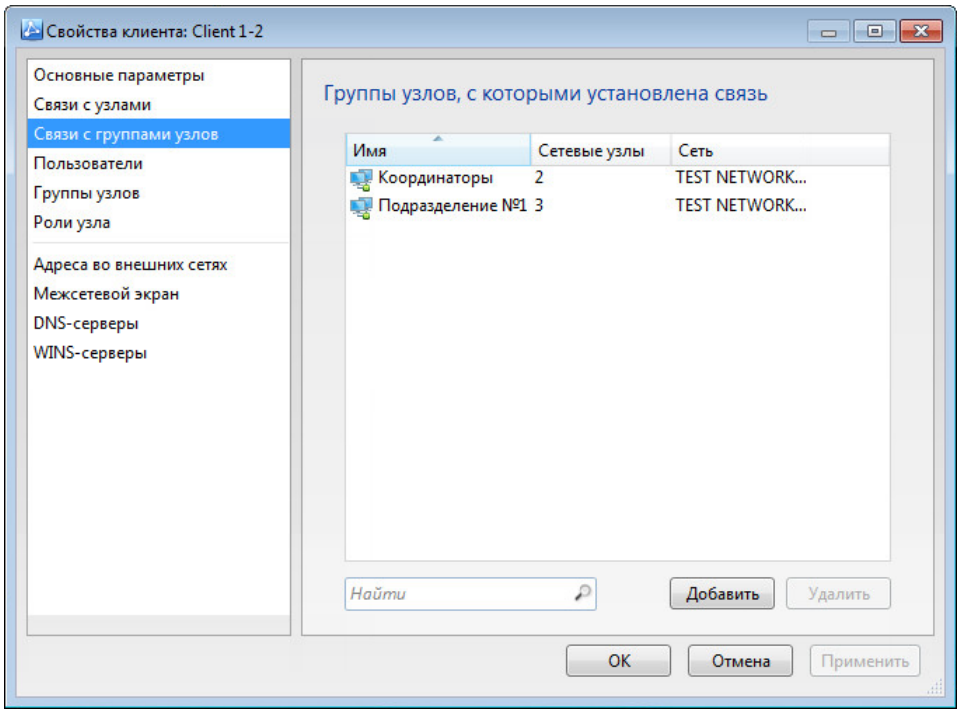

Рисунок 72. Связи с группами узлов

5 Для добавления связей нажмите кнопку **Добавить** и в открывшемся окне со списком доступных групп выберите одну или несколько групп узлов.

Выбранные группы будут добавлены в список связей текущего узла. При этом будут автоматически созданы связи со всеми узлами, входящими в эти группы. Эти связи будут отображены в разделе **Связи с узлами** (см. «Связи с сетевыми узлами» на стр. 138).

6 Чтобы удалить связи:

- Выберите в списке связей одну или несколько групп узлов и нажмите кнопку **Удалить**.
- Если требуется удалить связи со всеми узлами, входящими в группу, в окне подтверждения установите соответствующий флажок. Если флажок не будет установлен, то связь с группой узлов будет удалена, но связи с узлами группы будут сохранены.

- Нажмите кнопку **Удалить связи**. Выбранные связи будут удалены.

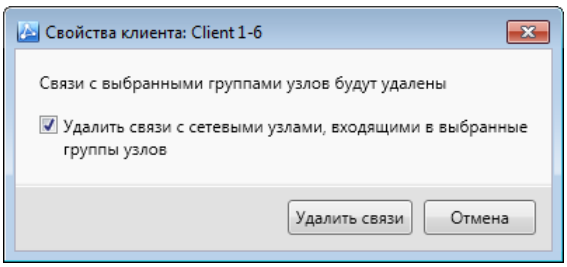

Рисунок 73. Подтверждение удаления связи с группой узлов

7 Чтобы сохранить изменения, нажмите кнопку **OK**.

Добавление ролей на сетевые узлы

Роли сетевого узла определяют, какие программы ViPNet могут работать на этом узле и какие задачи узел может выполнять. Для каждой роли существует лицензионное ограничение (см. «Лицензия на сеть ViPNet» на стр. 23) на количество узлов, для которых можно добавить эту роль. Также для каждой роли лицензией могут быть предусмотрены дополнительные ограничения на версии и период использования программного обеспечения.

Подробная информация о ролях, которые можно добавить на сетевые узлы, содержится в разделе Роли сетевых узлов (на стр. 266).

Изменение списка ролей сетевого узла

Чтобы просмотреть или изменить список ролей сетевого узла (см. «Роли сетевых узлов» на стр. 31), выполните следующие действия:

1. В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа сетевого узла, который требуется настроить.
3. На панели просмотра дважды щелкните сетевой узел, список ролей которого нужно просмотреть или изменить.
4. В окне свойств сетевого узла на левой панели выберите пункт **Роли узла**.

   В разделе **Роли узла** будет отображен список ролей, добавленных на текущий сетевой узел, с указанием максимальной версии и периода использования установленного программного обеспечения.

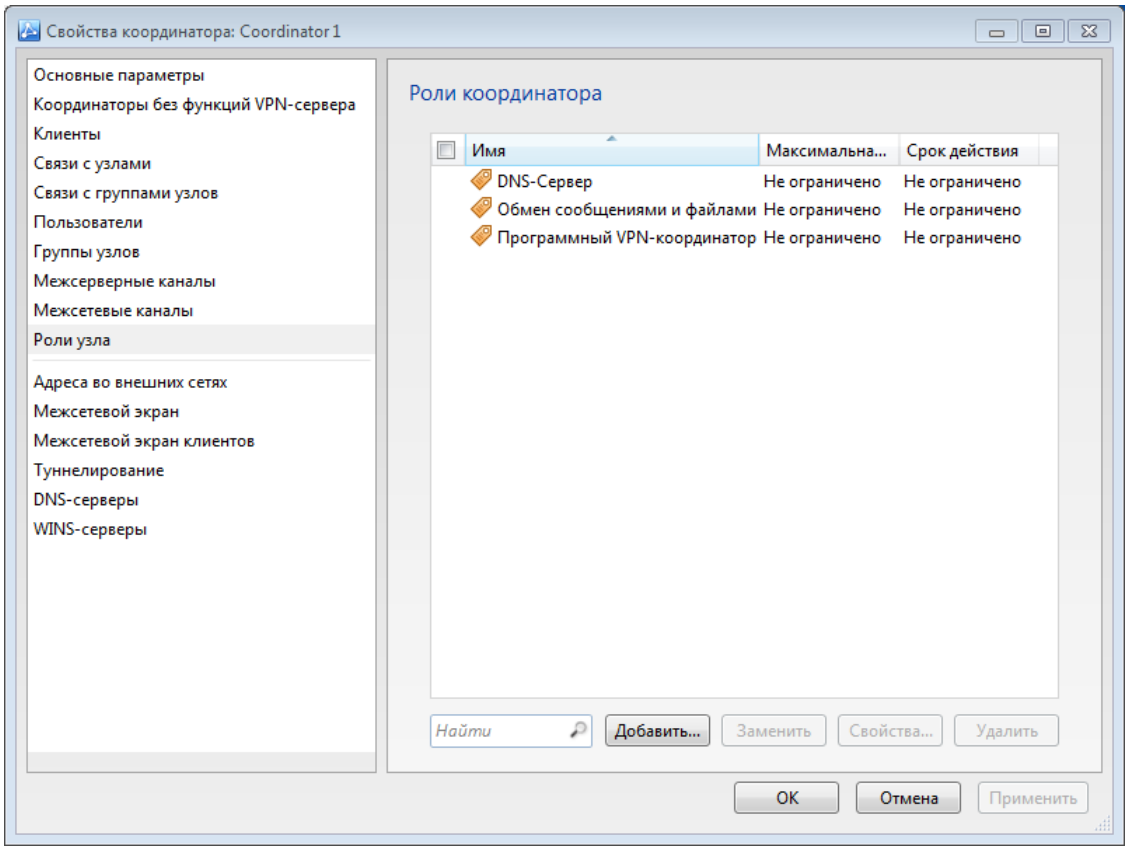

Рисунок 74. Список ролей координатора

5 Чтобы добавить на сетевой узел новые роли:

- Нажмите кнопку **Добавить**. Откроется окно **Выбор объектов** со списком ролей, которые могут быть добавлены на данный сетевой узел, и их свойств.

  Список доступных ролей зависит от того, какие роли уже зарегистрированы на данном узле. Например, на координатор с ролью «Coordinator HW1000» могут быть добавлены только роли «Failover1000», «DNS-Сервер» и «WINS-Сервер». Роли, для которых использованы все лицензии, в списке не отображаются.

- Выберите в списке одну или несколько ролей, которые требуется добавить на данный сетевой узел, и нажмите кнопку **Добавить**.

  Выбранные роли будут зарегистрированы на узле.

6 Чтобы просмотреть или изменить свойства роли, дважды щелкните роль и в окне свойств задайте необходимые параметры (см. «Изменение уровня полномочий пользователя» на стр. 146).

7 Чтобы изменить для роли дополнительные ограничения по версии и периоду использования устанавливаемого ПО:

7.1 Выберите в списке роль и нажмите кнопку **Заменить**.

7.2 В окне **Роли, на которые можно заменить выбранную роль** выберите ту же роль с другими дополнительными ограничениями и нажмите кнопку **Заменить**.

Внимание! Если выбор новых дополнительных ограничений для роли предполагает возврат к предыдущей версии программного обеспечения на узле, следует переустановить данное ПО на узле и затем в программе ViPNet Удостоверяющий и ключевой центр создать новый дистрибутив ключей для этого сетевого узла, передать его на узел и установить.

Информация о работе в программе ViPNet Удостоверяющий и ключевой центр содержится в документе «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

8 Чтобы удалить роли, добавленные на узел, выберите их в списке и нажмите кнопку **Удалить**.

9 Чтобы сохранить настройки, нажмите кнопку **OK**.

Добавить роли на сетевые узлы или удалить роли узлов можно также в разделе **Роли** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

Групповое добавление ролей на сетевые узлы

Групповое добавление ролей позволяет добавить одну роль сразу на несколько сетевых узлов. Для добавления ролей на узлы выполните следующие действия:

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

2 На панели навигации выберите раздел **Роли**.

На панели просмотра будет отображен список ролей, на которые имеются лицензии в данной сети ViPNet. Для ролей в столбцах отображается следующая информация:

- **Узлы с ролью** — количество сетевых узлов, на которые добавлена роль.
- **Свободные лицензии** — оставшееся количество лицензий для добавления роли на другие узлы.
- **Максимальная версия** — максимальная версия программного обеспечения, которое можно установить на узел с этой ролью.
- **Срок действия** — период использования программного обеспечения, которое можно установить на узел с этой ролью.
- **Идентификатор** — идентификатор лицензии программного обеспечения.

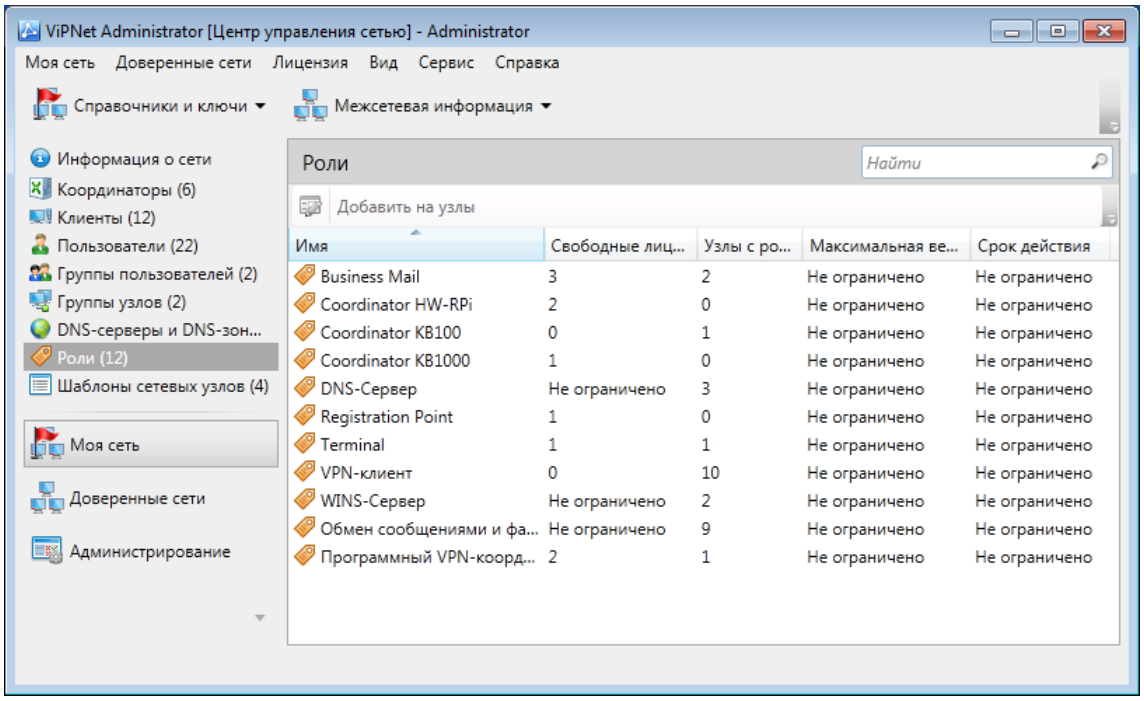

Рисунок 75. Список ролей

3 Для просмотра свойств роли дважды щелкните роль в списке. Откроется окно свойств роли, а в нем — раздел **Основные параметры**, содержащий описание роли и ее код.

4 Для просмотра и изменения списка узлов, на которые добавлена роль, в окне свойств роли на левой панели выберите пункт **Сетевые узлы**.

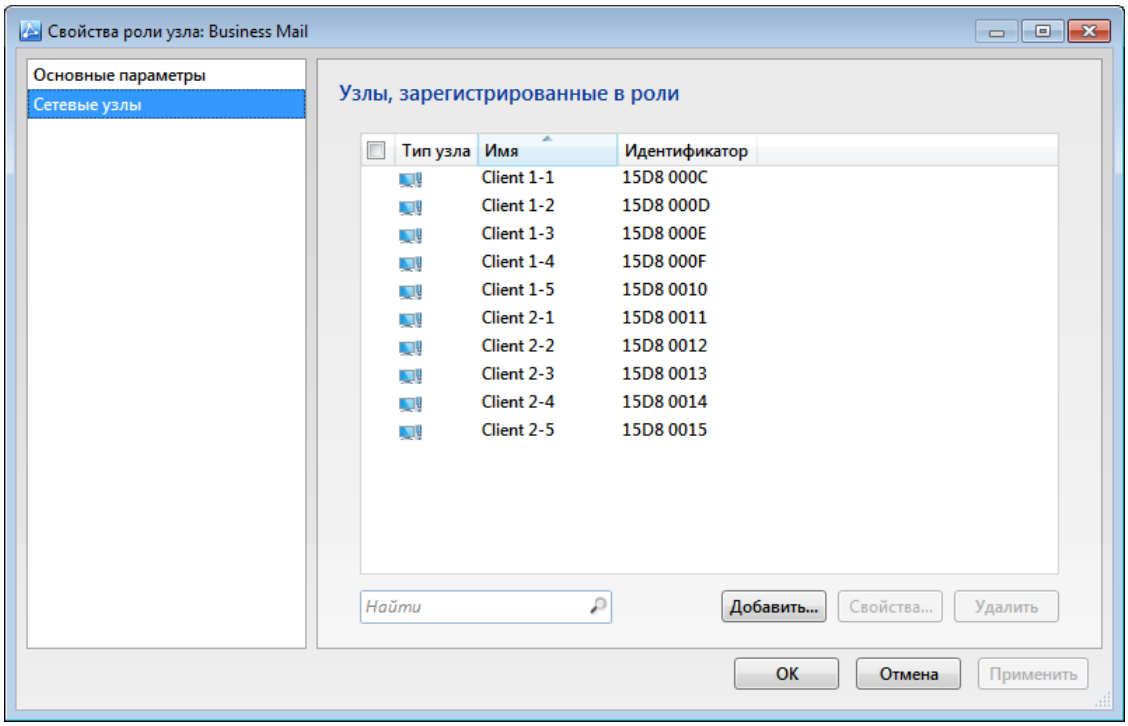

Рисунок 76. Сетевые узлы с выбранной ролью

5 Для добавления роли на сетевые узлы нажмите кнопку **Добавить** и в окне со списком сетевых узлов, на которые можно добавить данную роль, выберите один или несколько узлов.

Примечание. Для добавления роли на сетевые узлы можно также выбрать роль на панели просмотра в разделе **Роли** и нажать кнопку **Добавить на узлы** на панели инструментов.

6 Чтобы изменить свойства роли для определенного сетевого узла, выберите узел в списке и нажмите кнопку **Свойства**, в окне свойств роли задайте необходимые параметры (см. «Изменение уровня полномочий пользователя» на стр. 146).

7 Чтобы отменить добавление роли на сетевые узлы, выберите один или несколько сетевых узлов в списке и нажмите кнопку **Удалить**.

8 Выполнив необходимые действия, нажмите кнопку **ОК**.

9 После добавления ролей на сетевые узлы, удаления или изменения свойств ролей создайте справочники и отправьте их на узлы, роли которых были изменены (см. «Отправка справочников и ключей» на стр. 91).

Добавить роли на сетевые узлы или удалить роли узлов можно также в окне свойств сетевого узла (см. «Изменение списка ролей сетевого узла» на стр. 142).

Изменение уровня полномочий пользователя

Для сетевых узлов, на которые добавлены роли «VPN-клиент», «Программный VPN-координатор», «CryptoService», «Business Mail» и «VPN Client для мобильных устройств», вы можете задать уровень полномочий пользователя. От уровня полномочий зависит возможность изменения пользователями настроек программного обеспечения ViPNet, установленного на сетевом узле.

Внимание! Не следует задавать полномочия для координаторов с ролью «Программный VPN-координатор», на которые установлено ПО ViPNet Coordinator for Linux. Это может вызвать неполадки в функционировании таких координаторов.

Чтобы изменить уровень полномочий пользователя, выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните нужную роль (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 В окне **Свойства роли** выполните следующие действия:

- Если вы настраиваете уровень полномочий для роли «Программный VPN-координатор», установите флажок **Задать полномочия** и выберите уровень полномочий, как описано ниже.
- Чтобы задать один из стандартных уровней полномочий, установите переключатель в одно из положений: **Максимальные** (по умолчанию), **Средние**, **Минимальные**.

- Чтобы задать специальный уровень полномочий, установите переключатель в положение **Специальные** и в поле справа введите символ, обозначающий требуемый уровень полномочий.

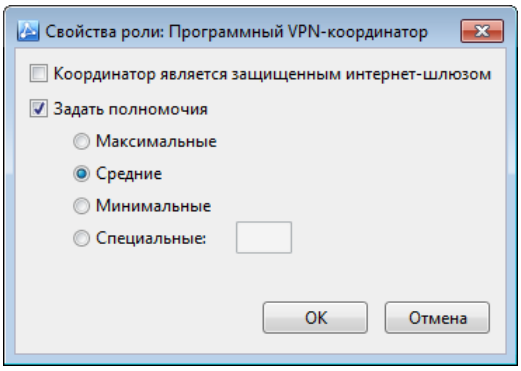

Рисунок 77. Настройка уровня полномочий для роли «Программный VPN-координатор»

3 Задав уровень полномочий, нажмите кнопку **OK**.

Описание уровней полномочий пользователя см. в документе «Классификация полномочий. Приложение к документации ViPNet».

Настройка параметров роли «Обмен сообщениями и файлами»

Роль «Обмен сообщениями и файлами» позволяет использовать на сетевом узле встроенные в ПО ViPNet Client и ViPNet Coordinator средства коммуникации — обмен защищенными сообщениями и обмен файлами. По умолчанию эта роль разрешает оба вида обмена. При необходимости вы можете запретить пользователям сетевого узла обмен сообщениями или обмен файлами.

Чтобы изменить права на использование обмена сообщениями и файлами, выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните роль «Обмен сообщениями и файлами» (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 В окне **Свойства роли** снимите или установите нужные флажки.

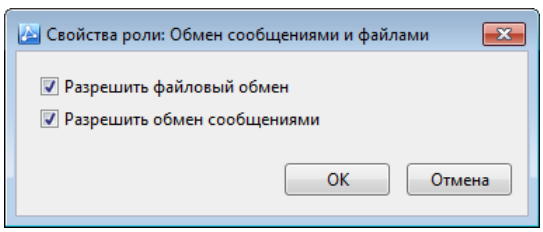

Рисунок 78. Задание разрешений на обмен сообщениями и файлами

3 Задав параметры, нажмите кнопку **OK**.

Добавление ролей «DNS-Сервер» и «WINS-Сервер»

Роли «DNS-Сервер» и «WINS-Сервер» следует добавлять на защищенные узлы (см. глоссарий, стр. 302), которые являются серверами DNS или WINS, а также на координаторы, которые туннелируют соответствующие серверы (см. глоссарий, стр. 309). После добавления роли «DNS-Сервер» или «WINS-Сервер» на защищенный узел вы сможете добавлять его в список DNS- или WINS-серверов узлов вашей сети ViPNet (см. «Настройка списков DNS- и WINS-серверов сетевого узла» на стр. 172). На сетевые узлы информация о заданных для них списках DNS- и WINS-серверов будет передана в составе справочников.

Использование этих ролей позволяет решить проблему доступа сетевых узлов ViPNet к защищенным корпоративным серверам DNS и WINS. Пользователи сети ViPNet могут подключаться к корпоративным ресурсам через Интернет. При этом часто требуется использовать корпоративный DNS-сервер, адрес доступа к которому может динамически изменяться. В этом случае пользователю приходится вручную изменять адрес DNS-сервера в свойствах сетевого подключения.

Если на сетевой узел из Центра управления сетью передана информация о серверах DNS и WINS, находящихся на защищенных и туннелируемых узлах, программа ViPNet Монитор будет автоматически определять текущие IP-адреса видимости корпоративных серверов DNS и WINS (реальные или виртуальные) и автоматически изменять адреса серверов в настройках сетевых интерфейсов компьютера.

Если вы добавили роль «DNS-Сервер» или «WINS-Сервер» на клиент, эта роль не имеет дополнительных параметров. Если вы добавили роль «DNS-Сервер» или «WINS-Сервер» на координатор, который туннелирует соответствующие серверы, в свойствах роли укажите IP-адреса этих серверов. Для этого:

1. В списке ролей координатора дважды щелкните нужную роль (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена роль, выберите координатор и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).
2. В окне **Свойства роли: DNS (WINS)-Сервер** с помощью кнопки **Добавить** укажите IP-адреса серверов DNS (или WINS), туннелируемых данным координатором.

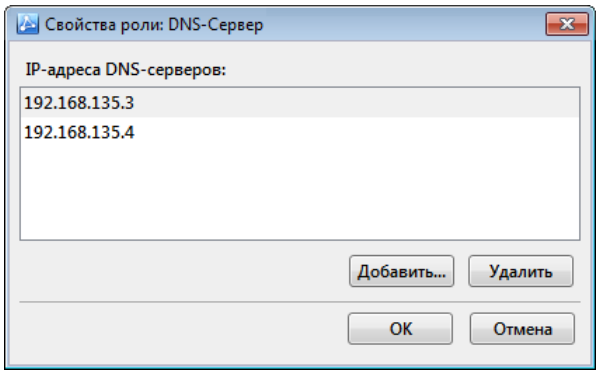

Рисунок 79. Адреса туннелируемых DNS-серверов

Если заданный IP-адрес отсутствует в списке туннелируемых адресов данного координатора (см. «Настройка туннелирования» на стр. 123), появится сообщение с предложением добавить адрес в этот список. Чтобы продолжить, нажмите кнопку **Добавить IP-адрес**.

Примечание. Если вы удалите IP-адреса, заданные в свойствах роли «Сервер DNS» или «Сервер WINS», из списка туннелируемых адресов координатора, они также будут удалены из списка серверов DNS или WINS.

3 В окне **Свойства роли: DNS (WINS)-Сервер** нажмите кнопку **OK**.

Настройка списка управляемых узлов для роли «Policy Manager»

При создании сетевого узла, который является Центром управления сетью, на него автоматически добавляется роль «Policy Manager». ЦУС выполняет функции сервера управления политиками безопасности, и для него необходимо задать список управляемых узлов. Для этого выполните следующие действия:

1 В списке ролей сетевого узла ЦУСа, отмеченного значком , дважды щелкните роль «Policy Manager» (см. «Изменение списка ролей сетевого узла» на стр. 142).

2 В окне **Свойства роли** выполните следующие действия:

- Чтобы добавить узлы в список, нажмите кнопку **Добавить**, в открывшемся окне выберите нужные сетевые узлы и нажмите кнопку **OK**.
- Чтобы удалить сетевые узлы, выберите их в списке и нажмите кнопку **Удалить**. Затем в окне подтверждения нажмите кнопку **OK**.

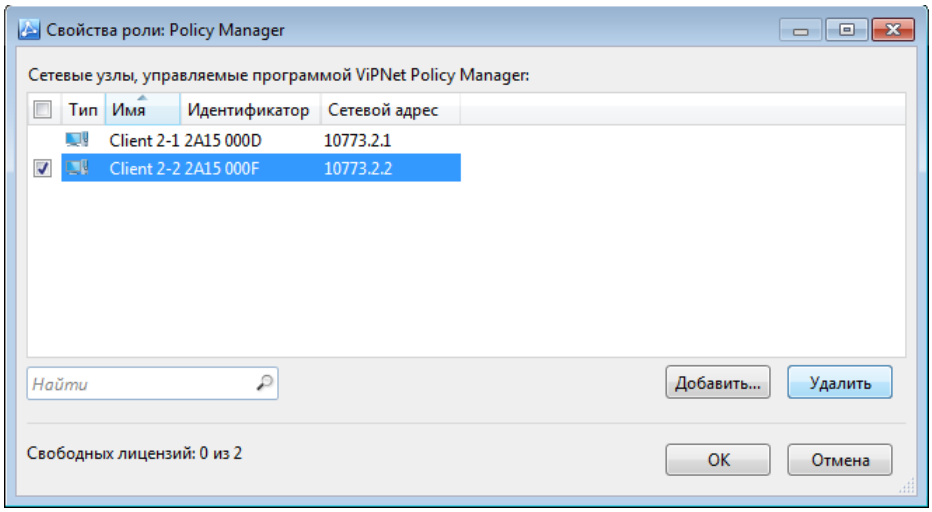

Рисунок 80. Изменение списка управляемых узлов

3 Задав список управляемых узлов, нажмите кнопку **OK**.

Подробную информацию о работе сервера управления политиками безопасности см. документ «ViPNet Policy Manager. Руководство администратора».

Изменение числа узлов мониторинга для роли «StateWatcher»

Сетевой узел, на который добавлена роль «StateWatcher», является сервером мониторинга и собирает информацию о состоянии узлов сети ViPNet. Для него требуется задать количество узлов мониторинга и дочерних серверов мониторинга. Для этого выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните роль «StateWatcher» (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена эта роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 В окне **Свойства роли** выполните следующие действия:

- В поле **Число узлов мониторинга** задайте количество сетевых узлов, за состоянием которых будет следить выбранный сервер мониторинга.
- В поле **Число дочерних серверов мониторинга** задайте количество подчиненных серверов мониторинга для выбранного сервера.

Невозможно добавить больше узлов мониторинга и дочерних серверов, чем количество свободных лицензий, указанное под каждым полем ввода.

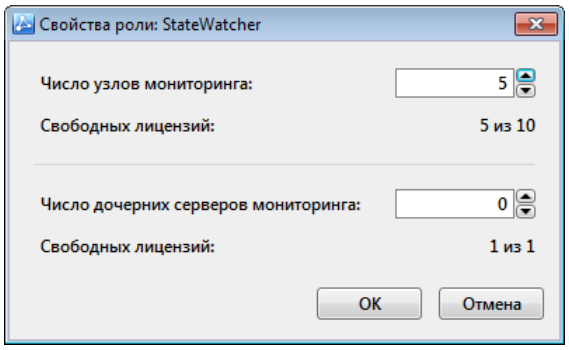

Рисунок 81. Изменение свойств роли «ViPNet StateWatcher»

3 Нажмите кнопку **OK**.

Подробнее о работе системы мониторинга сетевых узлов см. документ «Программный комплекс мониторинга защищенных сетей ViPNet StateWatcher. Общее описание».

Изменение допустимого числа запросов для роли «Registration Point»

Сетевой узел, на который добавлена роль «Registration Point», является центром регистрации пользователей. При необходимости вы можете ограничить количество запросов на дистрибутивы ключей и сертификаты пользователей, которые может создать центр регистрации. Для этого выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните роль «Registration Point» (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена эта роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 В окне **Свойства роли** выполните следующие действия:

- Чтобы разрешить центру регистрации создавать запросы на дистрибутивы ключей, установите флажок **Разрешить запросы на дистрибутивы** и в соответствующем поле укажите число запросов, которое может быть создано.
- Чтобы разрешить центру регистрации создавать запросы на сертификаты пользователей, установите флажок **Разрешить запросы на сертификаты** и в соответствующем поле укажите число запросов, которое может быть создано.

Оставшееся число запросов на дистрибутивы ключей или сертификаты, ограниченное лицензией на сеть ViPNet, вы можете посмотреть в соответствующих полях.

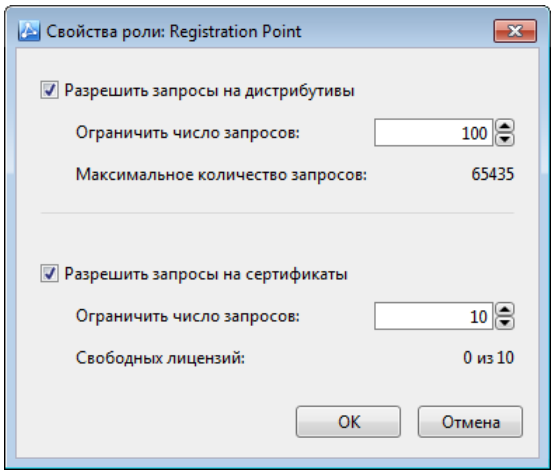

Рисунок 82. Изменение допустимого числа запросов

3 Нажмите кнопку **OK**.

Подробнее о работе центра регистрации см. документ «ViPNet Registration Point. Руководство администратора».

Настройка параметров роли «Terminal»

Роль «Terminal» позволяет установить на сетевом узле программное обеспечение ViPNet Terminal (ранее — ThinClient), которое обеспечивает защищенное подключение к удаленному рабочему столу или приложениям на терминальном сервере (см. глоссарий, стр. 308).

При добавлении на клиент роли «Terminal» вы можете задать параметры терминальных серверов, к которым будет подключаться пользователь, и полномочия пользователя при работе в терминальной сессии.

Чтобы задать параметры клиента с ролью «Terminal», выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните роль «Terminal» (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 На вкладке **Сессия** настройте полномочия пользователя ViPNet Terminal и параметры терминала (см. «Настройка полномочий пользователя ViPNet Terminal» на стр. 153).

3 На вкладке **Подключение к серверу** задайте список терминальных серверов, которые будут использоваться на узле (см. «Изменение списка терминальных серверов» на стр. 160).

   Если требуется указать параметры терминального сервера, которые поддерживаются программным обеспечением ViPNet Terminal, но отсутствуют в окне **Параметры подключения к серверу** (см. рисунок на стр. 161), вы можете задать эти параметры на вкладке **Пользовательские** (см. «Добавление пользовательских параметров» на стр. 164).

4 При необходимости на вкладке **USB-модем** настройте параметры подключения USB-модема к узлу (см. «Настройка параметров подключения USB-модема в терминальной сессии» на стр. 155).

5 На вкладке **Прокси** настройте параметры доступа к веб-ресурсам через прокси-сервер в терминальной сессии (см. «Настройка параметров прокси-сервера для веб-браузера» на стр. 157).

6 В окне **Свойства роли: Terminal** нажмите кнопку **OK**.

Настройка полномочий пользователя ViPNet Terminal

Чтобы задать полномочия пользователя ViPNet Terminal при работе в терминальной сессии и настроить параметры терминала, в окне **Свойства роли: Terminal** выполните следующие действия:

1 Перейдите на вкладку **Сессия**.

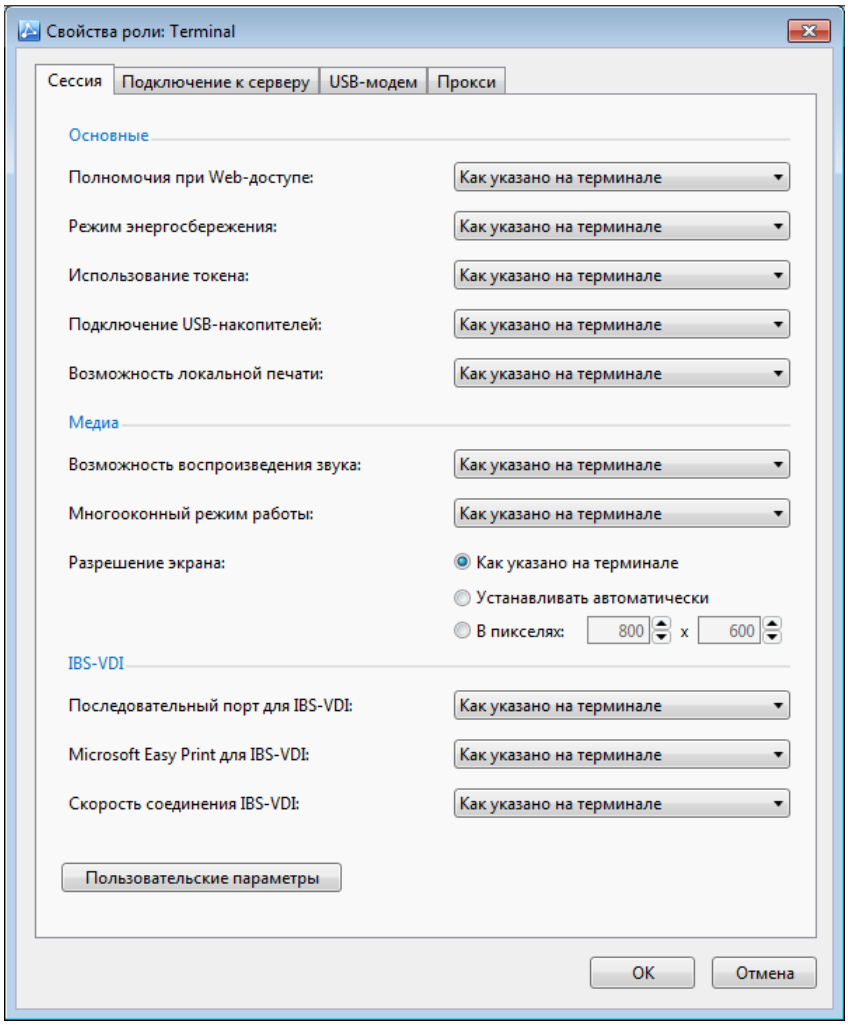

Рисунок 83. Настройка полномочий пользователя ViPNet Terminal

2 Задайте режим работы веб-браузера на терминале. Для этого в группе **Основные** в списке **Полномочия при Web-доступе** выберите одно из значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Администратор** — в этом режиме доступны все элементы управления веб-браузера, в окне веб-браузера могут быть открыты дополнительные вкладки.
- **Пользователь** — в этом режиме скрыты меню, адресная строка и другие элементы управления веб-браузера, в окне веб-браузера невозможно открыть дополнительные вкладки.

3 Настройте режим энергосбережения экрана. Для этого в группе **Основные** в списке **Режим энергосбережения** выберите одно из значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Включено** — режим энергосбережения включен. При отсутствии действий пользователя через 5 минут гаснет изображение на экране, через 30 минут отключается питание монитора.
- **Выключено** — режим энергосбережения выключен.

4 Задайте полномочия пользователя ViPNet Terminal при подключении к терминальному серверу в группе **Основные**:

- **Использование токена** — использование устройства аутентификации, в том числе для формирования электронной подписи с помощью ключей, хранящихся на устройстве.
- **Подключение USB-накопителей** — использование USB-накопителей для копирования файлов между локальным компьютером и терминальным сервером.
- **Возможность локальной печати** — использование локального принтера, подключенного к терминалу, для печати документов в терминальной сессии.

Для каждой функции вы можете выбрать в списке одно из следующих значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Включено** — разрешить использование функции.
- **Отключено** — запретить использование функции.

5 Задайте возможность воспроизведения звука и использования звуковых устройств, подключенных к терминалу. Для этого в группе **Медиа** в списке **Возможность воспроизведения звука** выберите одно из значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Включено** — разрешить использование функции.
- **Отключено** — запретить использование функции.

6 Настройте режим работы графического интерфейса ViPNet Terminal. Для этого в группе **Медиа** в списке **Многооконный режим работы** выберите одно из значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Включено** — многооконный режим работы, в котором на рабочем столе может быть одновременно открыто несколько окон терминальных сессий и веб-браузера Firefox.

- **Выключено** — полноэкранный режим работы, в котором автоматически выполняется подключение к терминальному серверу по умолчанию, окно терминальной сессии или веб-браузера Firefox разворачивается на весь экран.

7 Задайте разрешение экрана терминала. Для этого в группе **Медиа** установите переключатель **Разрешение экрана** в одно из положений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Устанавливать автоматически** — автоматически определять оптимальное разрешение экрана.
- **В пикселях** — указать фиксированное разрешение экрана. При выборе этого варианта в соответствующих полях введите размер экрана в пикселях по горизонтали и по вертикали.

8 Задайте настройки подключения пользователя к виртуальному рабочему столу IBS, использующему технологию Parallels VDI, в группе **IBS-VDI**:

- **Последовательный порт для IBS-VDI —** возможность использовать последовательный порт.
- **Microsoft Easy Print для IBS-VDI —** возможность печати в терминальной сессии при подключении пользователя к виртуальному рабочему столу.

Для указанных функций вы можете выбрать в списке одно из следующих значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Включено** — разрешить использование функции.
- **Отключено** — запретить использование функции.

9 Выберите скорость соединения при подключении пользователя ViPNet Terminal к виртуальному рабочему столу IBS, использующему технологию Parallels VDI. Для этого в группе **IBS-VDI** в списке **Скорость соединения IBS-VDI** выберите одно из значений, соответствующее скорости канала подключения ViPNet Terminal к серверу. Значение **По умолчанию** использует значение **Глобальная сеть (10 Мбит/с или выше с большой задержкой)**.

Настройка параметров подключения USB-модема в терминальной сессии

При необходимости организации терминальной сессии через сотовую сеть передачи данных вы можете использовать USB-модем на узле с ПО ViPNet Terminal. Для этого вы можете централизовано настроить для узла с ролью «ViPNet Terminal» параметры подключения USB-модема.

Чтобы задать параметры подключения USB-модема, выполните следующие действия:

1 В окне **Свойства роли узла: Terminal** перейдите на вкладку **USB-модем**.

2 Чтобы включить или отключить использование USB-модема в терминальной сессии, в списке **Способ включения USB-модема** выберите одно из значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Включен** — разрешить использование USB-модема.
- **Выключен** — запретить использование USB-модема.

3 Если требуется указать ПИН-код, введите его в соответствующее поле.

4 Чтобы удалить ПИН-код, установите флажок **Сброс ПИН-кода.**

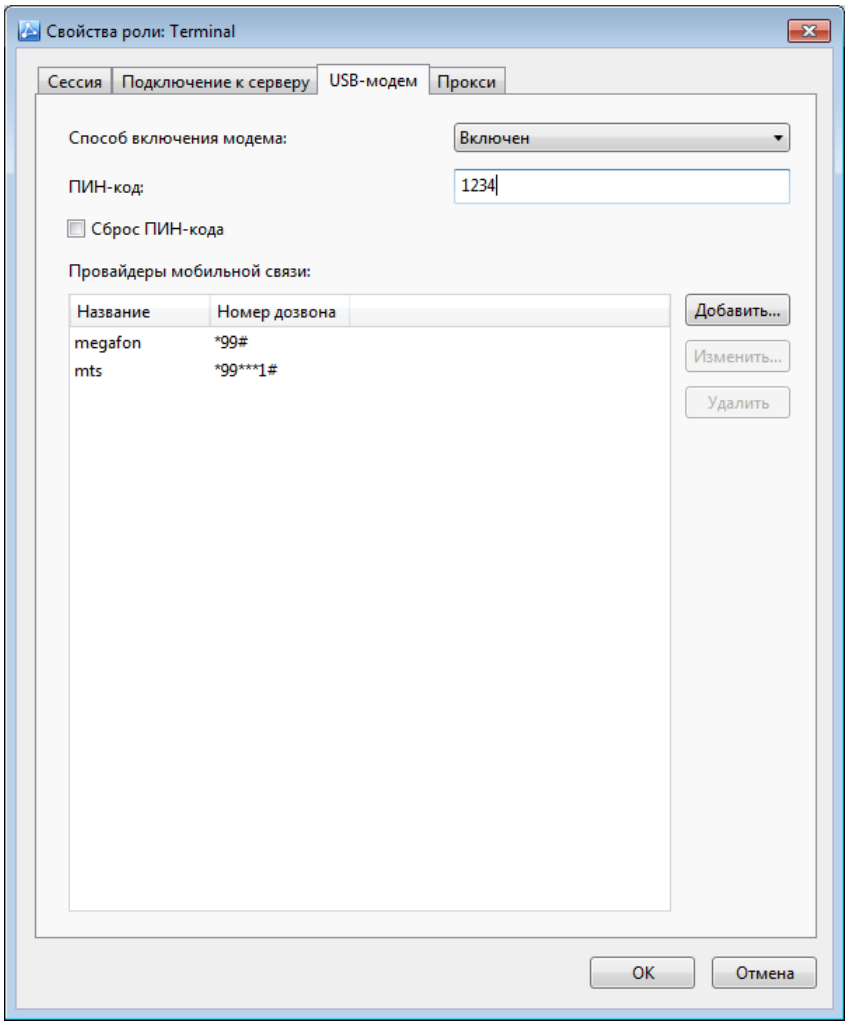

Рисунок 84. Настройка параметров подключения USB-модема в терминальной сессии

5 При необходимости добавьте информацию о провайдерах мобильной связи, услугами которых вы пользуетесь. Для этого в группе **Провайдеры мобильной связи** нажмите кнопку **Добавить**. В появившемся окне **Провайдер мобильной связи** укажите следующую информацию:

- В поле **Название** — введите имя провайдера мобильной связи.
- В поле **Номер дозвона** — введите номер дозвона до провайдера мобильной связи.

6 Чтобы задать адрес сервера, используемого при соединении с сетью передачи данных провайдера мобильной связи, в группе **Точка доступа (APN)** в поле **IP-адрес** или **DNS-имя** введите IP-адрес или DNS-имя сервера.

7 При необходимости задайте имя учетной записи и пароль для авторизации при подключении к провайдеру мобильной связи в соответствующих полях.

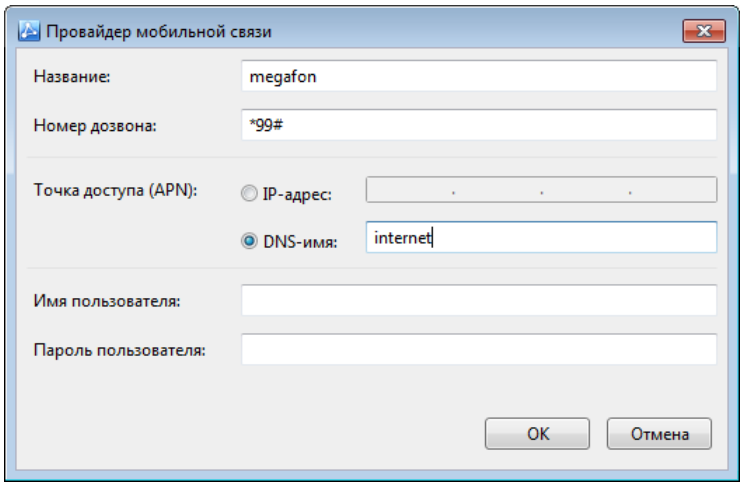

Рисунок 85. Задание параметров провайдера мобильной связи для USB-модема в терминальной сессии

Настройка параметров прокси-сервера для веб-браузера

Если в сети для узла ViPNet Terminal доступ в Интернет осуществляется через прокси-сервер, вы можете задать параметры доступа к этому серверу. Прокси-сервер используется для всех подключений, кроме тех, которые добавлены в исключения.

Чтобы задать параметры прокси-сервера для веб-браузера, выполните следующие действия:

1 В окне **Свойства роли узла: Terminal** перейдите на вкладку **Прокси**.

2 Чтобы включить использование прокси-сервера, установите флажок **Использовать прокси-сервер для всех подключений**.

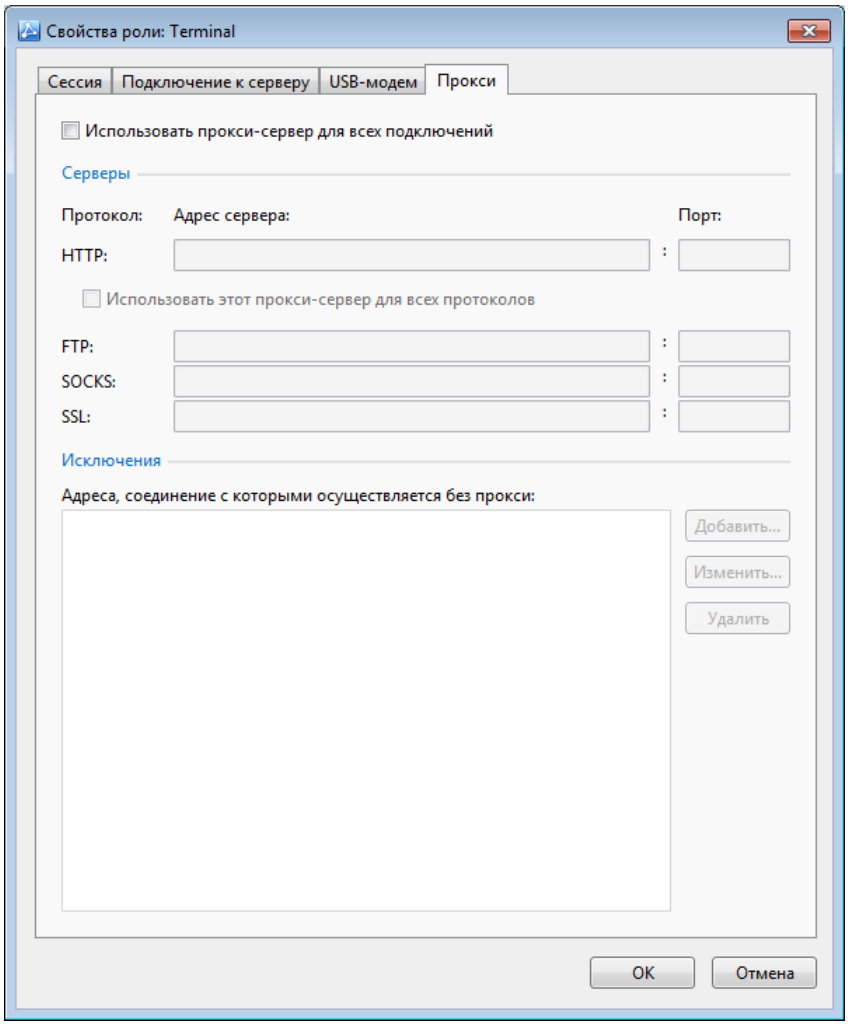

Рисунок 86. Настройка параметров прокси-сервера для веб-браузера

3 В строках протоколов, для которых планируется использовать прокси-серверы (HTTP, FTP, SOCKS или SSL), укажите следующую информацию:

- В поле **Адрес сервера** введите IP-адрес или DNS-имя прокси-сервера.
- В поле **Порт** задайте номер сетевого порта прокси-сервера.

4 Чтобы задать один прокси-сервер, тот, который задан для HTTP, для всех протоколов, установите флажок **Использовать этот прокси-сервер для всех протоколов**.

5 Чтобы добавить адрес, для соединения с которым не будет использоваться прокси-сервер, в группе **Исключения** нажмите кнопку **Добавить**. В появившемся окне в поле **IP-адрес** или **DNS-имя** введите нужный адрес.

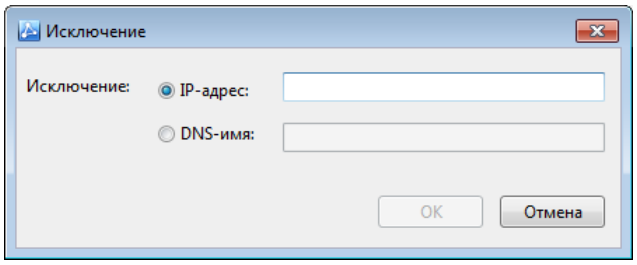

Рисунок 87. Задание адреса подключения без использования прокси-сервера

6 Чтобы изменить или удалить заданный адрес, для которого не будет использоваться прокси-сервер, выберите его в списке и нажмите соответствующую кнопку.

Настройка дополнительных параметров терминала

При необходимости с помощью программы ViPNet Центр управления сетью вы можете задать для узла с ролью «Terminal» дополнительные параметры терминала, которые поддерживаются программным обеспечением ViPNet Terminal, но отсутствуют на вкладке **Сессия**.

Примечание. Информацию о параметрах сессии, поддерживаемых программным обеспечением ViPNet Terminal (ранее — ViPNet ThinClient), см. в документе «ViPNet Terminal. Руководство администратора».

Для этого выполните следующие действия:

1 При настройке полномочий пользователя ViPNet Terminal на вкладке **Сессия** нажмите кнопку **Пользовательские параметры**.

2 Чтобы добавить новый параметр, нажмите кнопку **Добавить**.

Чтобы изменить значение существующего параметра, выберите его в списке и нажмите кнопку **Изменить**.

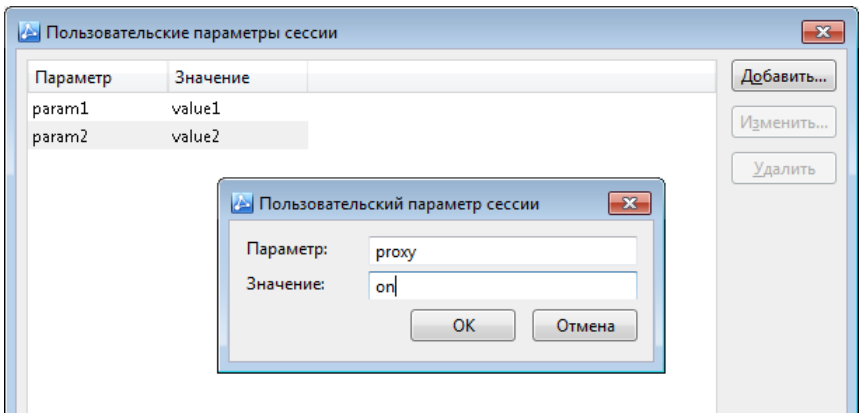

Рисунок 88. Добавление пользовательских параметров сессии

3 В окне **Пользовательский параметр сессии** в соответствующих полях укажите имя параметра и его значение, затем нажмите кнопку **OK**.

Изменение списка терминальных серверов

Чтобы указать терминальные серверы (см. глоссарий, стр. 308), к которым сможет подключаться пользователь ViPNet Terminal, в окне **Свойства роли: Terminal** выполните следующие действия:

1 Перейдите на вкладку **Подключение к серверу**.

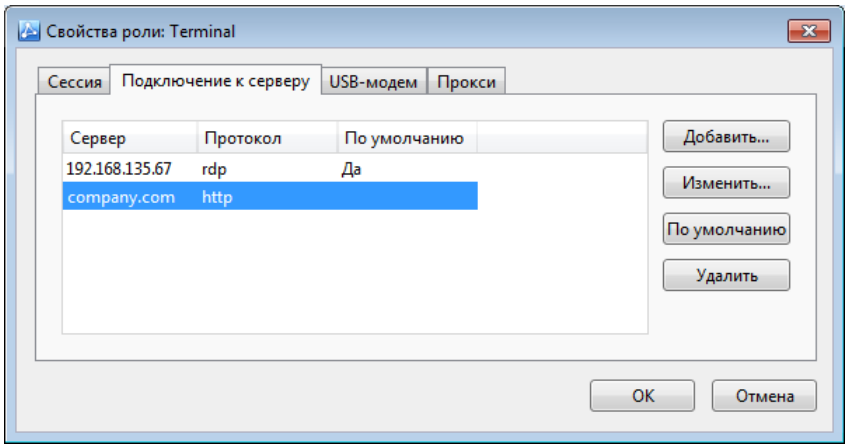

Рисунок 89. Список терминальных серверов

2 Чтобы добавить терминальный сервер, нажмите кнопку **Добавить** и задайте параметры подключения (см. «Настройка параметров подключения к терминальному серверу» на стр. 160).

3 Чтобы изменить параметры терминального сервера, выберите его в списке и нажмите кнопку **Изменить**, затем задайте необходимые параметры

4 Чтобы выбрать терминальный сервер для подключения по умолчанию в полноэкранном режиме работы ViPNet Terminal (см. «Настройка полномочий пользователя ViPNet Terminal» на стр. 153), выберите его в списке и нажмите кнопку **По умолчанию**.

5 Чтобы удалить терминальный сервер из списка, выберите его и нажмите кнопку **Удалить**.

Настройка параметров подключения к терминальному серверу

Чтобы настроить подключение к терминальному серверу, в окне **Параметры подключения к серверу** выполните следующие действия:

1 На вкладке **Сервер** укажите адрес терминального сервера. Для этого в группе **Подключение** выберите один из вариантов:

- Для подключения к серверу по IP-адресу выберите пункт **IP-адрес** и в соответствующем поле введите IP-адрес терминального сервера.
- Для подключения к серверу по DNS-имени выберите пункт **DNS-имя** и в соответствующем поле введите DNS-имя терминального сервера.
- Для подключения к терминальному серверу, который расположен на защищенном узле ViPNet, выберите пункт **Сетевой узел**. Затем нажмите кнопку **Выбрать** и в открывшемся окне укажите нужный сетевой узел.

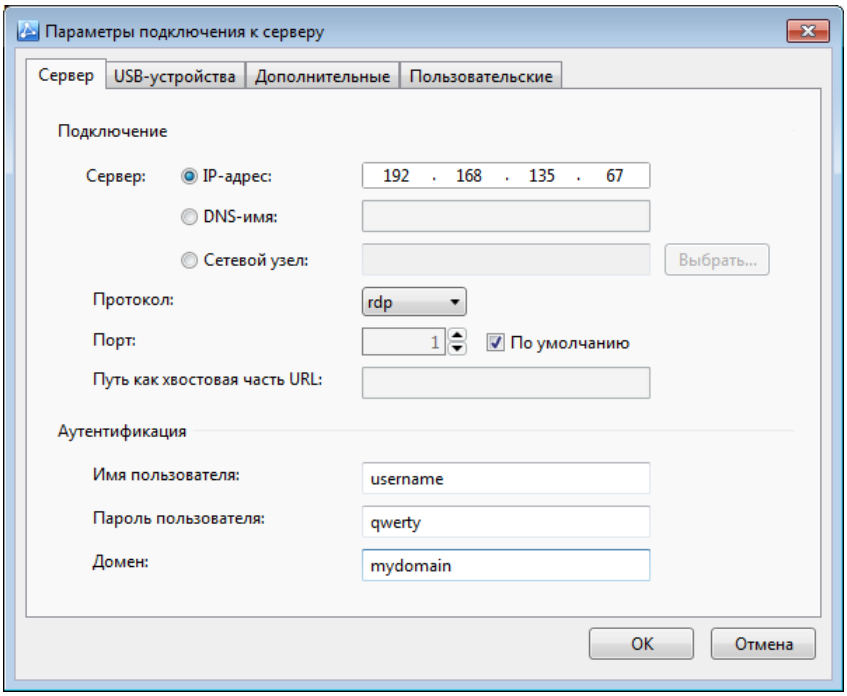

Рисунок 90. Настройка параметров подключения к серверу

2 В списке **Протокол** выберите протокол для подключения к терминальному серверу:

- **rdp** — для доступа к удаленному рабочему столу по протоколу RDP;
- **ica** — для доступа к удаленному рабочему столу или приложениям на сервере Citrix XenApp;
- **http** или **https** — для доступа к веб-сайтам или веб-приложениям;
- **ibs-vdi** — для доступа к виртуальному рабочему столу IBS.

3 При необходимости измените порт доступа к терминальному серверу. Для этого рядом с полем **Порт** снимите флажок **По умолчанию** и укажите нужный номер порта.

4 При необходимости для аутентификации пользователя на терминальном сервере соответствующих полях укажите:

- Имя пользователя.
- Пароль.
- Домен (только при подключении по протоколу RDP, ICA и IBS-VDI).

5 Если для подключения используется протокол HTTP или HTTPS, при необходимости в поле **Путь как хвостовая часть URL** введите относительный URL-адрес страницы или веб-приложения на сервере.

Например, если для сервера с адресом `myserver.com` задан относительный URL-адрес `myapplication`, подключение к серверу будет выполняться по адресу `http://myserver.com/myapplication`.

6 Чтобы удаленно подключить USB-устройство к серверу из терминальной сессии, для этого на вкладке **USB-устройства** выполните следующие действия:

- В группе **Классы перенаправляемых USB-устройств** добавьте номер классов перенаправляемых USB-устройств в виде шестнадцатеричного двухразрядного числа, принимающего значения от 00 до FF.

  Класс USB-устройства позволяет различать USB-устройства при их подключении к виртуальному или удаленному рабочему столу. Вы можете подсоединить к своему узлу USB-устройство и оно будет удаленно подключено к виртуальному рабочему столу (например, класс USB-устройств 01 перенаправляет звуковые аудиоустройства).

- В группе **Идентификаторы перенаправляемых USB-устройств** добавьте идентификационные коды производителя (VendorID, VID) и идентификационные коды продукта (изделия) (ProductID, PID) USB-устройств в виде двух шестнадцатеричных четырехсимвольных номеров от 0000 до FFFF, задаваемых по маске VID:PID.

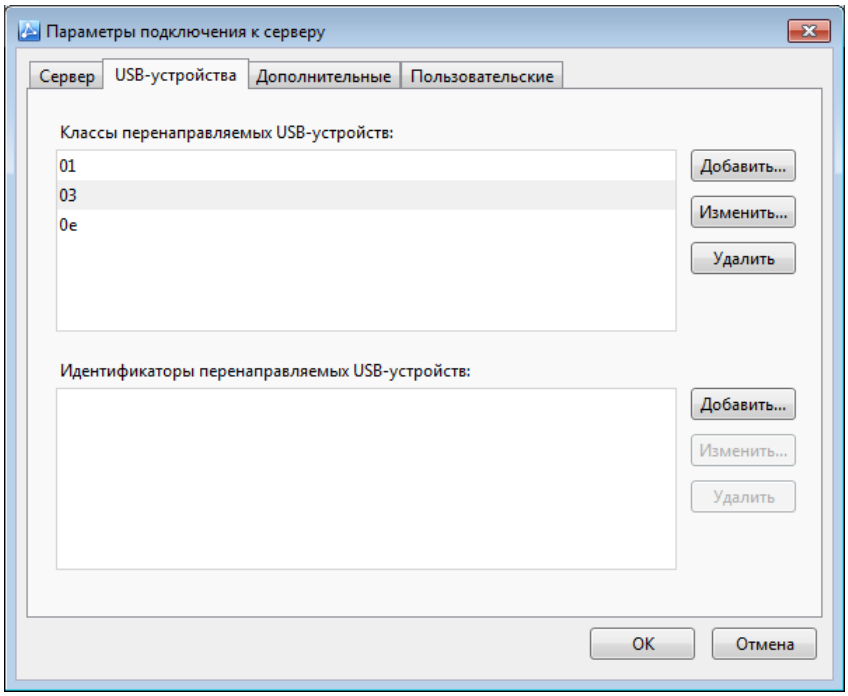

Рисунок 91. Настройка параметров перенаправляемых на сервер USB-устройств, подключаемых к узлу ViPNet Terminal в терминальной сессии

7 Если для подключения используется протокол ICA, при необходимости на вкладке **Дополнительные** вы можете настроить запуск приложения, опубликованного на сервере Citrix:

- В поле **Имя опубликованного приложения** введите имя приложения.
- Если вы указали имя приложения, в списке **Тип Citrix-сервера** выберите тип подключения к серверу:
  - **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
  - **Отдельный** — при подключении к отдельному серверу Citrix.
  - **Ферма** — при подключении к ферме серверов Citrix.

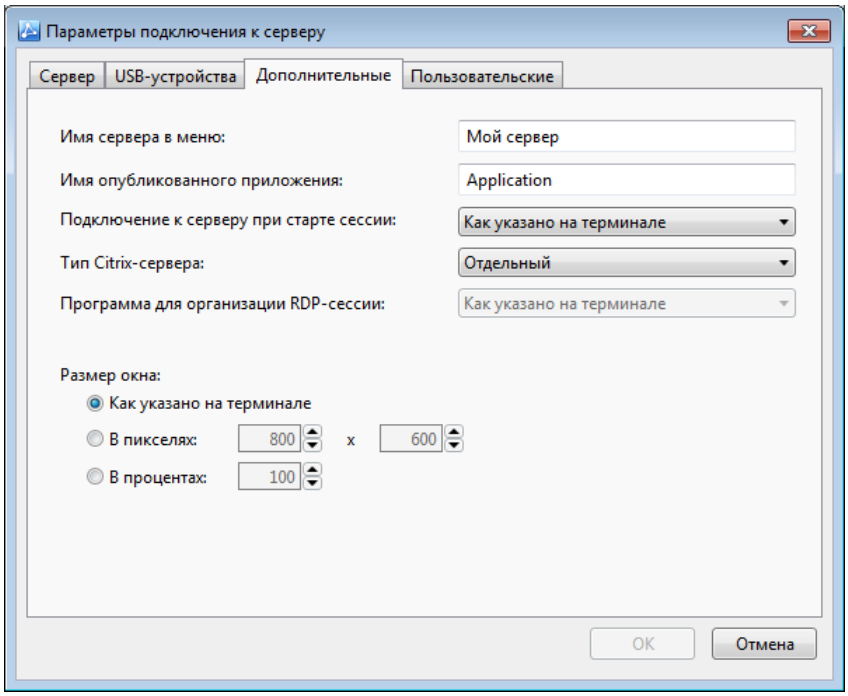

Рисунок 92. Дополнительные параметры терминального сервера

8 Если для подключения используется протокол RDP, вы можете выбрать RDP-клиент для работы с сервером. Для этого на вкладке **Дополнительные** в списке **Программа для организации RDP-сессии** выберите одно из значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Rdesktop** — клиент для работы с терминальными серверами Windows.
- **FreeRDP** — усовершенствованный клиент на основе Rdesktop.

9 При необходимости на вкладке **Дополнительные** в поле **Имя сервера в меню** введите имя, которое будет отображаться в списке терминальных серверов на узле ViPNet Terminal. По умолчанию имя сервера совпадает с адресом сервера (IP-адрес, DNS-имя либо имя сетевого узла ViPNet).

10 При необходимости укажите, требуется ли автоматическое подключение к данному серверу при запуске ViPNet Terminal. Для этого на вкладке **Дополнительно** в списке **Подключение к серверу при старте сессии** выберите одно из значений:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **Автоматически**.
- **Вручную**.

11 При необходимости укажите размер окна, в котором при подключении к серверу будет открываться терминальная сессия или веб-браузер. Для этого в группе **Размер окна** выберите один из вариантов:

- **Как указано на терминале** — сохранить параметры, заданные на узле ViPNet Terminal.
- **В пикселях** — указать абсолютный размер окна в пикселях. При выборе этого варианта в соответствующих полях задайте ширину и высоту окна.

- **В процентах** — чтобы указать размер окна в процентах относительно ширины и высоты экрана компьютера. При выборе этого варианта в соответствующем поле задайте размер окна в процентах.

12 Чтобы сохранить заданные параметры, нажмите кнопку **OK**.

Добавление пользовательских параметров

При необходимости вы можете также указать параметры терминального сервера, которые поддерживаются программным обеспечением ViPNet Terminal, но отсутствуют в окне **Параметры подключения к серверу**.

Примечание. Информацию о параметрах терминального сервера, поддерживаемых программным обеспечением ViPNet Terminal (ранее — ViPNet ThinClient), см. в документе «ViPNet Terminal. Руководство администратора».

Для этого выполните следующие действия:

1 При настройке параметров нового терминального сервера или при редактировании существующего терминального сервера (см. «Изменение списка терминальных серверов» на стр. 160) в окне **Параметры подключения к серверу** откройте вкладку **Пользовательские**.

2 Чтобы добавить параметр терминального сервера, нажмите кнопку **Добавить**.

Чтобы изменить значение существующего параметра, выберите его в списке и нажмите кнопку **Изменить**.

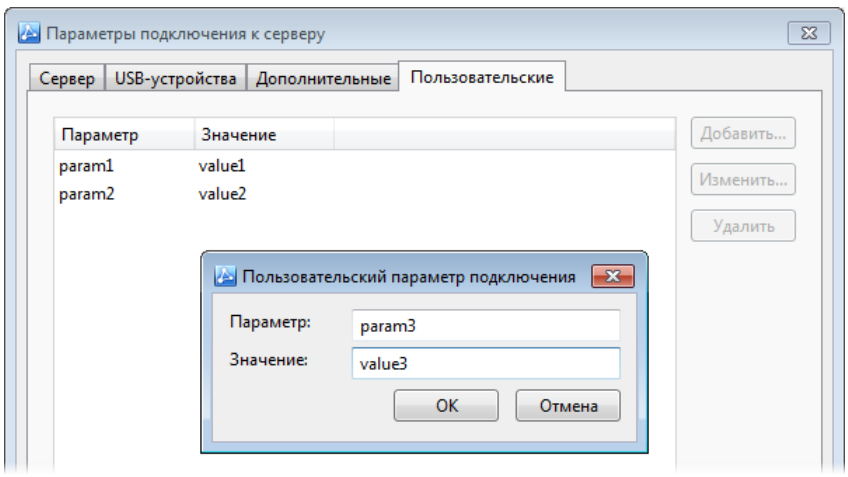

Рисунок 93. Добавление пользовательских параметров

3 В окне **Пользовательский параметр подключения** в соответствующих полях укажите имя параметра и его значение, затем нажмите кнопку **OK**.

Включение функции защищенного интернет-шлюза

Координаторы могут выполнять функцию защищенного интернет-шлюза, если на них добавлена одна из ролей:

- роль «Программный VPN-координатор»,
- роль из группы ролей «Coordinator HW».

Подробная информация о свойствах ролей приведена в приложении (см. «Роли сетевых узлов» на стр. 266).

Чтобы включить или отключить для координатора функцию защищенного интернет-шлюза, выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните нужную роль (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 В окне **Свойства роли: Программный VPN-координатор** установите или снимите флажок **Координатор является защищенным интернет-шлюзом**.

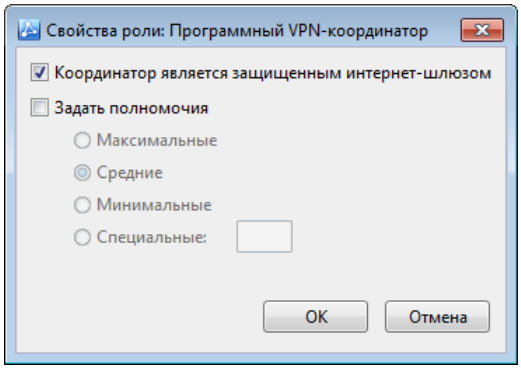

Рисунок 94. Включение функции защищенного интернет-шлюза

3 Нажмите кнопку **OK**.

Подробнее о функции защищенного интернет-шлюза (ранее — технология «Открытый Интернет») см. в документе «ViPNet Coordinator for Windows. Руководство администратора» либо в документе «ViPNet Coordinator HW. Сценарии работы».

Изменение числа элементов кластера для роли «Cluster Windows»

Для координатора, на который добавлена роль «Cluster Windows», требуется задать число элементов кластера. Для этого выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните роль «Cluster Windows» (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена эта роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 В окне **Свойства роли** в соответствующем поле задайте число элементов кластера, который будет развернут на выбранном сетевом узле. Невозможно добавить больше элементов кластера, чем количество свободных лицензий, указанное ниже поля ввода.

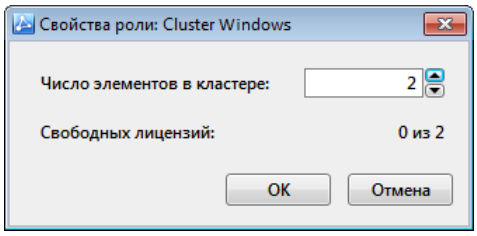

Рисунок 95. Изменение числа элементов кластера

3 Нажмите кнопку **OK**.

Подробнее о кластере ViPNet см. документ «ViPNet Cluster. Руководство администратора».

Настройка типа межсетевого экрана ПАК ViPNet Coordinator IG

Роли «Coordinator IG10 A/B» и «Coordinator IG100 A/B» (см. «Роли сетевых узлов» на стр. 266) позволяют развернуть координатор на базе соответствующих модификаций ПАК ViPNet Coordinator IG10 и ПАК ViPNet Coordinator IG100. При добавлении на координатор ролей «Coordinator IG10 A/B» и «Coordinator IG100 A/B» вы можете задать тип межсетевого экрана в свойствах роли.

В зависимости от требований ФСТЭК, предъявляемых к функциям безопасности межсетевых экранов, вы можете настроить межсетевой экран ПАК ViPNet Coordinator IG, выбрав один из следующих типов межсетевого экрана (см. глоссарий, стр. 308):

- межсетевой экран уровня сети (тип «А», настроен по умолчанию);
- межсетевой экран уровня промышленной сети (тип «Д»).

Информация о типе межсетевого экрана записывается в справочники и ключи и передается на сетевой узел по сети ViPNet. После получения справочников и ключей на сетевом узле

администратор ПАК ViPNet Coordinator IG сможет управлять режимами работы в соответствии с выбранным типом межсетевого экрана. Подробнее о режимах работы см. в комплекте документации на ПАК ViPNet Coordinator IG.

Чтобы настроить функции безопасности межсетевого экрана на координаторе на базе ПАК ViPNet Coordinator IG в соответствии с требованиями ФСТЭК, выполните следующие действия:

1 В списке ролей сетевого узла дважды щелкните роль «Coordinator IG10 A/B» или «Coordinator IG100 A/B» (см. «Изменение списка ролей сетевого узла» на стр. 142) либо в списке сетевых узлов, на которые добавлена роль, выберите сетевой узел и нажмите кнопку **Свойства** (см. «Групповое добавление ролей на сетевые узлы» на стр. 144).

2 В окне **Свойства роли** в списке **Тип межсетевого экрана на сетевом узле** выберите необходимый вам тип межсетевого экрана, определенный требованиями ФСТЭК (см. глоссарий, стр. 308).

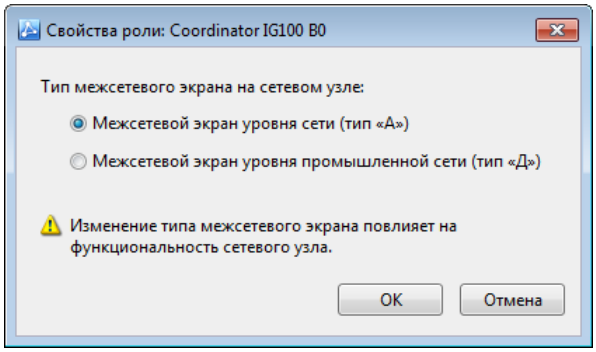

Рисунок 96. Настройка типа межсетевого экрана для ПАК ViPNet Coordinator IG

3 Нажмите кнопку **OK**.

4 После выбора типа межсетевого экрана создайте справочники и ключи и отправьте их на сетевой узел (см. «Обновление справочников и ключей» на стр. 87). Информация о функциях безопасности межсетевого экрана будет отправлена в составе справочников и ключей на сетевой узел ПАК ViPNet Coordinator IG по сети ViPNet.

В результате администратор сетевого узла с ПАК ViPNet Coordinator IG получит возможность управлять режимами работы в соответствии с выбранным типом межсетевого экрана.

Настройка защищенных DNS-серверов

При удаленном подключении к корпоративным ресурсам, расположенным в защищенной сети ViPNet, устройства мобильных клиентов и удаленных пользователей получают сетевые настройки из разных локальных сетей и сетей передачи данных. Для пользователя список доступных DNS-серверов может включать публичные DNS-серверы. При подключении из публичной сети к ресурсам сети ViPNet DNS-запрос может быть отправлен на публичные DNS-серверы. Это создает возможность атаки с подменой ресурса, при которой клиент в ответ на DNS-запрос получит IP-адрес сайта, контролируемого злоумышленником, и перейдет на него. Рекомендуется запросы на разрешение имен корпоративных ресурсов отправлять на выделенные защищенные DNS-серверы, для этого в ЦУСе необходимо задать доменные зоны для выбранного списка защищенных DNS-серверов. Для использования таких DNS-серверов на клиентах укажите их в настройках сетевого узла (см. «Настройка списков DNS- и WINS-серверов сетевого узла» на стр. 172).

По умолчанию защищенные DNS-серверы обрабатывают публичные ресурсы, то есть запросы всех ресурсов будут отправляться на защищенные DNS-серверы.

При разрешении DNS-имени клиент автоматически определяет, к какой доменной зоне относится запрашиваемое DNS-имя — к доменной зоне публичной или корпоративной сети. Список защищенных доменных зон и закрепленных за ними DNS-серверов передается на сетевые узлы в составе справочников.

В случаях если сеть ViPNet имеет не взаимодействующие между собой DNS-серверы, обслуживающие отдельные корпоративные ресурсы, такие DNS-серверы вам следует добавить в разные группы DNS-серверов (см. глоссарий, стр. 302) и задать для каждой группы список доменных зон.

Настройка списка защищенных DNS-серверов и доменных зон

Чтобы настроить список доменных зон, обслуживаемых выделенными защищенными DNS-серверами, выполните следующие действия:

1 В главном окне программы ViPNet Центр управления сетью в представлении **Моя сеть** на панели навигации выберите раздел **DNS-серверы и DNS-зоны**.

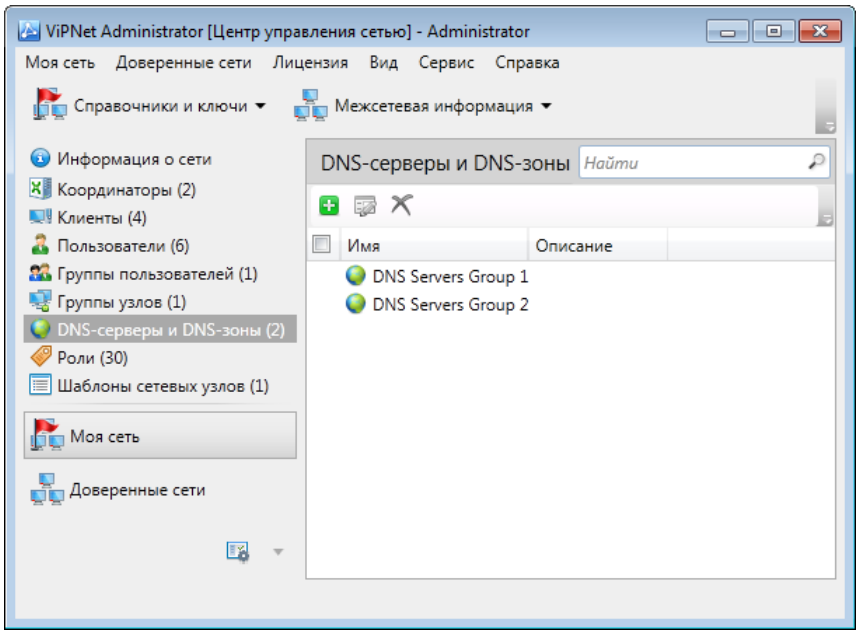

Рисунок 97. Создание списка защищенных DNS-серверов и доменных зон

2 Чтобы создать список выделенных защищенных DNS-серверов, обслуживающих корпоративные доменные зоны, на панели инструментов нажмите кнопку .

3 В появившемся окне введите название новой группы DNS-серверов и нажмите кнопку **Создать**.

4 В окне **Свойства группы DNS-серверов** в разделе **Основные параметры** при необходимости измените имя и описание группы DNS-серверов.

5 Чтобы для списка доменных зон выделить защищенные DNS-серверы, выберите раздел **DNS-серверы** и нажмите кнопку **Добавить.** Добавьте в разные группы DNS-серверы, не взаимодействующие между собой.

6 В открывшемся окне **Выбор объектов** выберите из списка один или несколько DNS-серверов. В окне отображены сетевые узлы, на которые добавлена роль DNS-сервер (см. «Добавление ролей „DNS-Сервер" и «WINS-Сервер»» на стр. 148).

Примечание. Если DNS-сервер добавлен в одну группу DNS-серверов, он не доступен для добавления в другой группе.

---

7 Чтобы запретить обрабатывать защищенным DNS-серверам DNS-имена сети Интернет, снимите флажок **DNS-серверы поддерживают разрешение имен публичных ресурсов**. По умолчанию флажок включен и от него зависит отображение флажка **Использовать для разрешения имен публичных ресурсов только заданные DNS-серверы** в настройках DNS-серверов сетевого узла (см. «Настройка списков DNS- и WINS-серверов сетевого узла» на стр. 172).

8 Чтобы добавить DNS-сервер доверенной сети, установите в группе **Отображать объекты** флажок **Доверенных сетей**.

9 Чтобы удалить DNS-сервер из списка защищенных DNS-серверов, нажмите соответствующую кнопку.

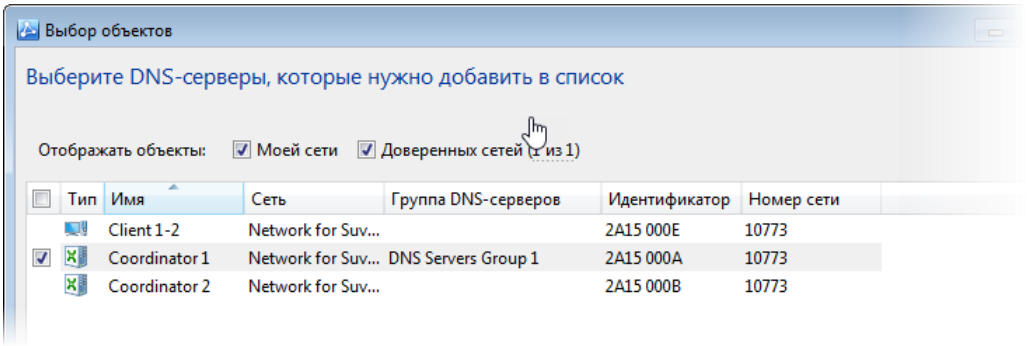

Рисунок 98. Добавление корпоративных DNS-серверов в список заданной группы DNS-серверов

10 Чтобы добавить доменную зону в список, выберите раздел **DNS-зоны** и на панели просмотра нажмите кнопку **Добавить**.

Одна и та же DNS-зона не может быть добавлена в группу DNS-серверов, если она уже используется в другой группе.

Для записи имени доменной зоны могут быть использованы строчные и прописные буквы, цифры и специальные символы «дефис» и «точка». Запись начинается с буквы и может заканчиваться буквой или цифрой.

Максимальное количество доменных зон в списке — 300.

11 Чтобы удалить или изменить доменную зону из списка, на панели просмотра нажмите соответствующую кнопку.

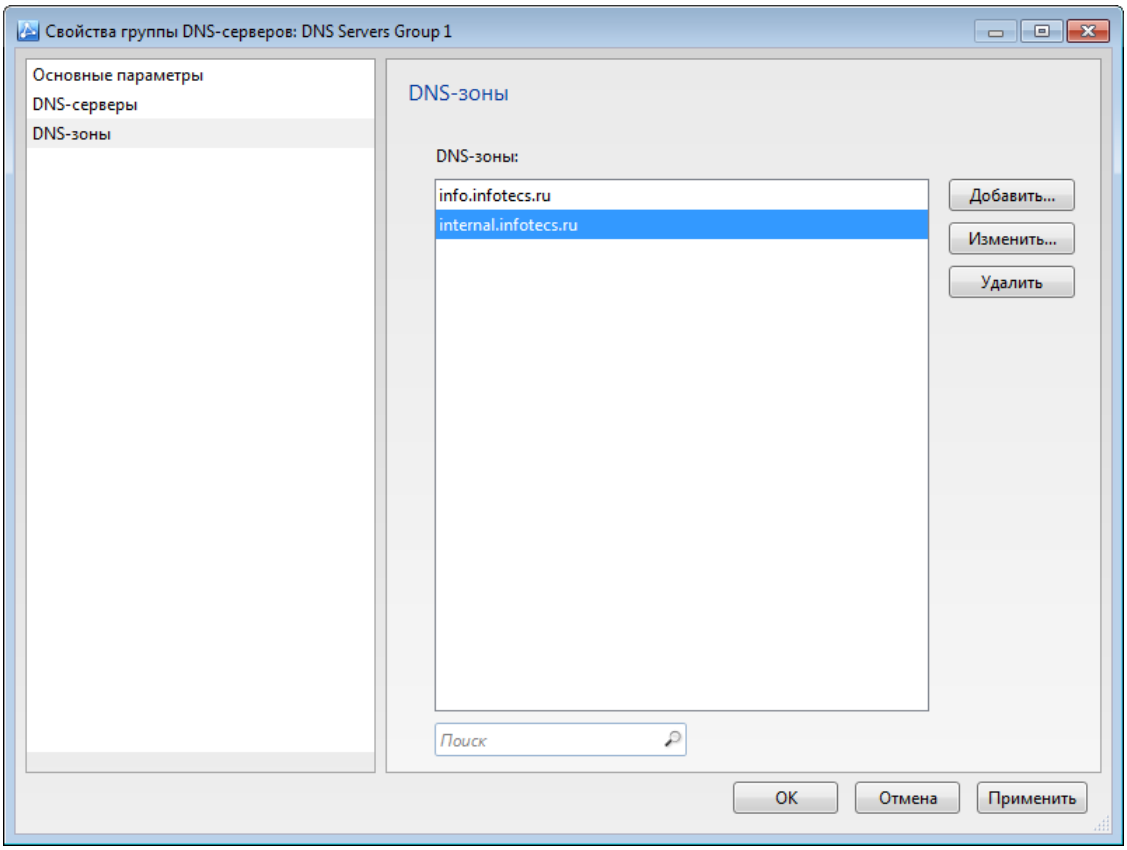

Рисунок 99. Добавление доменных зон, обслуживаемых группой DNS-серверов

Примечание. Если добавлено имя доменной зоны, которое включает доменную зону из списка, доменная зона в списке будет заменена. Например, если список **DNS-зоны** содержит доменную зону info.infotecs.ru и добавлена доменная зона infotecs.ru, зона в списке будет заменена на infotecs.ru.

Если добавляемая зона включает доменное имя зоны из списка (например, если список **DNS-зоны** содержит доменную зону infotecs.ru и добавлена доменная зона internal.infotecs.ru), добавление такой зоны невозможно.

12 Чтобы сохранить настройки, нажмите кнопку **OK**.

В списке **DNS-серверы и DNS-зоны** появится новая группа DNS-серверов.

13 Чтобы удалить группу DNS-серверов, на панели инструментов нажмите кнопку .

Примечание. При удалении группы DNS-серверов список DNS-серверов сетевого узла остается неизменным. Вместе с группой DNS-серверов удаляются обслуживаемые доменные зоны.

Настройка списков DNS- и WINS-серверов сетевого узла

В качестве защищенного DNS- или WINS-сервера на сетевых узлах ViPNet можно указать любой узел своей или доверенной сети ViPNet, на который добавлена соответствующая роль (см. «Добавление ролей „DNS-Сервер“ и «WINS-Сервер»» на стр. 148). Список защищенных DNS- и WINS-серверов узла поступает на него вместе со справочниками. Чтобы записи о наиболее приоритетных DNS- и WINS-серверах для узлов не оказались в конце списка и не были проигнорированы, и чтобы узел не использовал недоступные ему DNS- и WINS-серверы, для каждого сетевого узла необходимо задать список DNS- и WINS-серверов и настроить приоритет их использования.

Для разрешения публичных ресурсов по умолчанию используются защищенные DNS-серверы. При необходимости для отдельных сетевых узлов вы можете разрешить использовать публичные DNS-сервера для запросов публичных ресурсов.

Чтобы настроить список DNS- или WINS-серверов сетевого узла, выполните следующие действия:

1. В окне ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.
3. На панели просмотра дважды щелкните сетевой узел, для которого требуется задать список DNS- или WINS-серверов.
4. В окне свойств узла на левой панели выберите раздел **DNS-серверы** или **WINS-серверы** в зависимости от того, какой список вы хотите настроить.
5. Чтобы добавить DNS- или WINS-сервер в соответствующий список, выполните следующие действия:

   5.1 Нажмите кнопку **Выбрать**. Откроется окно со списком узлов, на которые добавлена роль «DNS-Сервер» или «WINS-Сервер» (см. «Добавление ролей на сетевые узлы» на стр. 142). Если какой-либо координатор туннелирует DNS- или WINS-серверы и в параметрах соответствующей роли этого координатора будут указаны их IP-адреса, то данные адреса также будут отображены в списке.

   5.2 Для отображения DNS- или WINS-серверов доверенных сетей установите соответствующий флажок в разделе **Отображать объекты**.

Примечание. Координатор доверенной сети, который является шлюзовым для вашей сети и на который добавлена роль «DNS-Сервер» или «WINS-Сервер», будет отображаться в списке доступных DNS- или WINS-серверов только в том случае, если в межсетевом взаимодействии участвует зарегистрированный на этом координаторе пользователь (см. «Изменение списка объектов, участвующих в межсетевом взаимодействии» на стр. 243).

5.3 Выберите в списке один или несколько узлов, которые требуется добавить в список DNS- или WINS-серверов узла, и нажмите кнопку **OK**.

Примечание. DNS-серверами узла могут быть DNS-серверы из одной группы или не включенные в какую-либо группу (см. глоссарий, стр. 302). Все DNS-серверы сети рекомендуется включать в группы DNS-серверов.

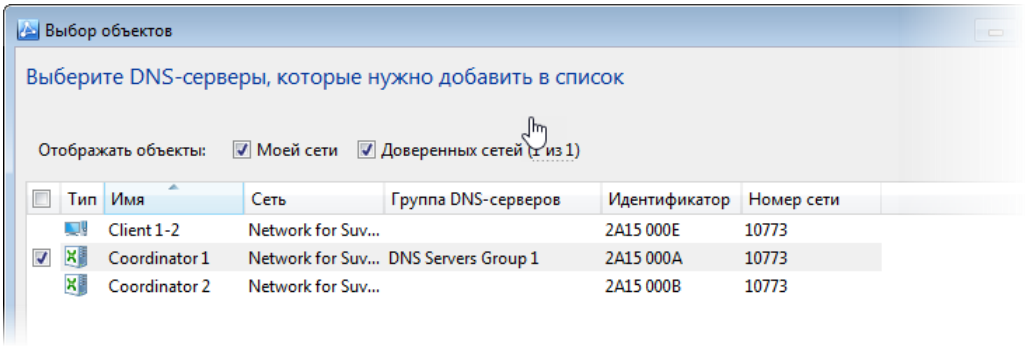

Рисунок 100. Выбор узлов для добавления в список DNS-серверов узла

6 Задайте приоритет добавленных DNS- или WINS-серверов, установив их положение в списке с помощью кнопок  и  . Для DNS- или WINS-серверов, туннелируемых координатором, приоритет можно изменять только по отношению к другим серверам, туннелируемым данным координатором.

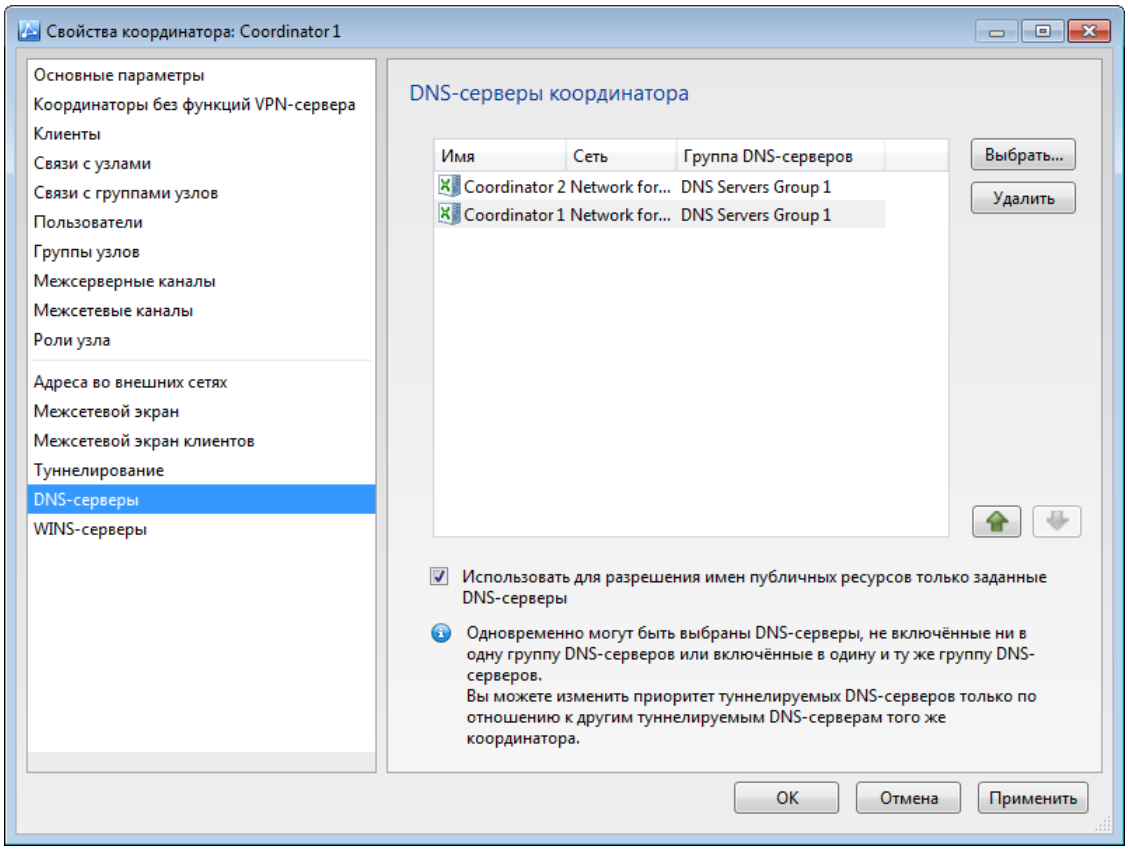

Рисунок 101. Настройка приоритета DNS-сервера

7 Чтобы изменить или удалить заданные DNS- или WINS-серверы, выберите их в списке и нажмите соответствующую кнопку.

8 Если необходимо отдельным сетевым узлам позволить отправлять DNS-запросы на разрешение имен интернет-ресурсов на публичные DNS-серверы, снимите флажок **Использовать для разрешения имен публичных ресурсов только заданные DNS-серверы**. В этом случае будет использоваться доступный DNS-сервер, в том числе публичный, на котором есть необходимая информация. По умолчанию флажок установлен.

Примечание. Флажок **Использовать для разрешения имен публичных ресурсов только заданные DNS-серверы** доступен, если в настройках групп DNS-серверов (см. «Настройка списка защищенных DNS-серверов и доменных зон» на стр. 168) установлен флажок **DNS-серверы поддерживают разрешение имен публичных ресурсов.**

9 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Задание адресов сетевого узла

Для того чтобы сетевые узлы ViPNet могли устанавливать соединения друг с другом, должны быть известны IP-адреса или DNS-имена других узлов.

Чтобы клиенты могли получить доступ к своим транспортным серверам и серверам IP-адресов, требуется задать адреса и другие параметры доступа к координаторам. Клиент получает информацию о параметрах доступа к сетевым узлам, с которыми он связан, от своего сервера IP-адресов. Для начала работы нового клиента в сети ViPNet достаточно, чтобы он мог установить соединение со своим сервером IP-адресов. Поэтому адреса клиентов задавать необязательно, достаточно выбрать для клиента сервер IP-адресов.

IP-адреса и DNS-имена сетевых узлов рекомендуется задать в программе ViPNet Центр управления сетью. В этом случае не потребуется вручную указывать эти адреса в программе ViPNet Монитор на каждом сетевом узле.

Задание IP-адресов сетевого узла

Чтобы изменить список IP-адресов сетевого узла, выполните следующие действия:

1. В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.
3. На панели просмотра дважды щелкните сетевой узел, IP-адреса которого требуется изменить.
4. В окне свойств узла на левой панели выберите раздел **Адреса во внешних сетях**.

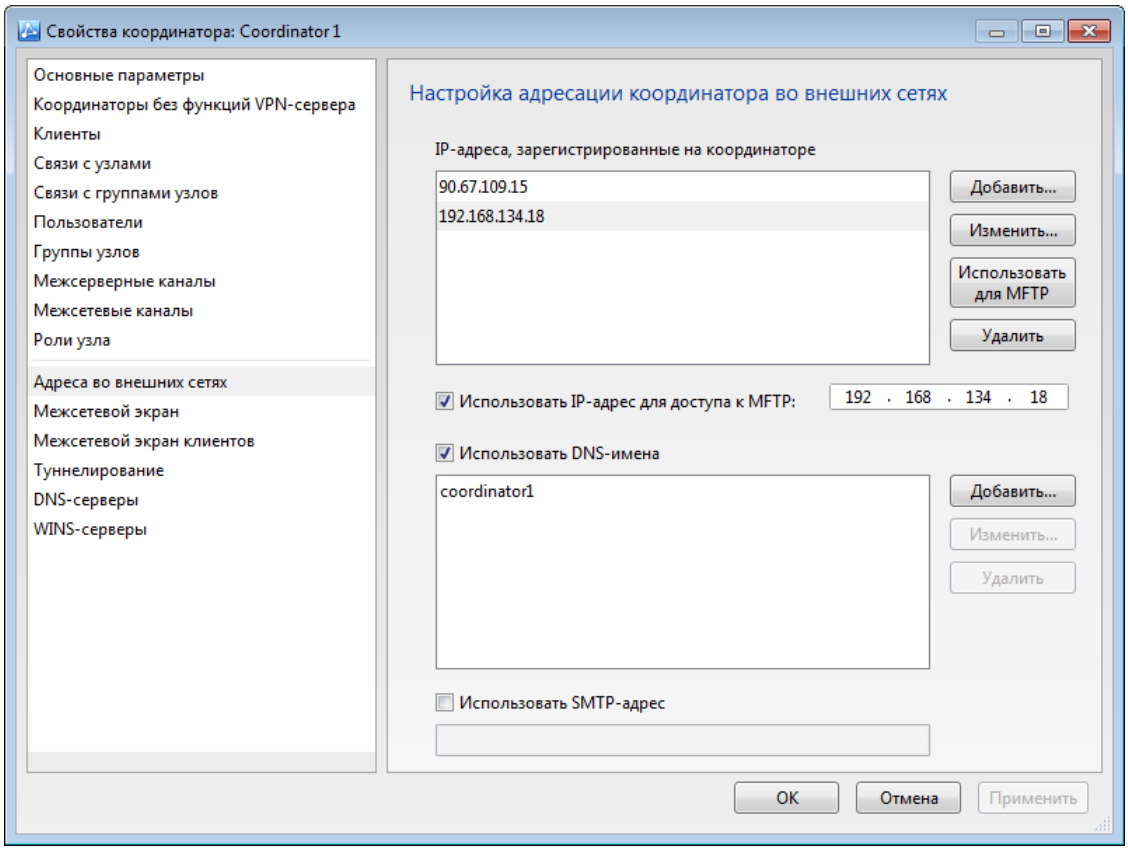

Рисунок 102. Задание адресов и DNS-имен сетевого узла

5 Чтобы добавить IP-адрес, нажмите кнопку **Добавить** рядом со списком адресов, в окне **IP-адрес** введите адрес и нажмите кнопку **OK**.

6 Если узел имеет несколько сетевых интерфейсов, добавьте IP-адрес для каждого из них.

7 Чтобы передавать транспортные конверты между узлами напрямую, укажите, по какому адресу к узлу будут подключаться другие узлы с помощью транспортного модуля MFTP. Для этого в списке IP-адресов выберите адрес и нажмите кнопку **Использовать для MFTP**. Выбранный IP-адрес будет скопирован и отобразится в соответствующем поле ниже.

   Используйте эту настройку для сетевых узлов с установленными программами, не использующими технологию VPN, например, для узлов с ролью «CryptoService».

8 Чтобы отключить возможность открытой передачи транспортных конвертов по каналу MFTP между узлами, снимите флажок **Использовать IP-адрес для доступа к MFTP**.

9 Чтобы изменить или удалить заданные IP-адреса, выберите их в списке и нажмите соответствующую кнопку.

10 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Задание DNS-имен сетевого узла

Чтобы изменить список DNS-имен сетевого узла, выполните следующие действия:

1. В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.
3. На панели просмотра дважды щелкните сетевой узел, DNS-имена которого требуется изменить.
4. В окне свойств узла на левой панели выберите раздел **Адреса во внешних сетях** (см. рисунок на стр. 176).
5. Если требуется доступ к сетевому узлу по DNS-имени, установите флажок **Использовать DNS-имена**. По умолчанию этот флажок снят.

   Изменение списка DNS-имен возможно только при установленном флажке **Использовать DNS-имена**.
6. Чтобы добавить DNS-имя, изменить или удалить заданное DNS-имя, воспользуйтесь соответствующей кнопкой.
7. Чтобы сохранить настройки, нажмите кнопку **Применить**.

Задание адреса для связи по каналу SMTP

Сетевые узлы могут использовать для обмена прикладными и служебными конвертами почтовые серверы. В этом случае транспортный модуль MFTP получает и отправляет транспортные конверты с определенного адреса электронной почты. Использование канала SMTP может быть полезно в том случае, если по каким-то причинам доступ в Интернет по протоколу TCP или UDP ограничен.

Чтобы задать адрес для подключения к узлу по каналу SMTP, выполните следующие действия:

1. В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа узла, который требуется настроить.
3. На панели просмотра дважды щелкните сетевой узел, SMTP-адреса которого требуется изменить.
4. В окне свойств узла на левой панели выберите раздел **Адреса во внешних сетях** (см. рисунок на стр. 176).
5. Если для подключения к сетевому узлу требуется использовать канал SMTP, установите флажок **Использовать SMTP-адрес**.
6. В поле под флажком введите адрес электронной почты, который будет использоваться для обмена транспортными конвертами.
7. Чтобы сохранить настройки, нажмите кнопку **Применить**.

Настройка параметров подключения к внешней сети

Параметры межсетевого экрана координатора

Если координатор не имеет прямого подключения к внешней сети, для него требуется задать настройки подключения через межсетевой экран, который установлен между координатором и внешней сетью. Эти настройки рекомендуется задать в программе ViPNet Центр управления сетью, тогда не потребуется выполнять настройку подключения в программе ViPNet Монитор непосредственно на координаторе.

Рекомендации по выбору типа межсетевого экрана содержатся в разделе Параметры подключения защищенных узлов к внешней сети (на стр. 37).

Чтобы настроить подключение координатора к внешней сети, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Координаторы**.
3. На панели просмотра дважды щелкните координатор, который требуется настроить.
4. В окне свойств координатора на левой панели выберите раздел **Межсетевой экран**.

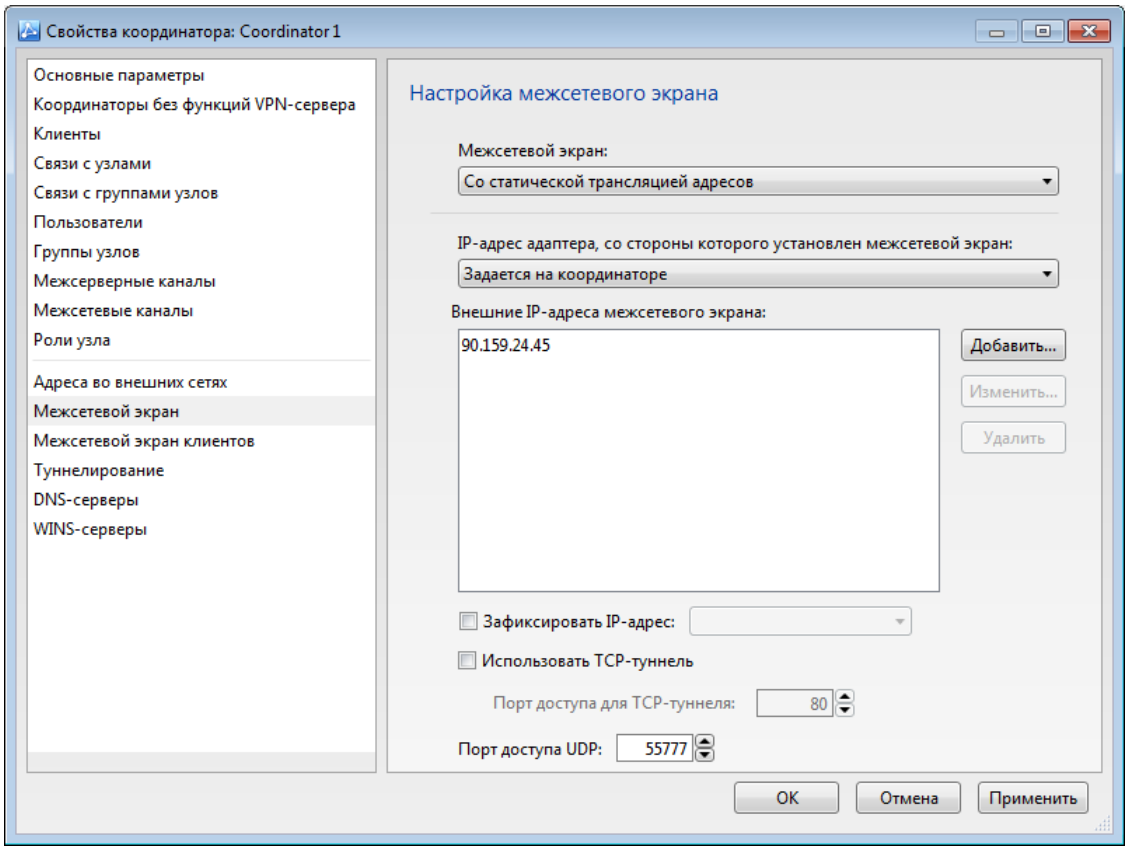

Рисунок 103. Настройка параметров межсетевого экрана координатора

5 Чтобы настроить подключение к внешней сети с использованием межсетевого экрана или отключить его использование, из списка **Межсетевой экран** выберите тип межсетевого экрана:

- **Не используется —** межсетевой экран не используется при подключении координатора к внешней сети.
- **Координатор в качестве межсетевого экрана** (см. «Настройка подключения через координатор в качестве межсетевого экрана» на стр. 185).
- **С динамической трансляцией адресов** (см. «Настройка подключения через межсетевой экран с динамической трансляцией адресов» на стр. 182).
- **Со статической трансляцией адресов** (см. «Настройка подключения через межсетевой экран со статической трансляцией адресов» на стр. 183).

По умолчанию для координаторов задано подключение через межсетевой экран со статической трансляцией адресов.

6 Из списка **IP-адрес адаптера, со стороны которого установлен межсетевой экран** выберите сетевой адаптер координатора, находящийся в одной подсети с межсетевым экраном, или оставьте значение по умолчанию **Задается на координаторе**.

7 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Параметры межсетевого экрана клиента

Если клиент не имеет прямого подключения к внешней сети, для него требуется задать настройки подключения через межсетевой экран, который установлен между клиентом и внешней сетью. Эти настройки рекомендуется задать в программе ViPNet Центр управления сетью, тогда не потребуется выполнять настройку подключения в программе ViPNet Монитор непосредственно на клиенте.

Примечание. Настройки подключения через межсетевой экран, заданные в ЦУСе, будут применяться только на клиентах с версией ПО ViPNet Client ниже 4.2. На клиентах с версией 4.2 и выше такие настройки отсутствуют, так как эти клиенты автоматически определяют параметры подключения к внешней сети и устанавливают взаимодействие с внешними узлами с помощью сервера соединений (см. глоссарий, стр. 306).

В ЦУСе можно либо задать общие настройки межсетевого экрана для всех конфигураций программы ViPNet Монитор на клиенте, либо задать настройки межсетевого экрана отдельно для каждой конфигурации.

Рекомендации по выбору типа межсетевого экрана содержатся в разделе Параметры подключения защищенных узлов к внешней сети (на стр. 37).

Чтобы настроить подключение клиента к внешней сети, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Клиенты**.
3. На панели просмотра дважды щелкните клиент, который требуется настроить.
4. В окне свойств клиента на левой панели выберите раздел **Межсетевой экран**.

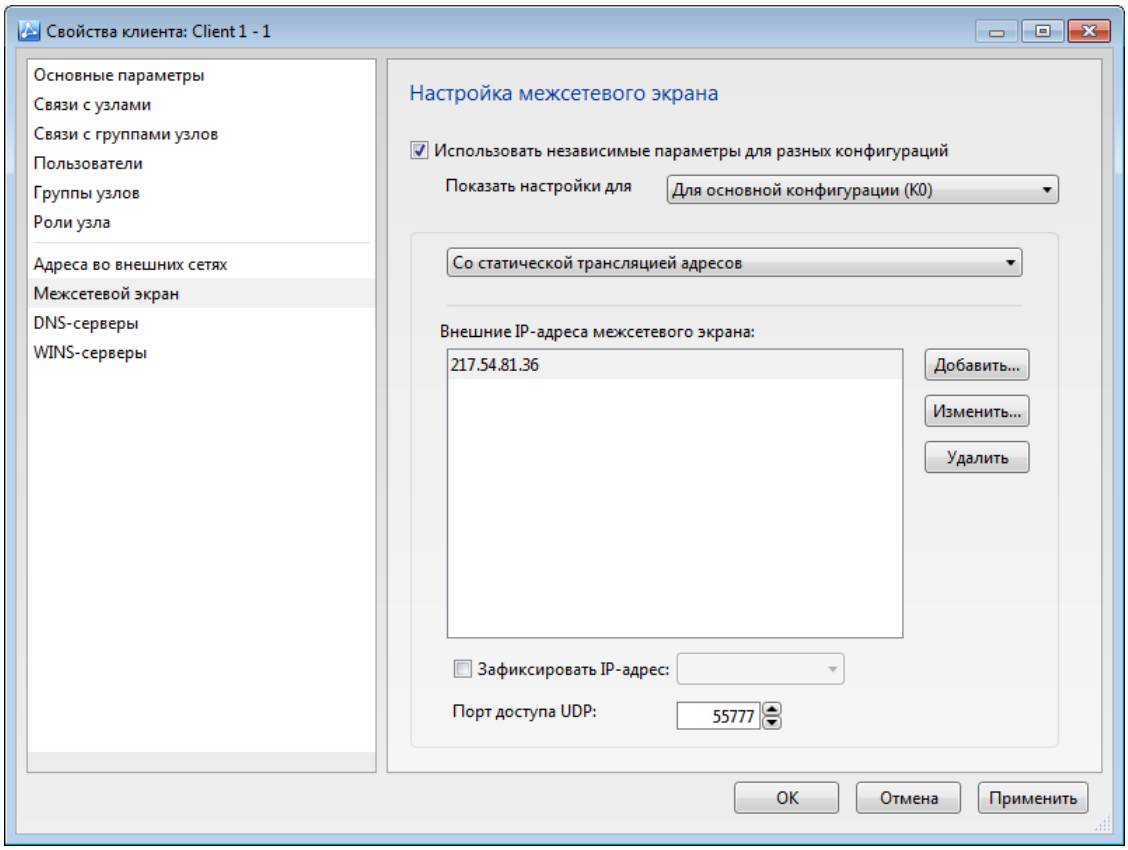

Рисунок 104. Настройка параметров межсетевого экрана клиента

5 Если требуется задать разные настройки межсетевого экрана для разных конфигураций программы ViPNet Монитор на клиенте, установите флажок **Использовать независимые параметры для разных конфигураций** и в списке **Показать настройки для** выберите конфигурацию для настройки.

По умолчанию флажок **Использовать независимые параметры для разных конфигураций** снят, то есть настройки заданы для всех конфигураций.

6 Чтобы настроить подключение к внешней сети с использованием межсетевого экрана или отключить его использование, щелкните стрелку в группе ниже и выберите тип межсетевого экрана:

- **Не используется —** межсетевой экран не используется при подключении клиента к внешней сети.
- **Со статической трансляцией адресов** (см. «Настройка подключения через межсетевой экран со статической трансляцией адресов» на стр. 183).
- **С динамической трансляцией адресов** (см. «Настройка подключения через межсетевой экран с динамической трансляцией адресов» на стр. 182).
- **Координатор в качестве межсетевого экрана** (см. «Настройка подключения через координатор в качестве межсетевого экрана» на стр. 185).
- **Согласно параметрам с сервера IP-адресов клиента** — в этом случае будут использоваться настройки межсетевого экрана, заданные на координаторе, который

назначен сервером IP-адресов клиента (см. «Настройка параметров межсетевого экрана клиентов на сервере IP-адресов» на стр. 186).

По умолчанию для клиентов задано подключение через межсетевой экран, заданный на сервере IP-адресов клиента (для всех конфигураций программы ViPNet Монитор).

7 В случае необходимости задайте настройки межсетевого экрана для других конфигураций программы ViPNet Монитор.

8 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Настройка подключения через межсетевой экран с динамической трансляцией адресов

Для настройки подключения через межсетевой экран с динамической трансляцией адресов выполните следующие действия:

1 В разделе **Настройка межсетевого экрана** (см. рисунок на стр. 179) в списке **Межсетевой экран** выберите пункт **С динамической трансляцией адресов**.

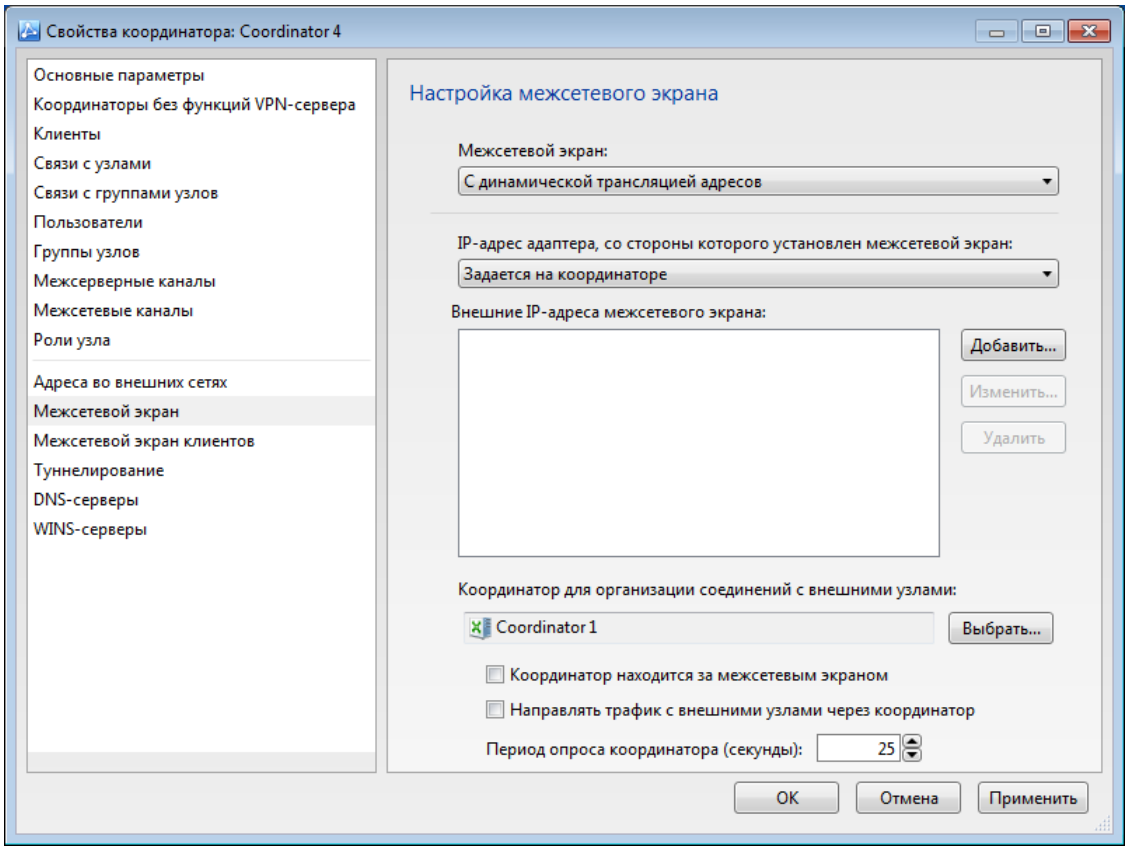

Рисунок 105. Настройка подключения через межсетевой экран с динамической трансляцией адресов

2 Из списка **IP-адрес адаптера, со стороны которого установлен межсетевой экран** выберите сетевой адаптер настраиваемого узла, который находится в одной подсети с межсетевым экраном, или оставьте значение по умолчанию **Задается на координаторе**.

3 Если межсетевой экран имеет постоянные внешние IP-адреса, добавьте эти адреса в список **Внешние IP-адреса межсетевого экрана** с помощью кнопки **Добавить**.

Чтобы изменить или удалить заданный IP-адрес, выберите его в списке и нажмите соответствующую кнопку.

4 В поле **Координатор для организации соединений с внешними узлами** с помощью кнопки **Выбрать** укажите координатор, который доступен из внешней сети напрямую или через межсетевой экран со статической трансляцией адресов.

Примечание. Для правильной работы данного типа подключения требуется, чтобы настраиваемый узел и координатор для организации внешних соединений находились в одной локальной (маршрутизируемой) сети. По этой причине недопустима ситуация, когда установлен флажок **Координатор находится за межсетевым экраном**.

---

5 Если требуется, чтобы соединения с внешними узлами всегда осуществлялись через координатор для организации внешних соединений, установите флажок **Направлять трафик с внешними узлами через координатор**. Данная настройка позволяет повысить надежность соединения, при этом может снизиться скорость обмена данными.

6 В поле **Период опроса координатора (секунды)** укажите период опроса координатора входящих соединений. Опрос координатора выполняется для поддержания на межсетевом экране динамического правила, обеспечивающего прохождение входящего трафика. По умолчанию установлено значение 25 секунд. Период опроса не должен превышать время жизни динамического правила на межсетевом экране.

7 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Подробная информация о данном типе подключения содержится в разделе Подключение через межсетевой экран с динамической трансляцией адресов (на стр. 42).

Настройка подключения через межсетевой экран со статической трансляцией адресов

Для настройки подключения через межсетевой экран со статической трансляцией адресов выполните следующие действия:

1 В разделе **Настройка межсетевого экрана** в списке **Межсетевой экран** выберите пункт **Со статической трансляцией адресов**.

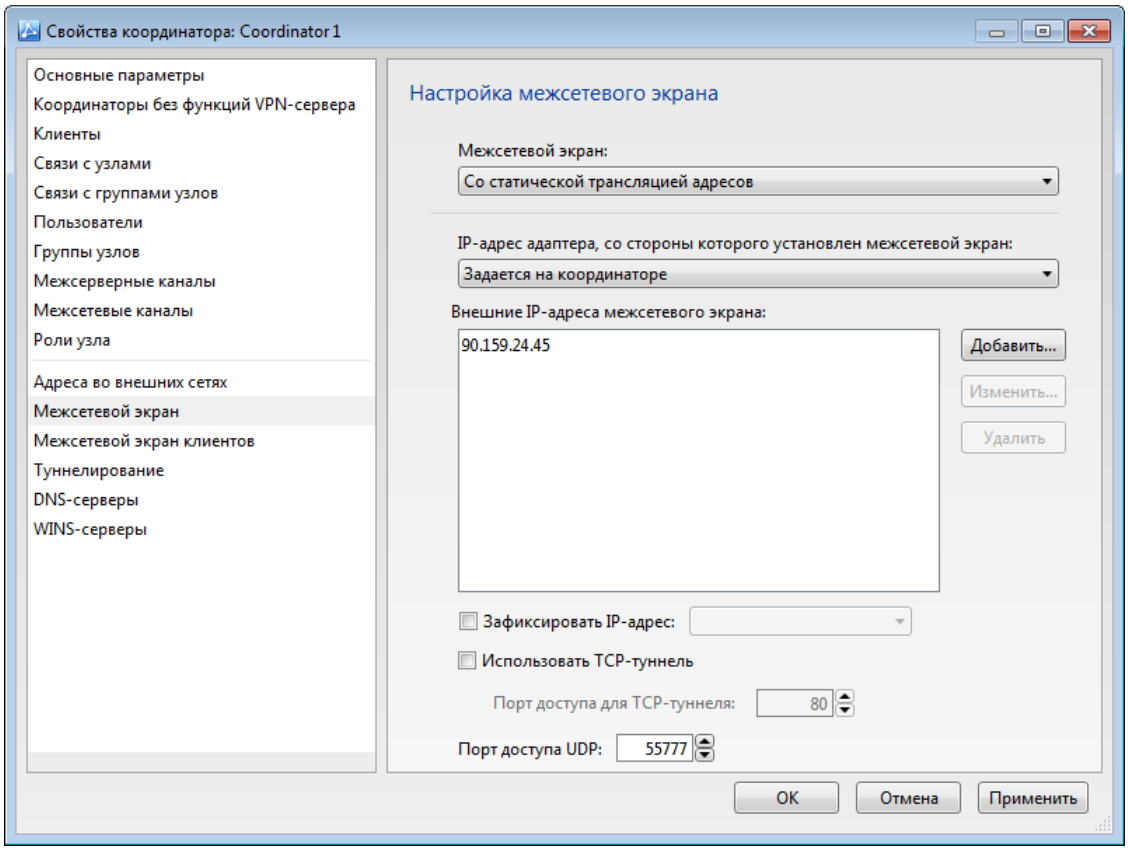

Рисунок 106. Настройка подключения через межсетевой экран со статической трансляцией адресов

2 В список **Внешние IP-адреса межсетевого экрана** добавьте внешние IP-адреса межсетевого экрана с помощью кнопки **Добавить**.

Чтобы изменить или удалить заданный IP-адрес, выберите его в списке и нажмите соответствующую кнопку.

3 При необходимости установите флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран** и выберите из списка требуемый IP-адрес межсетевого экрана.

Рекомендуется использовать эту настройку, только если межсетевой экран имеет хотя бы один внешний адрес и требуется направлять входящие пакеты через определенный адрес независимо от того, с какого адреса были отправлены исходящие пакеты.

4 При необходимости измените значение в поле **Порт доступа UDP**. По умолчанию задан порт номер 55777. Изменять номер порта нужно в том случае, если несколько сетевых узлов ViPNet подключены через один межсетевой экран. Каждый сетевой узел должен иметь собственный номер порта.

5 В случае недоступности передачи IP-пакетов по протоколу UDP вы можете настроить TCP-туннель на координаторе. Для этого установите флажок **Использовать TCP-туннель** и задайте порт, на который должны поступать переданные TCP-пакеты, в соответствующем поле. По умолчанию значение TCP-порта 80.

Примечание. TCP-туннель можно настроить только на координаторе, для которого задан тип подключения через межсетевой экран **Не используется** или **Со статической трансляцией адресов**.

6 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Подробная информация о данном типе подключения содержится в разделе Подключение через межсетевой экран со статической трансляцией адресов (на стр. 44).

Настройка подключения через координатор в качестве межсетевого экрана

Для настройки подключения с использованием координатора в качестве межсетевого экрана выполните следующие действия:

1 В разделе **Настройка межсетевого экрана** (см. рисунок на стр. 179) из списка **Межсетевой экран** выберите пункт **Координатор в качестве межсетевого экрана**.

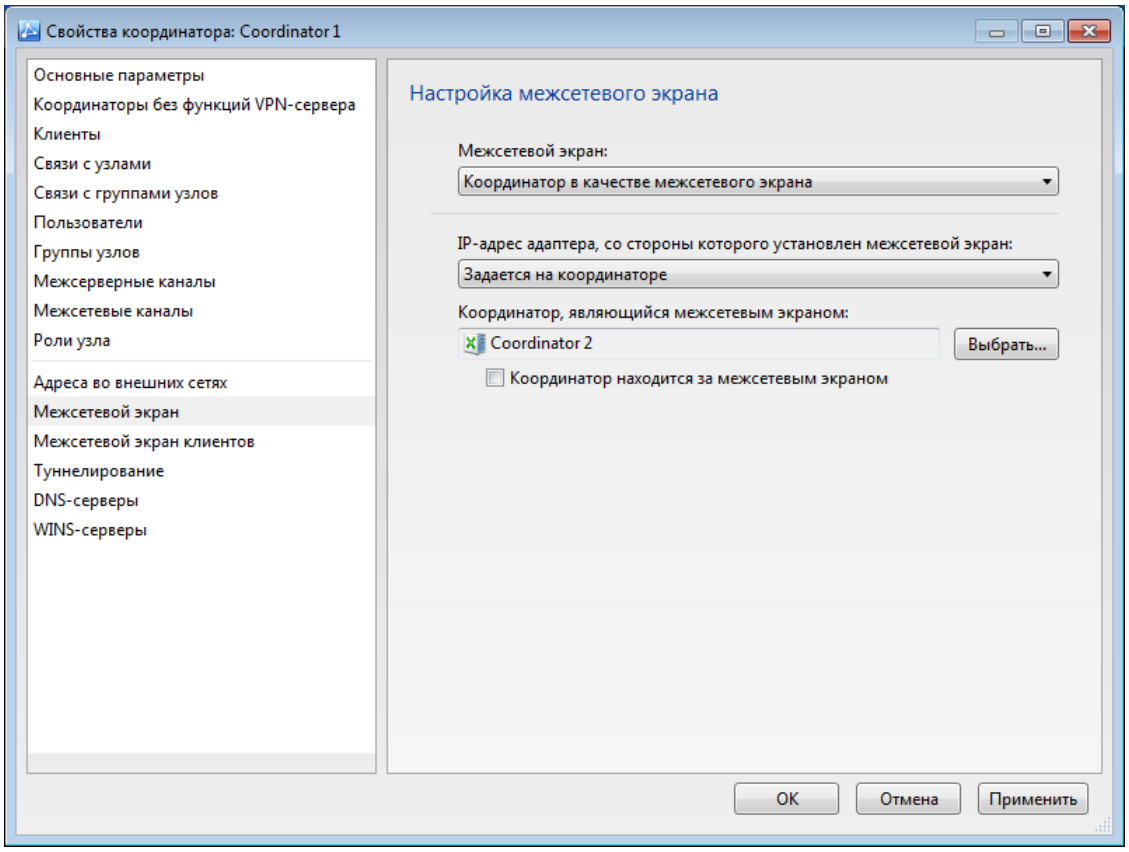

Рисунок 107. Настройка подключения через координатор в качестве межсетевого экрана

2 Из списка **IP-адрес адаптера, со стороны которого установлен межсетевой экран** выберите сетевой адаптер настраиваемого узла, который находится в одной подсети с межсетевым экраном, или оставьте значение по умолчанию **Задается на координаторе**.

3 В поле **Координатор, являющийся межсетевым экраном** укажите координатор, который требуется использовать в качестве межсетевого экрана. Для этого нажмите кнопку **Выбрать** и в открывшемся окне выберите из списка координаторов, с которыми есть связь, нужный координатор.

Примечание. Для правильной работы данного типа подключения требуется, чтобы настраиваемый узел и координатор, используемый в качестве межсетевого экрана, находились в одной локальной (маршрутизируемой) сети. По этой причине недопустима ситуация, когда установлен флажок **Координатор находится за межсетевым экраном**.

4 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Подробная информация о данном типе подключения содержится в разделе Подключение через координатор (на стр. 40).

Настройка параметров межсетевого экрана клиентов на сервере IP-адресов

На координаторе можно настроить параметры межсетевого экрана клиентов, для которых этот координатор назначен сервером IP-адресов. Эти параметры будут использоваться клиентами по умолчанию (см. «Параметры межсетевого экрана клиента» на стр. 180).

Чтобы задать на координаторе параметры межсетевого экрана клиентов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы**.

3 На панели просмотра дважды щелкните координатор, который требуется настроить.

4 В окне свойств координатора на левой панели выберите раздел **Межсетевой экран клиентов**.

По умолчанию в этом разделе для клиентов задано использование в качестве межсетевого экрана настраиваемого координатора.

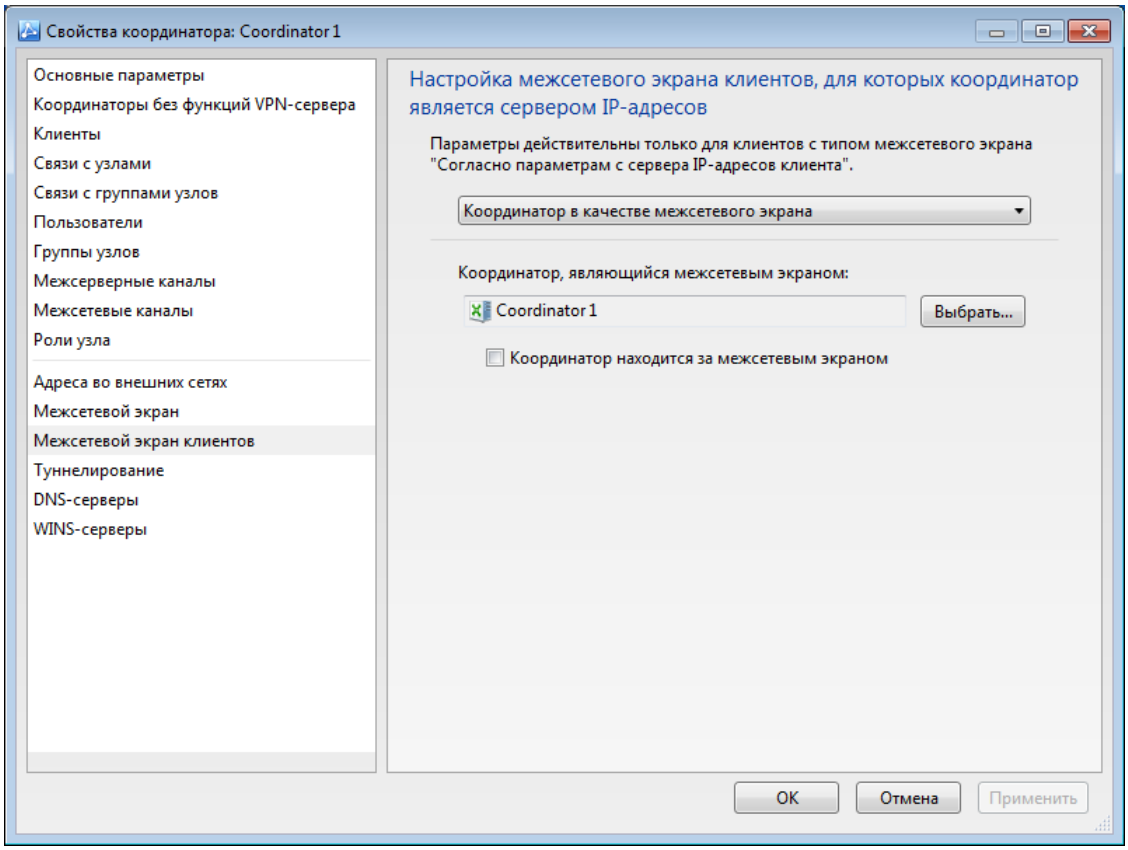

Рисунок 108. Настройка параметров межсетевого экрана клиентов

5 Если предполагается, что клиенты будут иметь прямое подключение к внешней сети, выберите из списка **Не используется**.

6 Если требуется, чтобы клиенты использовали в качестве межсетевого экрана координатор:

- В выпадающем списке выберите пункт **Координатор в качестве межсетевого экрана**.
- Чтобы изменить координатор, который будет использоваться в качестве межсетевого экрана, нажмите кнопку **Выбрать** и в открывшемся окне выберите из списка нужный координатор.

Примечание. Для правильной работы данного типа подключения требуется, чтобы клиенты и координатор, используемый в качестве межсетевого экрана, находились в одной локальной (маршрутизируемой) сети. По этой причине недопустима ситуация, когда установлен флажок **Координатор находится за межсетевым экраном**.

---

7 Если требуется, чтобы клиенты использовали межсетевой экран с динамической трансляцией адресов:

- В выпадающем списке выберите пункт **С динамической трансляцией адресов**.
- В случае необходимости установите флажок **Направлять трафик с внешними узлами через координатор** или измените период опроса координатора (см. «Настройка подключения через межсетевой экран с динамической трансляцией адресов» на стр. 182).

Другие параметры подключения потребуется задать в программе ViPNet Монитор непосредственно на клиенте.

8 Если требуется, чтобы клиенты использовали межсетевой экран со статической трансляцией адресов, в выпадающем списке выберите пункт **Со статической трансляцией адресов**.

Другие параметры подключения потребуется задать в программе ViPNet Монитор непосредственно на клиенте.

9 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Изменение списка групп, в которые входит сетевой узел

Узлы сети ViPNet могут входить в одну или несколько групп узлов (см. «Работа с группами узлов» на стр. 196). Чтобы добавить сетевой узел в группу узлов или удалить его из группы узлов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Клиенты** или **Координаторы**, в зависимости от типа нужного сетевого узла, который требуется настроить.

3 На панели просмотра дважды щелкните сетевой узел, список групп которого нужно просмотреть или изменить.

4 В окне свойств сетевого узла на левой панели выберите пункт **Группы узлов**.

В разделе **Группы узлов, в которые входит клиент (координатор)** будет отображен список групп.

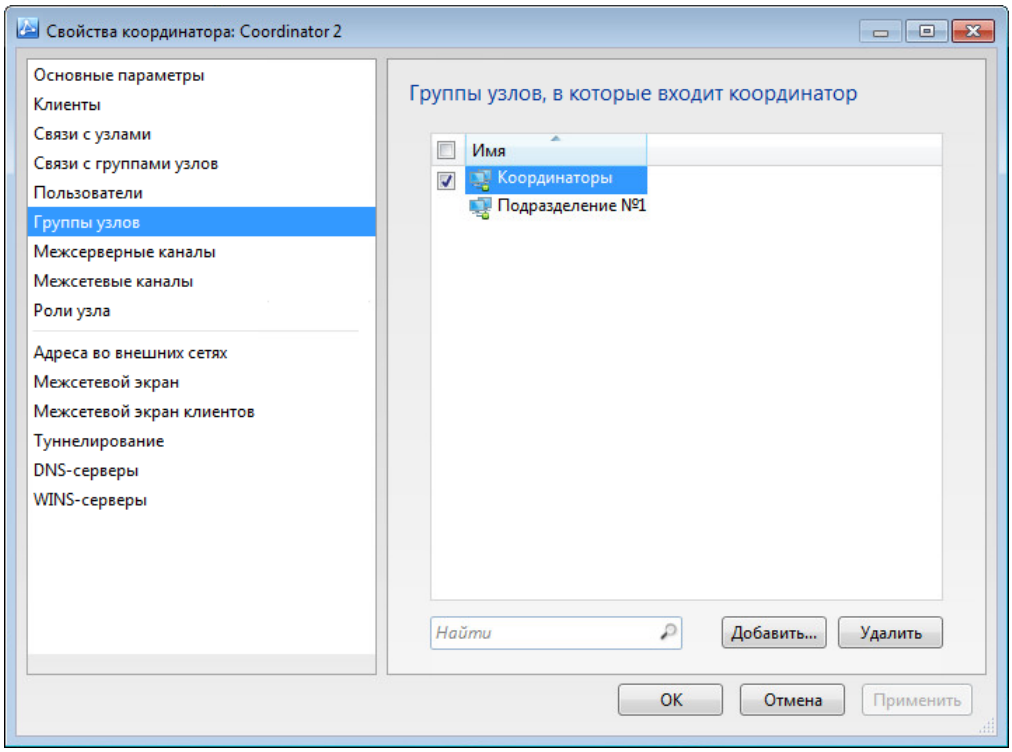

Рисунок 109. Группы узлов, в которые входит координатор

5 Для добавления текущего сетевого узла в одну или несколько групп узлов нажмите кнопку **Добавить** и в открывшемся окне из списка групп узлов, в которые не входит текущий сетевой узел, выберите одну или несколько групп.

Сетевой узел будет добавлен в выбранные группы, эти группы будут отображены в списке групп узла.

6 Чтобы удалить текущий сетевой узел из групп узлов:

- Выберите в списке одну или несколько групп, из которых требуется удалить текущий сетевой узел, и нажмите кнопку **Удалить**.
- Если требуется удалить связи узла со всеми узлами, входящими в выбранную группу, в окне подтверждения установите соответствующий флажок. Если флажок не будет установлен, то узел будет удален из группы, но его связи с узлами группы будут сохранены.
- Нажмите кнопку **Удалить из групп**. Сетевой узел будет удален из выбранных групп, эти группы будут исключены из списка групп узла.

7 Чтобы сохранить изменения, нажмите кнопку **Применить**.

Добавить сетевой узел в группу узлов или удалить узел из группы можно также в разделе **Группы узлов** (см. «Работа с группами узлов» на стр. 196).

Работа с шаблонами сетевых узлов

Для удобства создания большого количества новых сетевых узлов вы можете использовать шаблоны. В шаблонах указываются свойства, применяемые для всех узлов, которым будет назначен шаблон. Например, если в вашей организации открылось несколько новых филиалов, и для новых сотрудников необходимо создать сетевые узлы, то удобно создать шаблоны, в которых будут указаны все необходимые свойства, а затем при создании узлов указывать определенные шаблоны вместо выполнения целого ряда настроек вручную. Параметры для нового сетевого узла будут автоматически добавлены из шаблона.

Шаблоны применяются к создаваемым узлам в соответствии с заданным приоритетом (см. «Добавление координатора» на стр. 112). Если в нескольких шаблонах указаны аналогичные параметры, то узлу будут назначены настройки из более приоритетного шаблона.

Также вы можете применить шаблоны к уже созданным узлам. Например, если необходимо изменить настройки целого ряда сетевых узлов, то удобно выполнить данные настройки централизованно, создав нужный шаблон и применив его к узлам.

После создания или редактирования узла с помощью шаблона настройки узла можно изменять в окне его свойств. Удаление шаблонов не влияет на настройки узлов, к которым эти шаблоны были применены.

В программе ViPNet Центр управления сетью вы можете создавать следующие виды шаблонов:

- Шаблоны любых типов сетевых узлов. В данных шаблонах можно задать: маску имени и роли сетевых узлов.
- Шаблоны клиентов. В данных шаблонах можно задать: маску имени, роли, координатор и сервер IP-адресов клиентов.
- Шаблоны координаторов. В данных шаблонах можно задать: маску имени, роли, туннелируемые адреса и настройки межсетевого экрана координаторов.
- Шаблоны координаторов без функций VPN-сервера. В данных шаблонах можно задать: маску имени, роли, координатор узла, туннелируемые адреса и настройки межсетевого экрана координаторов.

При создании каждого сетевого узла определенного типа вы можете указать один или несколько шаблонов с необходимыми свойствами. Имя узла и координатор сетевого узла будут автоматически выбраны для нового сетевого узла на основании свойств, указанных в шаблонах.

Создание шаблона сетевых узлов

Чтобы создать шаблон сетевых узлов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Шаблоны сетевых узлов**.

3 В разделе **Шаблоны сетевых узлов** на панели инструментов нажмите кнопку .

4 В окне **Новый шаблон** укажите имя шаблона и тип сетевых узлов: **Любые сетевые узлы**, **Только клиенты, Только координаторы** или **Только координаторы без функций VPN-сервера.**

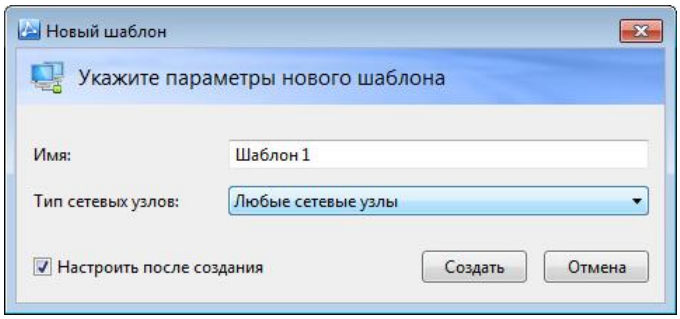

Рисунок 110. Создание шаблона сетевых узлов

5 Чтобы настроить свойства шаблона сразу после создания, установите флажок **Настроить после создания** (по умолчанию снят).

6 Нажмите кнопку **Создать**. В списке **Шаблоны сетевых узлов** появится новый шаблон.

7 Настройте параметры созданного шаблона (см. «Настройка шаблона сетевых узлов» на стр. 192).

В результате будет создан шаблон, который вы сможете использовать для задания свойств сетевых узлов.

Настройка шаблона сетевых узлов

Для настройки параметров шаблона сетевых узлов выполните следующие действия:

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

2 На панели навигации выберите раздел **Шаблоны сетевых узлов**.

3 На панели навигации дважды щелкните шаблон, параметры которого необходимо изменить.

4 В окне свойств шаблона при необходимости измените имя шаблона или введите его описание.

5 На левой панели окна нажмите кнопку **Добавить атрибуты** и выберите нужный атрибут. Набор доступных атрибутов зависит от типа шаблона (от типа узлов, к которым будет применяться шаблон).

6 Для настройки добавленного атрибута на левой панели окна выберите соответствующий раздел и выполните следующие действия:

- Для атрибута **Именование узлов** введите маску имени узлов либо оставьте маску по умолчанию.

- Для атрибута **Роли узлов** добавьте нужные роли и настройте их параметры (см. «Изменение списка ролей сетевого узла» на стр. 142).

  Чтобы в случае применения шаблона к уже созданным узлам удалять все ранее заданные роли узла, установите соответствующий флажок (по умолчанию снят).

- Для атрибутов **Сервер IP-адресов** с помощью кнопки **Выбрать** укажите нужный сервер IP-адресов клиентов.

- Для атрибута **Координатор узла** с помощью кнопки **Выбрать** укажите координатор, на котором будет зарегистрирован сетевой узел.

- Для атрибута **Межсетевой экран** укажите настройки подключения координаторов к внешней сети: тип межсетевого экрана (см. «Настройка параметров подключения к внешней сети» на стр. 178), координатор для организации соединений с внешними узлами и другие дополнительные параметры.

- Для атрибута **Туннелирование** укажите IP-адреса туннелируемых соединений (см. «Настройка туннелирования» на стр. 123). Если шаблон будет применяться к уже созданным узлам, при необходимости установите или снимите флажок **Удалять все адреса туннелируемых соединений узла перед добавлением адресов из шаблона** (по умолчанию снят).

- Для атрибутов **DNS-серверы** и **WINS-серверы** задайте список защищенных DNS- и WINS-серверов для использования на узлах, к которым будет применен шаблон (см. «Настройка списков DNS- и WINS-серверов сетевого узла» на стр. 172).

  Чтобы в случае применения шаблона к уже созданным узлам удалять ранее заданные списки WINS-серверов, установите соответствующий флажок (по умолчанию снят).

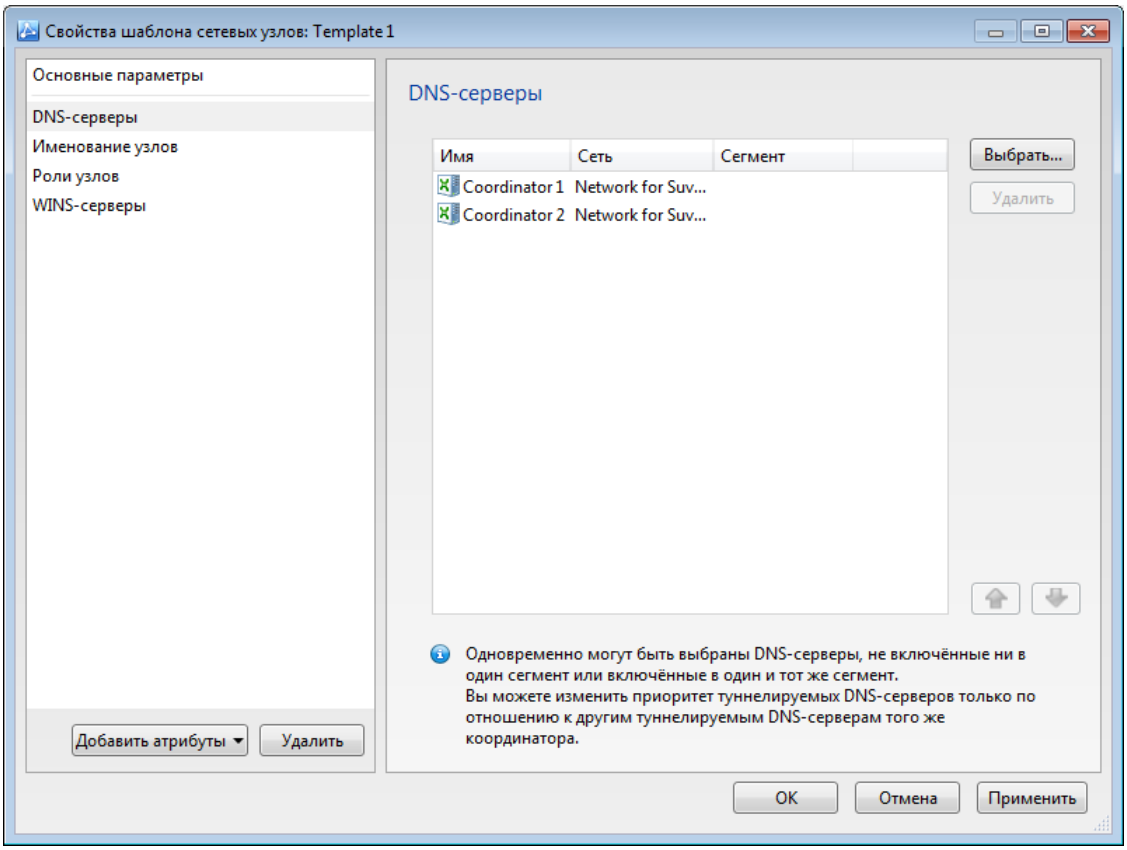

Рисунок 111. Настройка шаблона сетевых узлов

Примечание. Для каждого добавленного атрибута должны быть указаны его параметры, иначе шаблон будет считаться недействительным. Если какой-либо атрибут не используется в шаблоне, удалите его с помощью кнопки **Удалить** на левой панели.

7 Нажмите кнопку **Применить**.

В результате параметры шаблона будут настроены.

Применение шаблонов для редактирования свойств сетевых узлов

Чтобы применить шаблон к уже созданному сетевому узлу, выполните следующие действия:

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

2 На панели навигации выберите раздел **Координаторы** или **Клиенты** (в зависимости от типа редактируемого узла).

3 На панели просмотра выберите один или несколько узлов и щелкните их правой кнопкой мыши, после чего в контекстном меню выберите **Применить шаблон**.

4 В окне **Применение шаблона** выберите шаблон с нужными настройками и нажмите кнопку **Применить шаблон**.

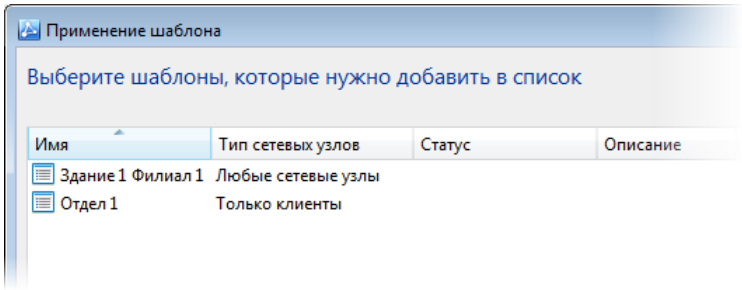

Рисунок 112. Выбор шаблона сетевых узлов

5 В появившемся окне подтвердите применение шаблона. Для этого нажмите кнопку **Продолжить**.

В результате настройки узлов будут изменены в соответствии с выбранным шаблоном. Если к узлам необходимо применить несколько шаблонов, повторите описанные действия для всех шаблонов. Если в шаблонах заданы аналогичные параметры узлов, то эти параметры будут изменяться при последовательном применении данных шаблонов.

После применения шаблона настройки узла можно изменять в окне его свойств. Изменение свойств узлов не влияет на параметры шаблонов, которые ранее были применены к узлам.

Удаление шаблона сетевых узлов

Чтобы удалить шаблон сетевых узлов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Шаблоны сетевых узлов**.

3 На панели просмотра выберите в списке один или несколько шаблонов сетевых узлов и выполните одно из следующих действий:

- Нажмите кнопку на панели инструментов.
- В контекстном меню выберите пункт **Удалить**.

4 В появившемся окне подтвердите удаление шаблонов. Для этого нажмите кнопку **Удалить шаблоны**.

В результате выбранный шаблон или несколько шаблонов будут удалены. Удаление шаблонов не влияет на свойства узлов, заданные с помощью этих шаблонов.

Работа с группами узлов

Группы узлов предназначены для логического объединения сетевых узлов со следующими целями:

- Назначение узлам общего пароля администратора в программе ViPNet Удостоверяющий и ключевой центр. Данная функция позволяет распределить работу по управлению сетевыми узлами между несколькими администраторами.
- Создание и управление связями между сетевыми узлами. Удобно использовать данную функцию при работе с большим количеством узлов — можно создать группы узлов и задать связь между ними вместо настройки связей для каждого узла вручную.
- Рассылка справочников, ключей и обновлений ПО ViPNet для отдельных групп узлов (например, для группы серверов с ПО ViPNet Coordinator for Linux).

Каждая группа узлов должна иметь уникальное имя в рамках сети ViPNet. По умолчанию узлы внутри каждой группы не связаны между собой. Если вы хотите связать эти узлы, установите связь данной группы с самой собой (см. «Изменение связей с группами узлов» на стр. 199).

По умолчанию существует группа с именем «Вся сеть», которая не отображается в интерфейсе программы ViPNet Центр управления сетью. Эта группа объединяет все узлы сети ViPNet, и ее можно использовать только для создания пароля администратора узлов ViPNet в УКЦ. Новые сетевые узлы автоматически добавляются в эту группу при создании.

Добавление группы узлов

Чтобы добавить новую группу узлов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Группы узлов**.

3 На панели просмотра в разделе **Группы узлов** нажмите кнопку .

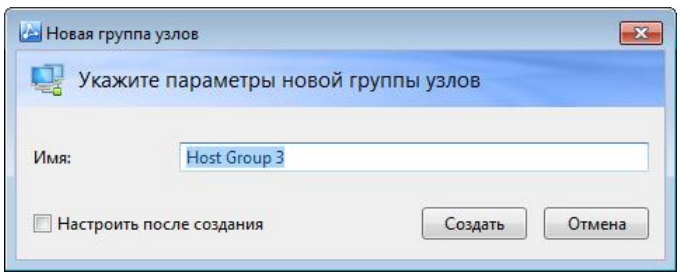

Рисунок 113. Окно создания группы узлов

4 В окне **Новая группа узлов** выполните следующие действия:

4.1 В соответствующее поле введите имя создаваемой группы.

4.2 Чтобы после создания группы открыть окно для ее настройки, установите флажок **Настроить после создания** (по умолчанию снят).

4.3 Нажмите кнопку **Создать**. В списке **Группы узлов** появится новая группа.

5 При необходимости измените параметры созданной группы узлов (см. «Работа с группами узлов» на стр. 196).

Удаление группы узлов

Чтобы удалить группу узлов, выполните следующие действия:

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

2 На панели навигации выберите раздел **Группы узлов**.

3 На панели просмотра в разделе **Группы узлов** выберите одну или несколько групп для удаления.

4 Нажмите кнопку  на панели инструментов или в контекстном меню группы выберите пункт **Удалить**.

5 Если требуется удалить связи узлов, входящих в удаляемую группу, со связанными с группой узлами, в окне подтверждения установите соответствующий флажок. Если флажок не будет установлен, то связи узлов группы с этими узлами будут сохранены.

6 Нажмите кнопку **Удалить группы**.

Выбранные группы будут удалены. При этом сетевые узлы, входившие в группу, не будут удалены или изменены.

Изменение списка сетевых узлов в группе

Чтобы изменить список сетевых узлов, входящих в группу, выполните следующие действия:

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

2 На панели навигации выберите раздел **Группы узлов**.

3 На панели просмотра дважды щелкните группу, список узлов которой требуется изменить.

4 В окне свойств группы на левой панели выберите раздел **Сетевые узлы**.

В панели просмотра будет отображен список узлов, входящих в данную группу.

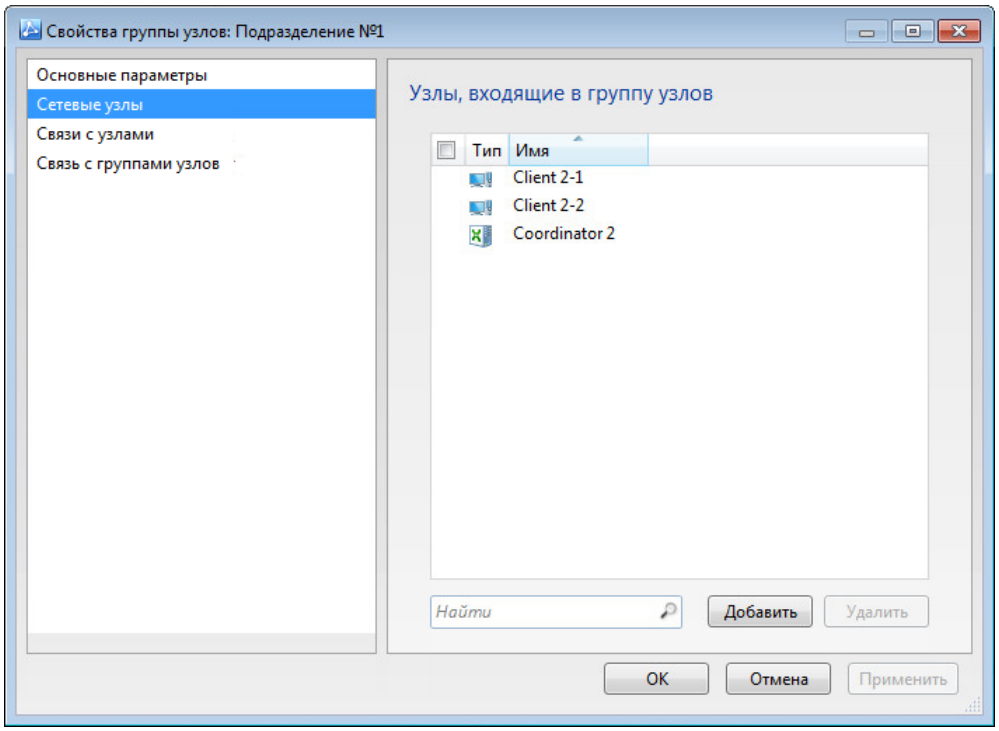

Рисунок 114. Список узлов, входящих в группу

5 Для добавления узлов в группу нажмите кнопку **Добавить** и в открывшемся окне выберите из списка нужные сетевые узлы.

6 Для удаления узлов из группы выберите в списке один или несколько сетевых узлов и нажмите кнопку **Удалить**:

- Если требуется удалить связи выбранного узла со всеми узлами, входящими в текущую группу и в связанные с ней группы, в окне подтверждения установите соответствующий флажок. Если флажок не будет установлен, то связи узла с узлами текущей группы и других связанных групп будут сохранены.
- Нажмите кнопку **Удалить из группы**.

7 Выполнив необходимые изменения, нажмите кнопку **OK**.

Изменение связей с сетевыми узлами

Для просмотра и изменения списка узлов, с которыми связана группа, выполните следующие действия:

1 В окне **ViPNet Центр управления сетью** на панели навигации нажмите кнопку **Моя сеть**.

2 На панели навигации в списке **Моя сеть** выберите пункт **Группы узлов**.

3 На панели просмотра дважды щелкните группу, связи которой требуется изменить.

4 В окне свойств группы узлов на левой панели выберите пункт **Связи с узлами**.

В панели просмотра будет отображен список узлов, с которыми связана данная группа.

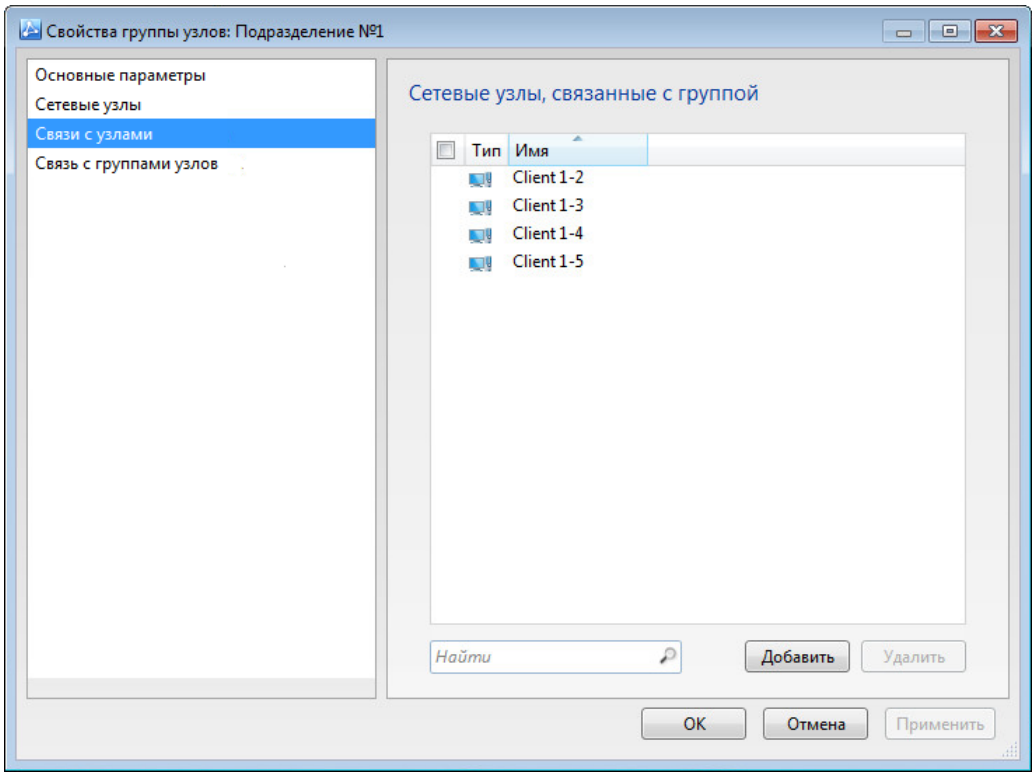

Рисунок 115. Связи группы с сетевыми узлами

5 Для добавления связей нажмите кнопку **Добавить** и в окне со списком доступных узлов выберите один или несколько узлов.

Выбранные группы будут добавлены в список связей текущей группы узлов. При этом будут созданы связи добавленного узла со всеми узлами, входящими в группу.

6 Чтобы удалить связи, выберите в списке связей один или несколько узлов и нажмите кнопку **Удалить**:

- Если требуется удалить связи выбранного узла со всеми узлами, входящими в группу, в окне подтверждения установите соответствующий флажок. Если флажок не будет установлен, то связь узла с группой узлов будет удалена, но связи с узлами группы будут сохранены.
- Нажмите кнопку **Да**. Выбранные связи будут удалены.

7 Чтобы сохранить изменения, нажмите кнопку **OK**.

Изменение связей с группами узлов

Для просмотра и изменения списка групп узлов, с которыми связана группа, выполните следующие действия:

1 В окне **ViPNet Центр управления сетью** на панели навигации нажмите кнопку **Моя сеть**.

2 На панели навигации в списке **Моя сеть** выберите пункт **Группы узлов**.

3 На панели просмотра дважды щелкните группу, связи которой требуется изменить.

4 В окне свойств группы узлов на левой панели выберите пункт **Связь с группами узлов**.

На панели просмотра будет отображен список групп узлов, с которыми связана данная группа.

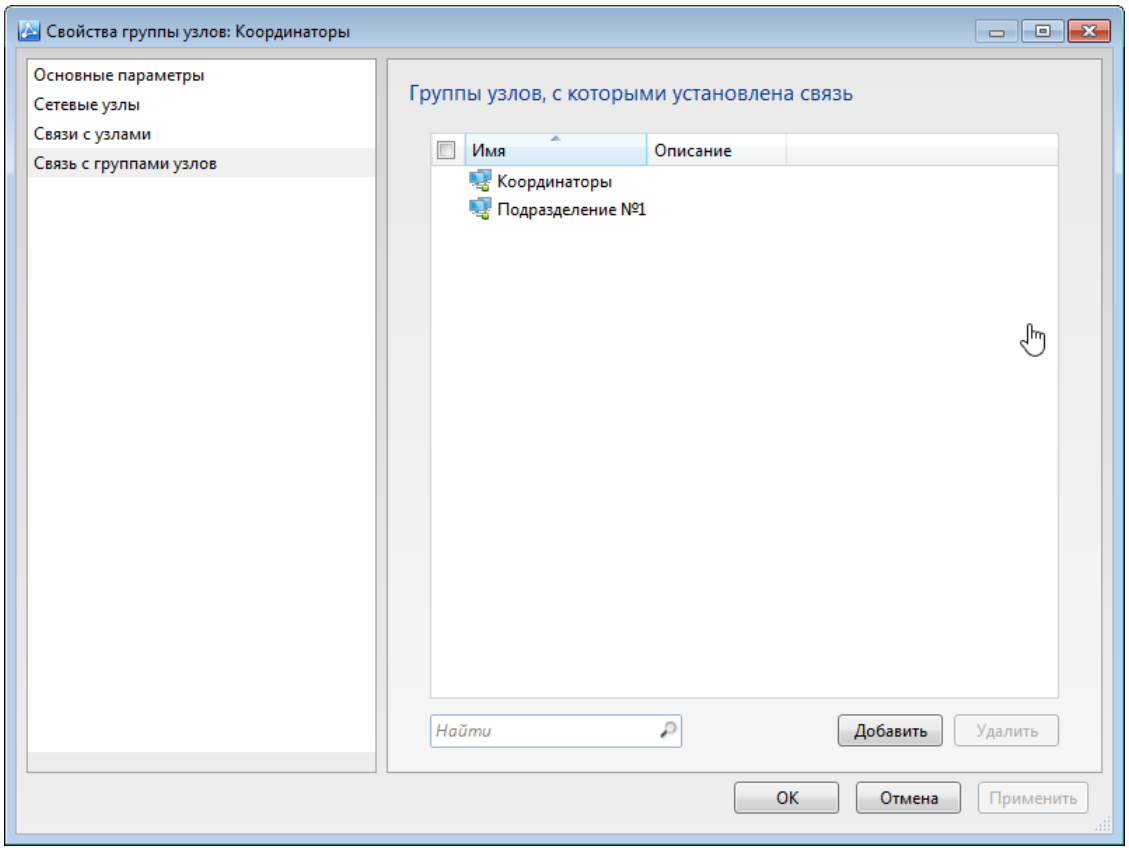

Рисунок 116. Связанные группы сетевых узлов

5 Для добавления связей нажмите кнопку **Добавить** и в окне со списком доступных групп выберите одну или несколько групп узлов.

Выбранные группы будут добавлены в список связей текущей группы. При этом будут автоматически созданы связи между узлами текущей группы и узлами, входящими в добавленные группы.

Примечание. Если требуется связать сетевые узлы, входящие в одну группу, установите связь группы с самой собой.

---

6 Чтобы удалить связи, выберите в списке связей одну или несколько групп узлов и нажмите кнопку **Удалить**:

- Если требуется удалить связи текущей группы со всеми узлами, входящими в удаляемую группу, в окне подтверждения установите соответствующий флажок. Если флажок не будет установлен, то связь группы узлов с группой будет удалена, но связи с узлами удаленной группы будут сохранены.
- Нажмите кнопку **Да**. Выбранные связи будут удалены.

7 Чтобы сохранить изменения, нажмите кнопку **OK**.

5

Настройка параметров пользователей

Создание пользователя и настройка его параметров 203

Работа с группами пользователей 215

Создание пользователя и настройка его параметров

На каждый сетевой узел должен быть добавлен по крайней мере один пользователь, иначе невозможно будет создать справочники для сетевого узла. На одном сетевом узле может работать несколько пользователей. В то же время, каждый пользователь может быть добавлен на один или несколько сетевых узлов.

Настройка параметров пользователя в программе ViPNet Центр управления сетью включает такие действия, как добавление пользователя на сетевые узлы, на которых он будет работать, создание связей с другими пользователями и группами пользователей. Связи между пользователями позволяют им вести конфиденциальную переписку в программе ViPNet Деловая почта. Связь между пользователями сетевых узлов, связанных обязательными связями (см. «Изменение связей между сетевыми узлами» на стр. 138), может потребоваться для отображения обязательных связей в программе ViPNet Монитор.

Если пользователь сетевого узла работает в сторонней информационной системе, использующей программное обеспечение ViPNet, имя пользователя в этой системе нужно задать в качестве псевдонима.

Для настройки параметров пользователя рекомендуется выполнить следующие шаги:

Таблица 8. Последовательность настройки параметров пользователя

	Действие	Ссылка
☐	Добавление пользователя на сетевые узлы	См. раздел Изменение списка сетевых узлов пользователя (на стр. 206).
☐	Задание псевдонимов пользователя	См. раздел Изменение псевдонимов пользователя (на стр. 210).
☐	Добавление пользователя в группы	См. раздел Изменение списка групп, в которые входит пользователь (на стр. 211).
☐	Создание связей с другими пользователями	См. раздел Изменение связей между пользователями (на стр. 207).
☐	Создание связей с группами пользователей	См. раздел Изменение связей пользователя с группами пользователей (на стр. 212).

Для каждого сетевого узла, на который был добавлен новый пользователь, в программе ViPNet Удостоверяющий и ключевой центр нужно создать дистрибутив ключей. Если на сетевой узел добавлено несколько пользователей, для каждого из них будет создан свой дистрибутив. После установки ключей на сетевых узлах пользователи смогут войти в программное обеспечение ViPNet на этих узлах с помощью своего пароля или внешнего устройства аутентификации.

Добавление пользователя

Чтобы добавить нового пользователя сети ViPNet, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 В разделе **Пользователи** на панели инструментов нажмите кнопку .

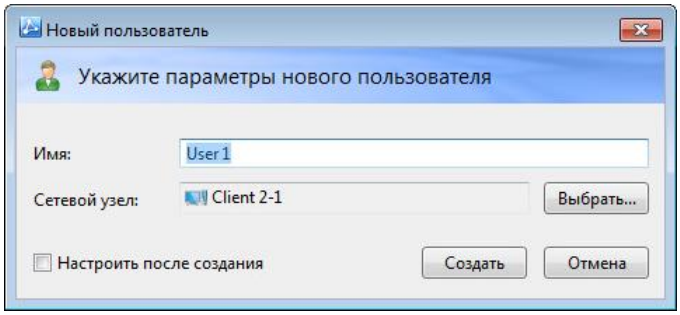

Рисунок 117. Окно создания пользователя

4 В окне **Новый пользователь** выполните следующие действия:

4.1 В соответствующее поле введите имя создаваемого пользователя.

4.2 Если требуется, в поле **Сетевой узел** с помощью кнопки **Выбрать** укажите узел, на котором требуется зарегистрировать нового пользователя.

Добавить созданного пользователя на сетевой узел можно позже в окне свойств пользователя (см. «Изменение списка сетевых узлов пользователя» на стр. 206) или в окне свойств узла (см. «Изменение списка пользователей сетевого узла» на стр. 136).

4.3 Чтобы после создания пользователя открыть окно для его настройки, установите флажок **Настроить после создания** (по умолчанию снят).

4.4 Нажмите кнопку **Создать**.

В списке **Пользователи** появится новый пользователь.

5 Настройте параметры созданного пользователя (см. «Создание пользователя и настройка его параметров» на стр. 203).

После добавления пользователя и настройки его параметров создайте справочники, в программе ViPNet Удостоверяющий и ключевой центр создайте дистрибутивы ключей для сетевых узлов, на которые добавлен пользователь. Затем с помощью дистрибутивов установите ключи на этих узлах.

Удаление пользователя

Чтобы удалить пользователя сети ViPNet, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра в разделе **Пользователи** выберите в списке одного или нескольких пользователей и выполните одно из следующих действий:

- Нажмите кнопку  на панели инструментов.
- В контекстном меню пользователей выберите пункт **Удалить**.

4 Если какие-либо из выбранных пользователей являются единственными пользователями на своих сетевых узлах и эти узлы требуется удалить вместе с пользователями, в окне **Удаление пользователей** установите флажок **Удалить сетевые узлы, на которые добавлены только эти пользователи**.

Этот флажок установлен по умолчанию, если были заданы соответствующие параметры для удаляемых пользователей (см. «Параметры работы с объектами сети» на стр. 75).

5 Нажмите кнопку **Удалить пользователей**.

6 После удаления пользователей создайте справочники и ключи и отправьте их на узлы своей сети (см. «Отправка справочников и ключей» на стр. 91). Если требуется, отправьте межсетевую информацию в доверенные сети (см. «Отправка межсетевой информации» на стр. 251).

Основные параметры пользователя

Для просмотра и изменения таких параметров пользователя, как имя или описание, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра дважды щелкните пользователя, параметры которого нужно просмотреть.

4 В окне свойств пользователя на левой панели выберите пункт **Основные параметры**.

В разделе **Основные параметры пользователя** будут отображены имя, описание и шестнадцатеричный идентификатор пользователя.

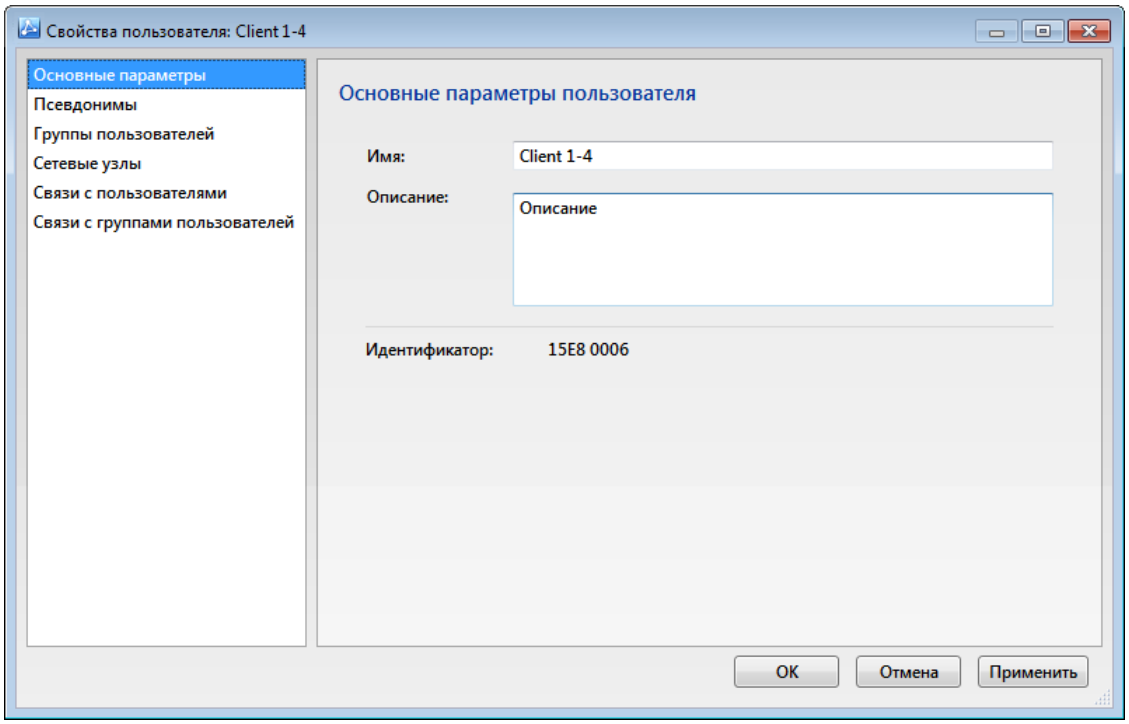

Рисунок 118. Основные параметры пользователя

5 Если требуется, в соответствующих полях измените имя и описание пользователя. Редактировать идентификатор пользователя нельзя.

Если вы измените имя пользователя, который зарегистрирован только на одном узле и является единственным пользователем своего узла, появится сообщение с предложением присвоить этому узлу новое имя пользователя.

6 Чтобы сохранить изменения, нажмите кнопку **Применить**.

Изменение списка сетевых узлов пользователя

Чтобы просмотреть или изменить список узлов пользователя, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра дважды щелкните пользователя, список узлов которого нужно изменить.

4 В окне свойств пользователя на левой панели выберите пункт **Сетевые узлы**.

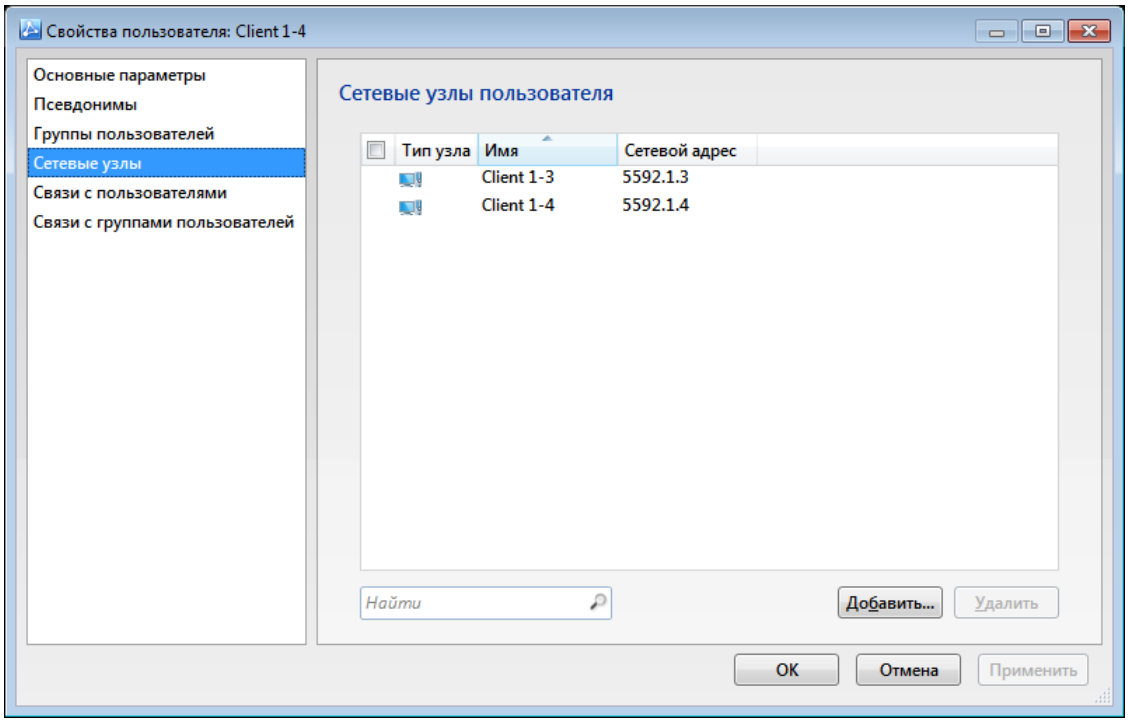

Рисунок 119. Список узлов пользователя

5 Для добавления пользователя на сетевые узлы нажмите кнопку **Добавить** и в открывшемся окне в списке сетевых узлов выберите один или несколько узлов.

Внимание! Если пользователь зарегистрирован на нескольких сетевых узлах, его ключи пользователя (см. глоссарий, стр. 303) могут быть отправлены только на первый узел, на который он был добавлен.

6 Чтобы удалить пользователя с сетевых узлов, выберите в списке узлы, с которых нужно удалить пользователя, и нажмите кнопку **Удалить**.

7 Выполнив необходимые настройки, нажмите кнопку **OK**.

Добавить пользователя на сетевой узел или удалить пользователя с сетевого узла можно также в окне свойств узла (см. «Изменение списка пользователей сетевого узла» на стр. 136).

Изменение связей между пользователями

Чтобы изменить связи пользователя, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра дважды щелкните пользователя, связи которого требуется изменить.

4 В окне свойств пользователя на левой панели выберите раздел **Связи с пользователями**.

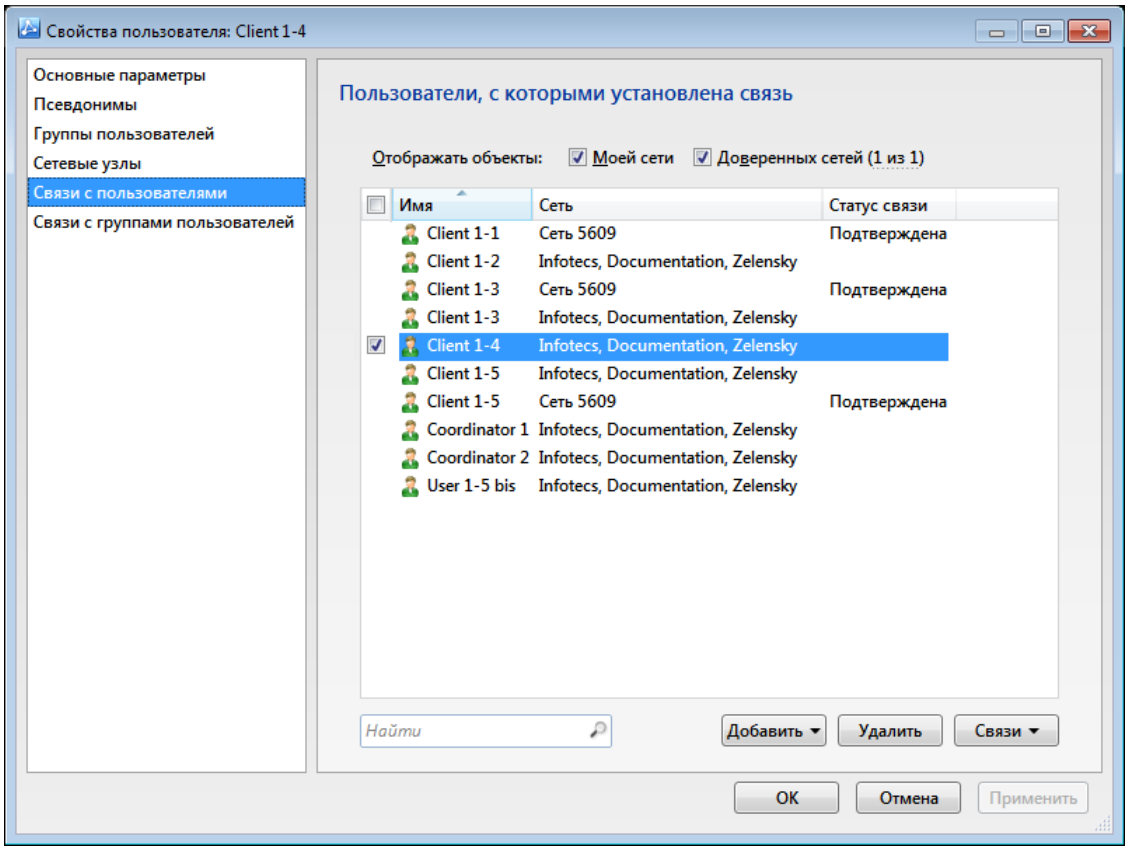

Рисунок 120. Связи пользователя с другими пользователями

5 Чтобы создать связи с определенными пользователями, нажмите кнопку **Добавить** и в меню выберите пункт **Связи с пользователями**. В открывшемся окне выполните следующие действия:

- При необходимости установите флажок **Доверенных сетей** или нажмите ссылку справа от флажка, чтобы выбрать доверенные сети, с пользователями которых требуется создать связи.

  Для создания связей между сетевыми узлами связываемых пользователей установите флажок **Установить связи с узлами, на которые добавлены связываемые пользователи (только для своей сети)**. Это обеспечит возможность установления защищенного соединения между сетевыми узлами. Пользователи данных узлов смогут обмениваться зашифрованными сообщениями в программе ViPNet Деловая почта.

- Выберите одного или несколько пользователей, которых нужно добавить в список связей, и нажмите кнопку **Добавить**.

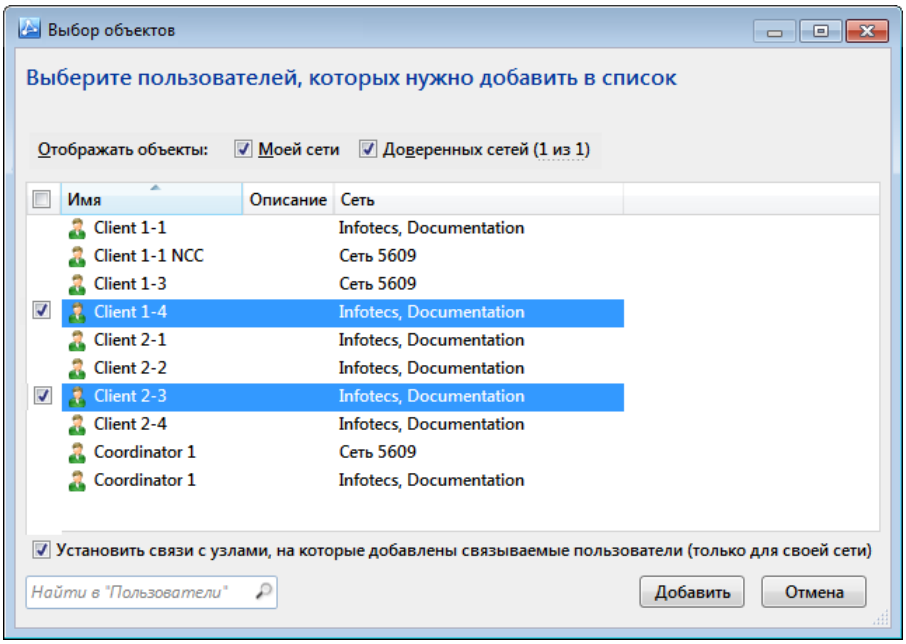

Рисунок 121. Добавление связей с пользователями

6 Чтобы скопировать связи другого пользователя, нажмите кнопку **Добавить** и в меню выберите пункт **Связи по образцу**.

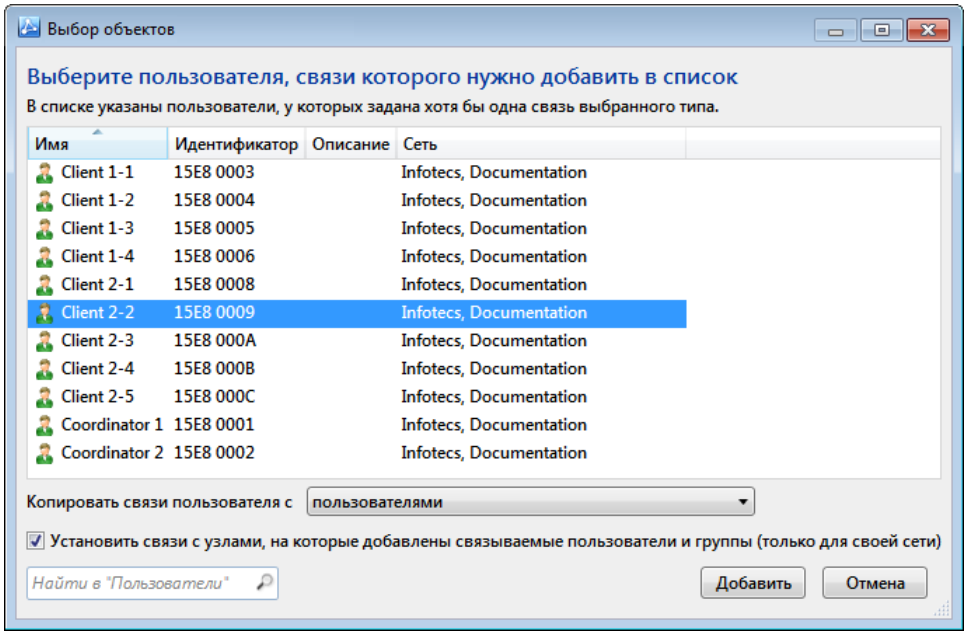

Рисунок 122. Копирование связей другого пользователя

- В открывшемся окне из списка **Копировать связи пользователя с** выберите тип связей для копирования.
- Выберите пользователя, связи которого требуется скопировать.
- Для создания связей между сетевыми узлами связываемых пользователей установите флажок **Установить связи с узлами, на которые добавлены связываемые пользователи и группы (только для своей сети)**.

- Нажмите кнопку **Добавить**. Связи выбранного пользователя будут добавлены к существующему списку связей.

7 Чтобы удалить связи с пользователями, выберите пользователей в списке и нажмите кнопку **Удалить**.

8 Если установлено межсетевое взаимодействие с другими сетями ViPNet, то статус связей с пользователями доверенных сетей можно изменить с помощью кнопки **Связи** (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).

Примечание. Если изменены связи пользователя с пользователями доверенных сетей, соответствующим образом будут изменены связи сетевых узлов, на которые добавлен данный пользователь.

9 Выполнив необходимые изменения, нажмите кнопку **ОК**.

Изменение псевдонимов пользователя

Псевдонимы пользователей применяются при встраивании программного обеспечения ViPNet в сторонние информационные системы. Если пользователь сетевого узла ViPNet работает в сторонней информационной системе, то его имя в этой системе нужно указать в качестве псевдонима. Каждый пользователь ViPNet может иметь несколько псевдонимов, все псевдонимы пользователей должны быть уникальными.

Чтобы изменить список псевдонимов пользователя, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра дважды щелкните пользователя, псевдонимы которого нужно изменить.

4 В окне свойств пользователя на левой панели выберите пункт **Псевдонимы**.

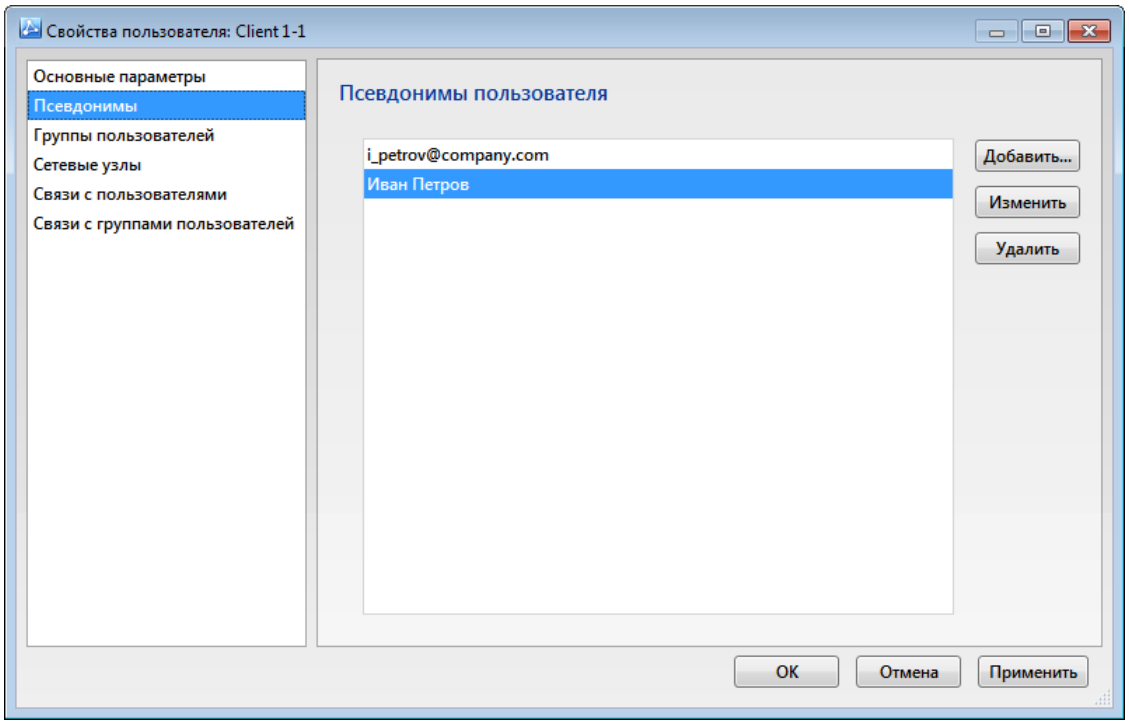

Рисунок 123. Список псевдонимов пользователя

5 Добавьте, измените или удалите псевдоним пользователя с помощью соответствующей кнопки.

6 Чтобы сохранить изменения, нажмите кнопку **Применить**.

Изменение списка групп, в которые входит пользователь

Группы пользователей упрощают управление связями между пользователями (см. «Изменение связей между пользователями» на стр. 207). При добавлении пользователя в группу автоматически создается связь между пользователем и этой группой (см. «Изменение связей пользователя с группами пользователей» на стр. 212).

Подробнее о создании и управлении группами пользователей см. раздел Работа с группами пользователей (на стр. 215).

Чтобы просмотреть или изменить список групп, в которые входит пользователь, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра дважды щелкните пользователя, список групп которого требуется просмотреть или изменить.

4 В окне свойств пользователя на левой панели выберите пункт **Группы пользователей**.

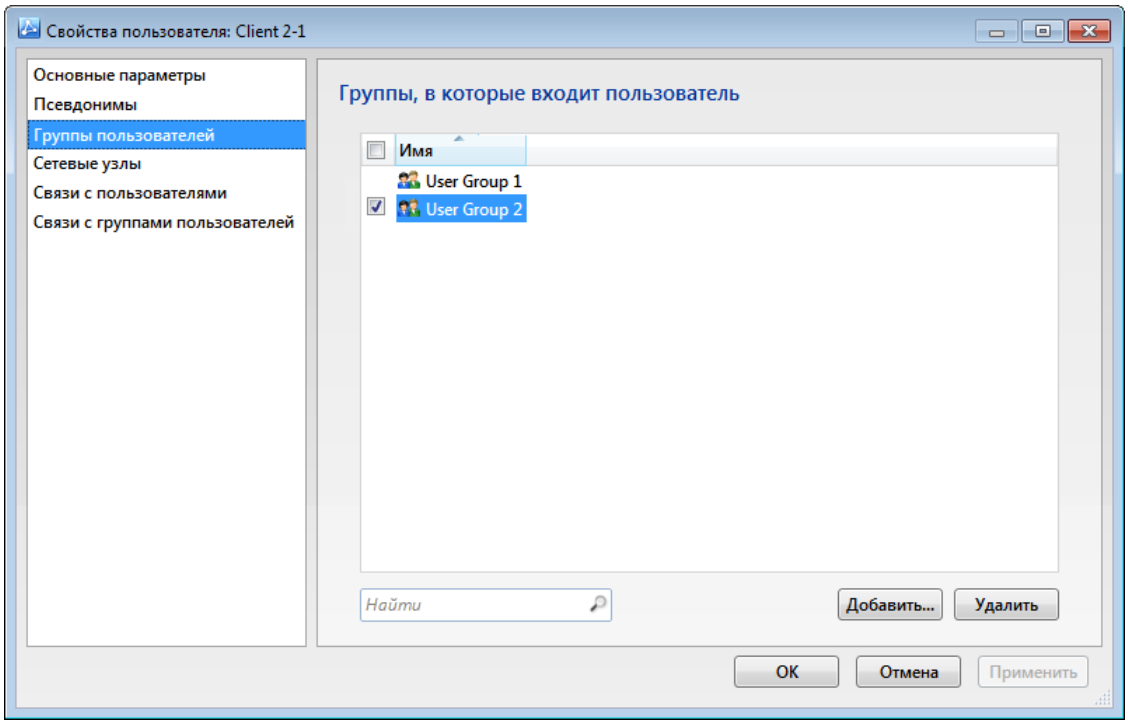

Рисунок 124. Список групп, в которые входит пользователь

5 Для добавления пользователя в группы нажмите кнопку **Добавить** и в открывшемся окне из списка групп, в которые не входит пользователь, выберите одну или несколько групп.

Выбранные группы будут добавлены в список групп пользователя. Автоматически будет создана связь между пользователем и добавленными группами.

6 Чтобы удалить пользователя из групп, выберите в списке группы, из которых требуется удалить пользователя, и нажмите кнопку **Удалить**:

- Если требуется удалить связи пользователя с выбранными группами, в окне подтверждения установите флажок **Удалить связи пользователя с группами пользователей**.
- В окне подтверждения нажмите кнопку **Да**. Выбранные группы будут удалены из списка групп пользователя. При установке соответствующего флажка будут удалены связи пользователя с этими группами.

7 Выполнив необходимые настройки, нажмите кнопку **OK**.

Добавлять пользователей в группы можно также в разделе **Группы пользователей** (см. «Работа с группами пользователей» на стр. 215).

Изменение связей пользователя с группами пользователей

Если пользователь связан с группой пользователей, в программе ViPNet Деловая почта он может адресовать зашифрованные сообщения отдельным участникам группы или нескольким

пользователям определенного сетевого узла, входящим в группу. Это возможно при условии, что связаны сетевые узлы пользователей (см. «Изменение связей между сетевыми узлами» на стр. 138), которые будут обмениваться сообщениями.

Чтобы изменить связи пользователя с группами пользователей, выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра дважды щелкните пользователя, связи которого требуется изменить.

4 В окне свойств пользователя на левой панели выберите раздел **Связи с группами пользователей**.

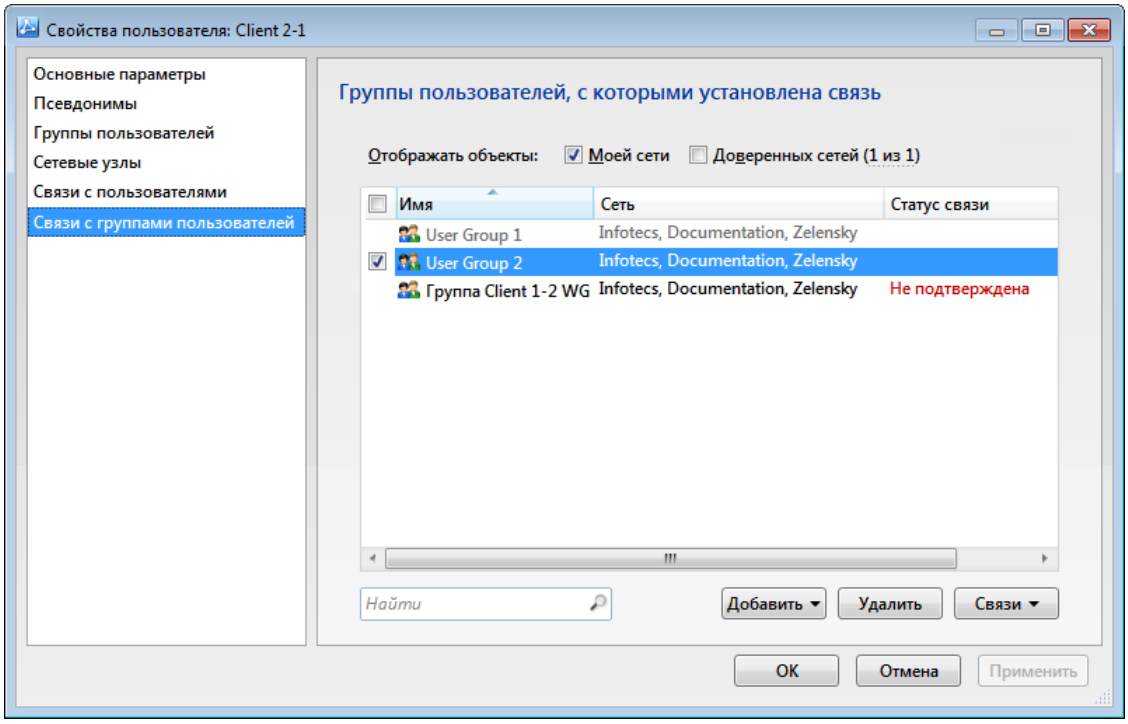

Рисунок 125. Связи пользователя с группами пользователей

5 В разделе **Группы пользователей, с которыми установлена связь** выполните нужные действия:

- Добавьте связи с группами пользователей.
- Удалите связи с группами пользователей.

Примечание. Нельзя удалить связь пользователя с группой, участником которой он является.

- Скопируйте связи другого пользователя.
- Подтвердите, запретите или предложите связи между текущим пользователем и пользователями доверенных сетей.

Для выполнения перечисленных операций выполните действия, описанные в пунктах **5–8** раздела Изменение связей между пользователями (на стр. 207).

Примечание. Если изменены связи пользователя с группами пользователей из доверенных сетей, соответствующим образом будут изменены связи сетевых узлов, на которые добавлен данный пользователь.

6 Выполнив необходимые изменения, нажмите кнопку **OK**.

Работа с группами пользователей

Группы пользователей упрощают управление связями между пользователями. При добавлении пользователя в группу автоматически создается связь между пользователем и этой группой (см. «Изменение связей пользователя с группами пользователей» на стр. 212). Если пользователь связан с группой пользователей, в программе ViPNet Деловая почта он может адресовать зашифрованные сообщения отдельным участникам группы или нескольким пользователям определенного сетевого узла, входящим в группу.

Добавление группы пользователей

Группы пользователей упрощают управление связями между пользователями. Создание связи пользователя с группой (см. «Изменение связей пользователя с группами пользователей» на стр. 212) эквивалентно созданию связей пользователя с каждым участником группы.

Чтобы создать группу пользователей, выполните следующие действия:

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

2 На панели навигации выберите раздел **Группы пользователей**.

3 В разделе **Группы пользователей** на панели инструментов нажмите кнопку  .

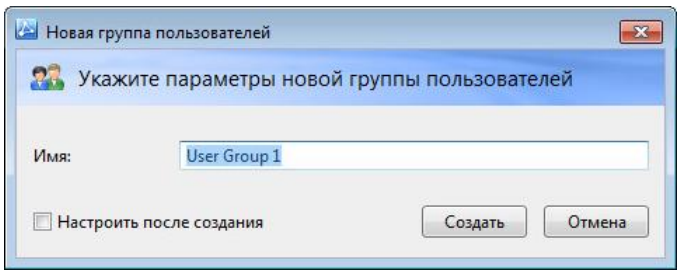

Рисунок 126. Создание группы пользователей

4 В окне **Новая группа пользователей** выполните следующие действия:

4.1 В соответствующее поле введите имя создаваемой группы пользователей.

4.2 Чтобы после создания группы открыть окно для ее настройки, установите флажок **Настроить после создания** (по умолчанию снят).

4.3 Нажмите кнопку **Создать**. В списке **Группы пользователей** появится новая группа.

5 При необходимости измените параметры созданной группы пользователей (см. «Работа с группами пользователей» на стр. 215).

Удаление группы пользователей

Чтобы удалить группы пользователей, выполните следующие действия:

1. В окне **ViPNet Центр управления сетью** выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Группы пользователей**.
3. На панели просмотра в разделе **Группы пользователей** выберите одну или несколько групп для удаления.
4. Нажмите кнопку  на панели инструментов или в контекстном меню группы выберите пункт **Удалить**.
5. В окне подтверждения нажмите кнопку **Удалить группы**.

   Выбранные группы пользователей будут удалены. При этом пользователи, входившие в эти группы, не будут удалены. Связи пользователей с удаленными группами также будут удалены.

Изменение списка участников группы пользователей

Чтобы изменить список пользователей, входящих в группу, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Моя сеть**.
2. На панели навигации выберите раздел **Группы пользователей**.
3. На панели просмотра дважды щелкните группу, список участников которой нужно изменить.
4. В окне свойств группы на левой панели выберите раздел **Пользователи**.

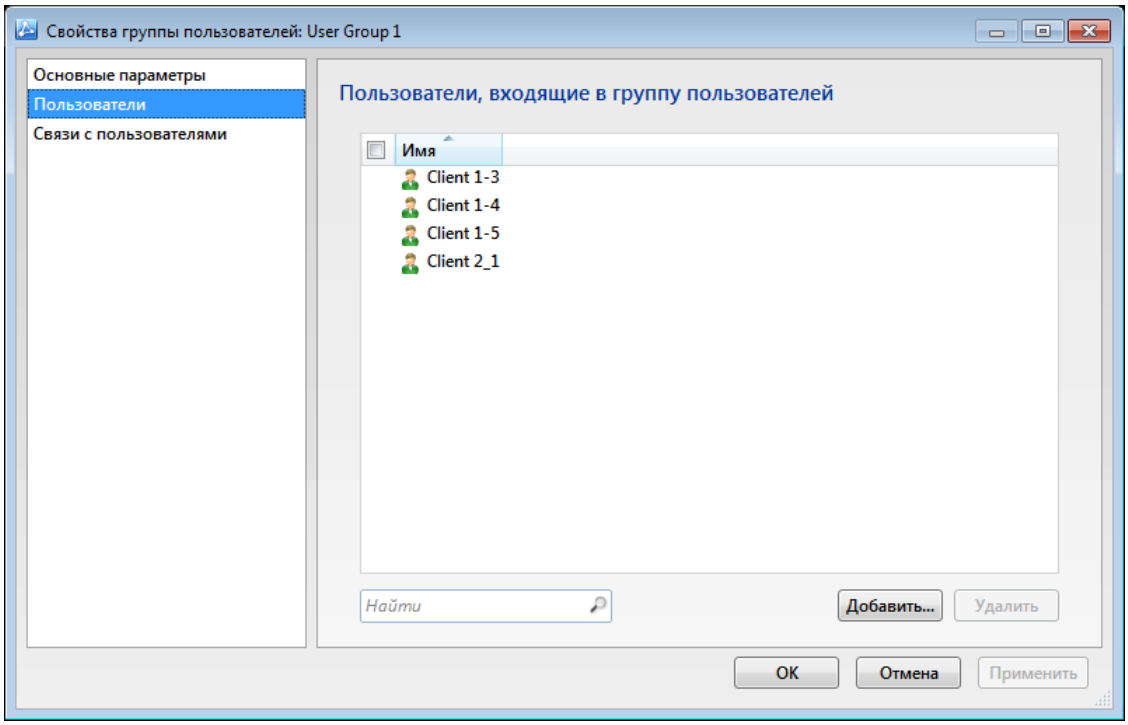

Рисунок 127. Список пользователей, входящих в группу

5 Для добавления пользователей в группу нажмите кнопку **Добавить** и в открывшемся окне выберите из списка нужных пользователей.

Выбранные пользователи будут добавлены в список, автоматически будет создана связь между добавленными пользователями и группой (см. ниже).

6 Для удаления пользователей из группы выберите в списке нужных пользователей и нажмите кнопку **Удалить**:

- Если требуется удалить связи между группой и выбранными пользователями, в окне подтверждения установите флажок **Удалить связи пользователей с группой пользователей**.

  Этот флажок установлен по умолчанию, если были заданы соответствующие параметры удаления пользователей из группы (см. «Параметры работы с объектами сети» на стр. 75).

- В окне подтверждения нажмите кнопку **Да**. Выбранные пользователи будут удалены из списка участников группы.

7 Выполнив необходимые настройки, нажмите кнопку **OK**.

Примечание. Добавить пользователя в группу можно также в окне свойств пользователя в разделе **Группы пользователей** (см. «Изменение списка групп, в которые входит пользователь» на стр. 211).

Изменение связей группы пользователей

Чтобы изменить связи группы пользователей, выполните следующие действия:

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

2 На панели навигации выберите раздел **Группы пользователей**.

3 На панели просмотра дважды щелкните группу, связи которой нужно изменить.

4 В окне свойств группы на левой панели выберите раздел **Связи с пользователями**.

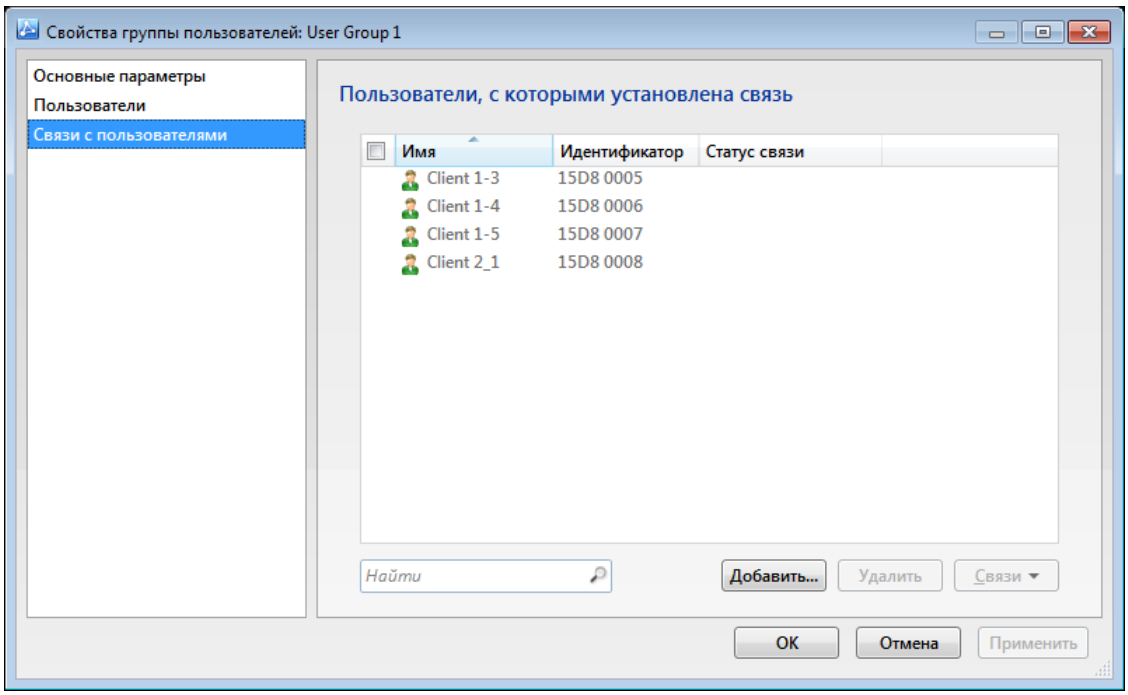

Рисунок 128. Пользователи, связанные с группой пользователей

5 Для добавления связи с пользователями нажмите кнопку **Добавить** и в открывшемся окне выберите из списка пользователей, с которыми нужно создать связь.

6 Для удаления связей с пользователями выберите в списке нужных пользователей и нажмите кнопку **Удалить**.

Примечание. Нельзя удалить связь с пользователем, который является участником группы.

---

7 Если установлено межсетевое взаимодействие с другими сетями ViPNet, то для пользователей доверенных сетей по нажатию кнопки **Связи** доступны следующие действия:

- **Подтвердить связи с группами пользователей** — создать связь текущей группы с выбранным пользователем доверенной сети, если такая связь предложена администратором доверенной сети.

- **Запретить доверенным сетям устанавливать связи с группами** — отказаться от связи текущей группы с выбранным пользователем доверенной сети, если такая связь предложена администратором доверенной сети или подтверждена в своей сети.
- **Предложить доверенной сети связи с группами** — предложить администратору доверенной сети создать связь текущей группы с выбранным пользователем доверенной сети, если такая связь запрещена в своей сети.

8 Выполнив необходимые настройки, нажмите кнопку **OK**.

Примечание. Добавить связь отдельного пользователя с группой пользователей можно также в окне свойств этого пользователя в разделе **Связи с группами пользователей**.

6

Иерархическая система сетей ViPNet

Принцип работы иерархической системы сетей ViPNet 221

Развертывание иерархической системы сетей ViPNet 223

Распределение общей лицензии между сетями 225

Просмотр сведений об общей лицензии 230

Принцип работы иерархической системы сетей ViPNet

При развертывании сети ViPNet в крупной организации, которая имеет большое число филиалов и сотрудников, целесообразно вместо одной корпоративной сети ViPNet создать несколько отдельных сетей (например, по территориальному принципу) и объединить их в иерархическую систему.

Иерархическая система сетей ViPNet включает одну главную сеть и несколько подчиненных сетей. Между главной сетью и каждой подчиненной сетью устанавливается межсетевое взаимодействие (на стр. 232). На все сети ViPNet, входящие в иерархическую систему, выдается специальный файл лицензии `*.itcslic` или `infotecs.reg` (см. «Лицензия на сеть ViPNet» на стр. 23), в котором содержится информация о номерах главной и подчиненных сетей и общих лицензионных ограничениях для всех сетей. В Центре управления сетью главной сети лицензионные ограничения распределяются между подчиненными сетями.

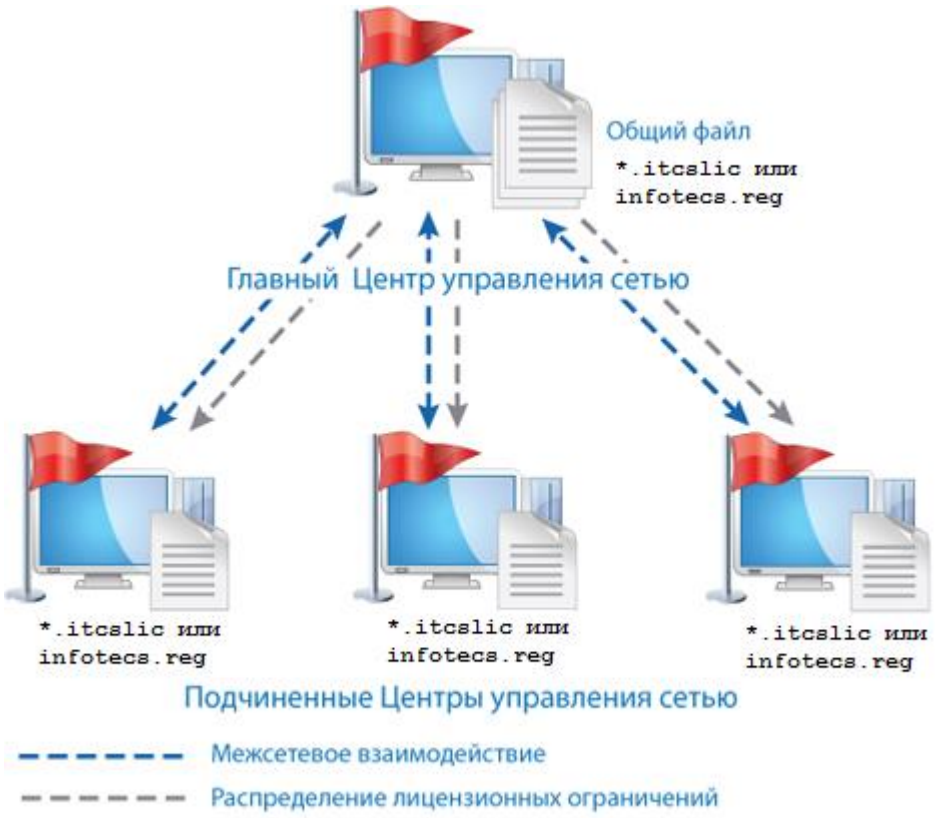

Рисунок 129. Иерархическая система сетей ViPNet

Примечание. Если в главной сети используется файл лицензии `*.itcslic`, перед распределением лицензионных ограничений между подчиненными сетями убедитесь, что для их управления используется ПО ViPNet Administrator версии не

ниже 4.4. Иначе заданные лицензионные ограничения не будут приняты в подчиненных сетях.

Объединение нескольких сетей ViPNet в иерархическую систему имеет следующие преимущества:

- Распределение нагрузки по управлению сетями между несколькими администраторами. Это проще, чем централизованное управление крупной распределенной сетью со сложной структурой.
- Возможность контролировать связи между узлами разных сетей в рамках межсетевого взаимодействия.
- Централизованное распределение лицензионных ограничений между сетями, возможность перераспределения лицензий.

Для объединения нескольких сетей ViPNet в иерархическую систему требуется специальный файл лицензии, содержащий общие лицензионные ограничения для всех сетей. Для получения такого файла обратитесь к представителю ОАО «ИнфоТеКС» (см. «Обратная связь» на стр. 19).

Развертывание иерархической системы сетей ViPNet

Развертывание иерархической системы ViPNet следует начать с установки программы ViPNet Центр управления сетью в главной сети и распределения лицензионных ограничений для подчиненных сетей.

Чтобы создать иерархическую систему сетей ViPNet, выполните следующие действия:

1 Определите основные параметры иерархической системы сетей ViPNet, которую вы хотите создать:

- Требуемое количество сетей ViPNet в вашей иерархической системе. Если вы хотите включить с состав иерархической системы существующие сети ViPNet, сообщите номера этих сетей представителю ОАО «ИнфоТеКС».
- Роли сетевых узлов, которые вы планируете использовать, общее количество узлов в каждой роли.

Подробнее о планировании сети ViPNet см. документ «Развертывание сети ViPNet. Руководство администратора».

2 Запросите у представителя ОАО «ИнфоТеКС» (см. «Обратная связь» на стр. 19) файл лицензии `*.itcslic` или `infotecs.reg` с требуемыми параметрами.

3 Подготовьте рабочее место администратора главной сети ViPNet:

- Если вы создаете главную сеть заново, на рабочем месте администратора главной сети ViPNet установите программу ViPNet Центр управления сетью (см. «Установка программы ViPNet Центр управления сетью» на стр. 48). Во время установки серверного приложения укажите общий для всей иерархической системы файл лицензии.
- Если вы хотите сделать главной сетью какую-либо существующую сеть ViPNet, замените текущий файл лицензии этой сети на общий файл лицензии (см. «Обновление лицензии» на стр. 108). При этом необходимо, чтобы номер этой сети был указан в общем файле лицензии в качестве номера главной сети.

В результате в представлении **Доверенные сети** (см. «Представление „Доверенные сети“» на стр. 56) автоматически появятся подчиненные сети ViPNet (если межсетевое взаимодействие с ними не было установлено ранее).

Примечание. В Центре управления сетью главной сети ViPNet подчиненные сети отмечены значком  . В Центре управления сетью подчиненной сети ViPNet главная сеть отмечена значком  .

---

4 В Центре управления сетью главной сети ViPNet распределите лицензионные ограничения между подчиненными сетями (см. «Распределение общей лицензии между сетями» на стр. 225).

5 Если какие-либо из подчиненных сетей уже развернуты и функционируют, для передачи в эти сети новых лицензионных файлов с заданными вами ограничениями используйте механизм межсетевого взаимодействия:

- Если с какой-либо сетью уже установлено межсетевое взаимодействие, отправьте в эту сеть межсетевую информацию (см. «Отправка межсетевой информации» на стр. 251).
- Если подчиненная сеть существует, но с ней не установлено межсетевое взаимодействие, установите взаимодействие (см. «Организация межсетевого взаимодействия» на стр. 233).

Вместе с межсетевой информацией в подчиненные сети будут переданы новые файлы лицензии.

6 Если какие-либо из подчиненных сетей еще не существуют, для таких сетей выполните следующие действия:

- В представлении **Доверенные сети** выберите раздел **Свойства сетей**.
- На панели просмотра дважды щелкните нужную подчиненную сеть.
- В открывшемся окне **Свойства подчиненной сети** сохраните файл лицензии для подчиненной сети (см. «Назначение лицензионных ограничений для отдельной сети» на стр. 227).
- Используйте сохраненный файл лицензии для установки программного обеспечения ViPNet Administrator в подчиненной сети.
- Завершите организацию межсетевого взаимодействия с подчиненной сетью (см. «Организация межсетевого взаимодействия» на стр. 233).

В результате выполненных действий в подчиненные сети будут переданы файлы лицензии, содержащие заданные вами лицензионные ограничения, и со всеми подчиненными сетями будет установлено межсетевое взаимодействие.

Распределение общей лицензии между сетями

В Центре управления сетью главной сети ViPNet вы можете распределить суммарные лицензионные ограничения, заданные в общем файле лицензии `*.itcslic` или `infotecs.reg` для иерархической системы сетей ViPNet, между своей сетью и подчиненными сетями.

Примечание. Если в главной сети используется файл лицензии `*.itcslic`, распределение лицензионных ограничений между подчиненными сетями, управляемыми с помощью ПО ViPNet Administrator версии 4.2 и ниже, будет невозможно.

Распределение лицензий можно выполнить двумя способами:

- Одновременно для всех сетей, входящих в состав иерархической системы.
- Для каждой сети по отдельности.

Распределение лицензии для всех сетей

Чтобы распределить лицензионные ограничения для всех сетей одновременно, выполните следующие действия:

1 В программе ViPNet Центр управления сетью главной сети в меню **Лицензия** выберите пункт **Распределить лицензию**.

Откроется окно **Распределение лицензий**, в котором представлен список лицензионных ограничений. Представление информации в этом окне аналогично представлению информации в окне **Сведения о лицензии для своей сети** (см. «Просмотр сведений о лицензии для своей сети» на стр. 106).

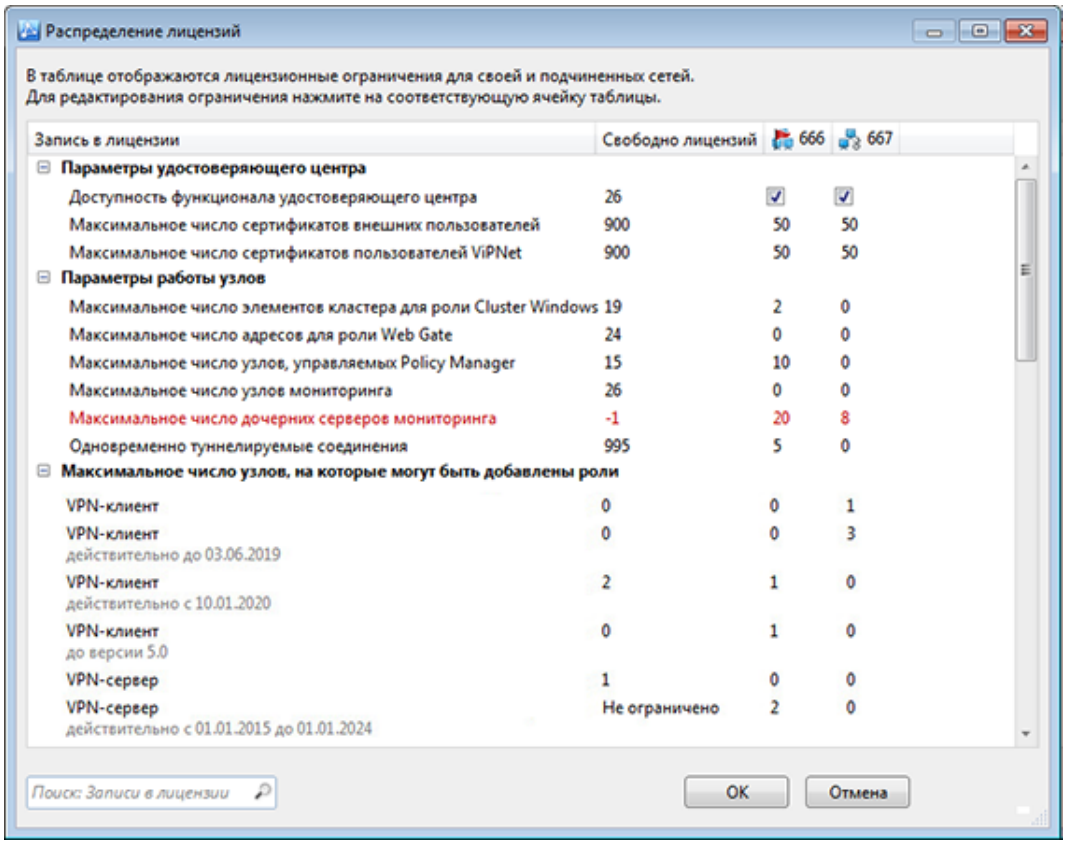

Рисунок 130. Распределение лицензионных ограничений

2 Чтобы изменить лицензионные ограничения для своей или подчиненной сети:

- В столбце выбранной сети щелкните число, выражающее лицензионное ограничение какого-либо параметра.
- В появившемся поле введите значение лицензионного ограничения, которое вы хотите задать для выбранной сети.
- Таким же образом задайте другие необходимые ограничения для выбранной сети.

Для каждого параметра сумма заданных ограничений всех сетей не должна превышать общего ограничения для иерархической системы. Если по какому-либо параметру общее ограничение будет превышено, соответствующая строка в списке будет выделена красным цветом и сохранение изменений, внесенных в распределение лицензий, будет невозможно.

3 Завершив распределение лицензионных ограничений, нажмите кнопку **OK**. После сохранения изменений появится сообщение об успешном распределении лицензии.

4 Отправьте обновление межсетевой информации (см. «Отправка межсетевой информации» на стр. 251) в подчиненные сети, для которых были изменены лицензионные ограничения.

Если с какой-либо подчиненной сетью межсетевое взаимодействие не установлено, сохраните новый файл лицензии (см. «Назначение лицензионных ограничений для отдельной сети» на стр. 227) и передайте его администратору подчиненной сети для обновления лицензии (см. «Обновление лицензии» на стр. 108).

Назначение лицензионных ограничений для отдельной сети

Чтобы назначить лицензионные ограничения для какой-либо подчиненной сети ViPNet, выполните следующие действия:

1 В программе ViPNet Центр управления сетью главной сети выберите представление **Доверенные сети** (см. «Представление „Доверенные сети“» на стр. 56).

2 На панели навигации выберите раздел **Свойства сетей**.

3 На панели просмотра дважды щелкните нужную подчиненную сеть.

4 В открывшемся окне **Свойства подчиненной сети ViPNet** на панели навигации выберите раздел **Лицензионные ограничения** (см. рисунок на стр. 227).

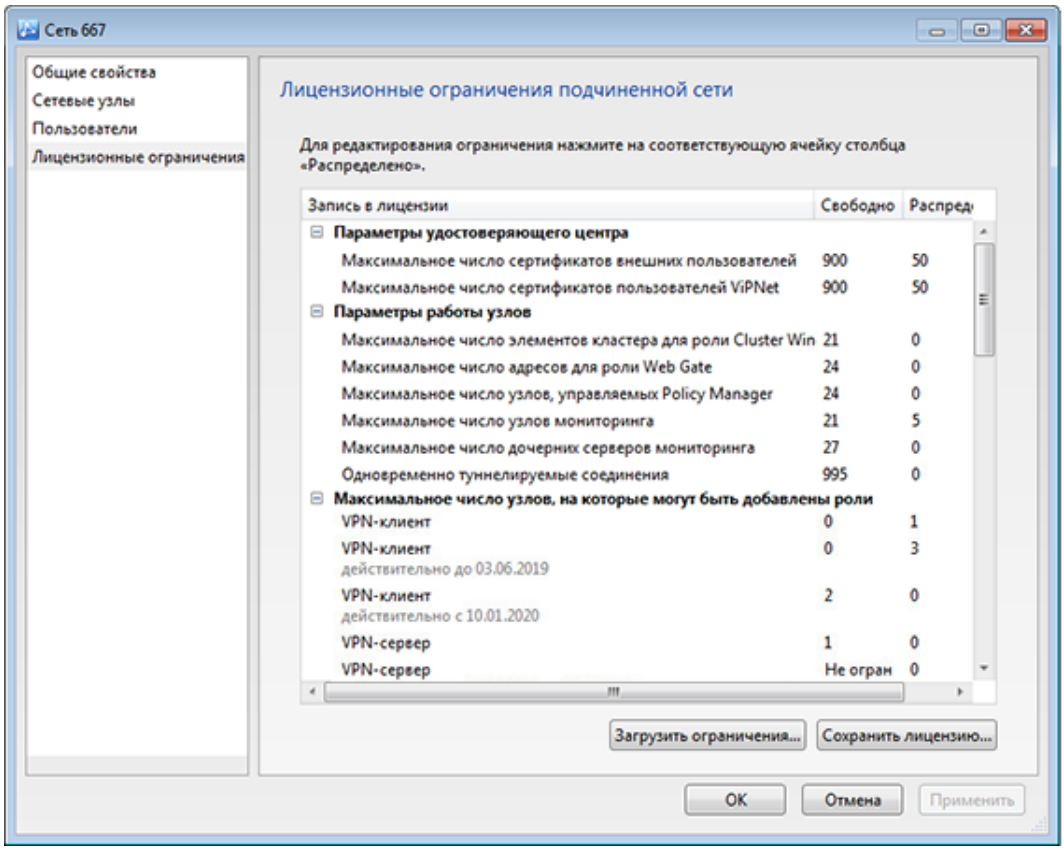

Рисунок 131. Сохранение файла лицензии

5 Задайте лицензионные ограничения для данной подчиненной сети, как описано в разделе Распределение лицензии для всех сетей (на стр. 225).

6 Если у вас имеется предыдущая версия файла `*.itcslic` или `infotecs.reg` для данной подчиненной сети, вы можете загрузить лицензионные ограничения из этого файла. Для этого:

- Нажмите кнопку **Загрузить ограничения**.
- В окне **Открыть** укажите предыдущую версию лицензионного файла для данной подчиненной сети.

В случае успешной загрузки лицензионных ограничений появится соответствующее сообщение. В столбце **Распределено** будут отображены ограничения, загруженные из файла.

7 Чтобы сохранить изменения, нажмите кнопку **Применить**.

8 Если установлено межсетевое взаимодействие, отправьте в эту сеть обновление межсетевой информации (см. «Отправка межсетевой информации» на стр. 251). Вместе с межсетевой информацией в подчиненную сеть будет передан новый файл лицензии.

9 Если межсетевое взаимодействие с подчиненной сетью не установлено, сохраните новый файл лицензии и передайте его администратору этой сети. Для этого:

- Нажмите кнопку **Сохранить лицензию**.
- В окне **Обзор папок** укажите папку для сохранения файлов лицензии и нажмите кнопку **ОК**.

  В указанную папку будет сохранен файл `*.itcslic` или `infotecs.reg` для данной подчиненной сети.
- Передайте сохраненный файл администратору подчиненной сети для обновления лицензии (см. «Обновление лицензии» на стр. 108).

Вы также можете назначить лицензионные ограничения для своей сети. Например, это может потребоваться при переходе на иерархическую систему сетей ViPNet. В данном случае лицензионные ограничения вы можете загрузить из старого файла лицензии и при необходимости отредактировать их вручную. Для этого после обновления общей лицензии на сеть ViPNet выполните следующие действия:

1 В программе ViPNet Центр управления сетью своей сети в меню **Лицензия** выберите пункт **Лицензионные ограничения своей сети**.

2 В открывшемся окне **Лицензионные ограничения своей сети** с помощью кнопки **Загрузить ограничения** загрузите лицензионные ограничения из предыдущего файла лицензии, после чего при необходимости отредактируйте их вручную (как описано в разделе Распределение лицензии для всех сетей (на стр. 225)).

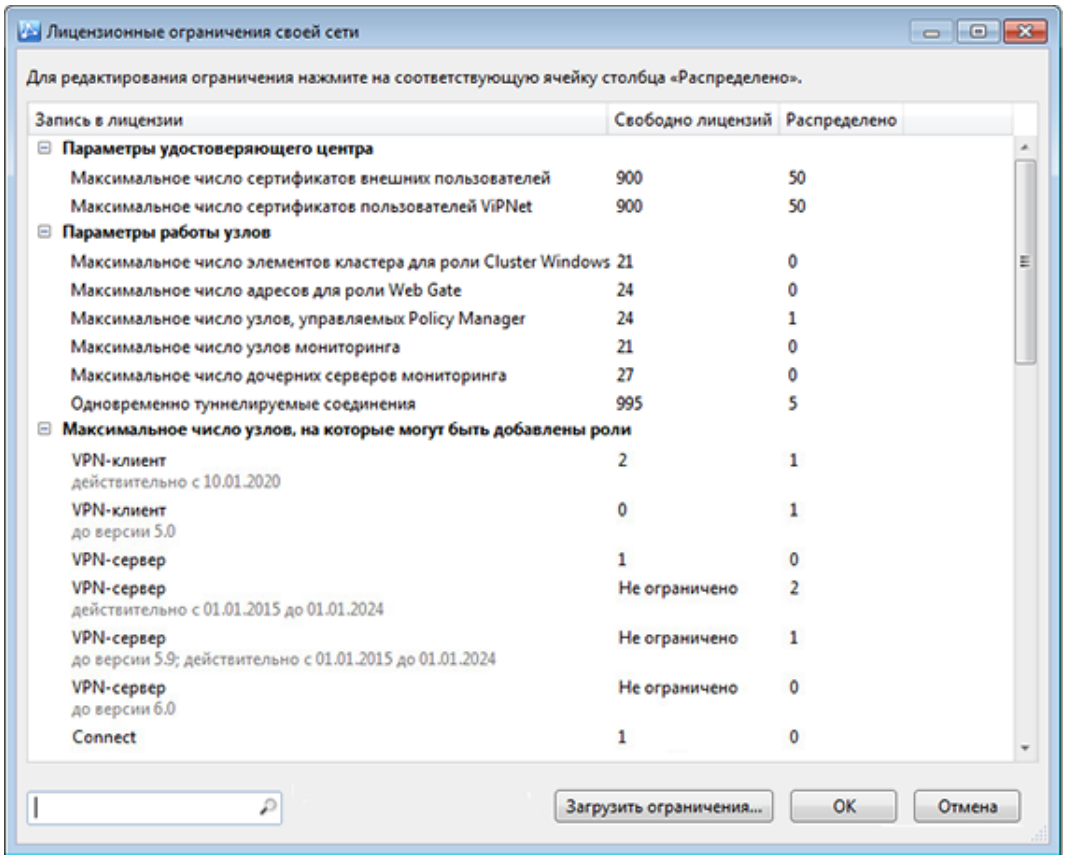

Рисунок 132. Назначение лицензионных ограничений для своей сети

3 Для сохранения настроек нажмите кнопку **OK**.

Просмотр сведений об общей лицензии

Для просмотра информации об общей лицензии для иерархической системы сетей ViPNet и об использовании этой лицензии выполните следующие действия:

1 В программе ViPNet Центр управления сетью главной сети в меню **Лицензия** выберите пункт **Сведения об общей лицензии**.

Откроется окно **Сведения об общей лицензии**. Представление информации в этом окне аналогично представлению информации в окне **Сведения о лицензии для своей сети** (см. «Просмотр сведений о лицензии для своей сети» на стр. 106).

2 На вкладке **Общая информация** просмотрите сведения о номерах главной и подчиненных сетей ViPNet, сроке действия лицензии, максимальной допустимой версии программного обеспечения ViPNet Administrator, а также контактные данные поставщика лицензии.

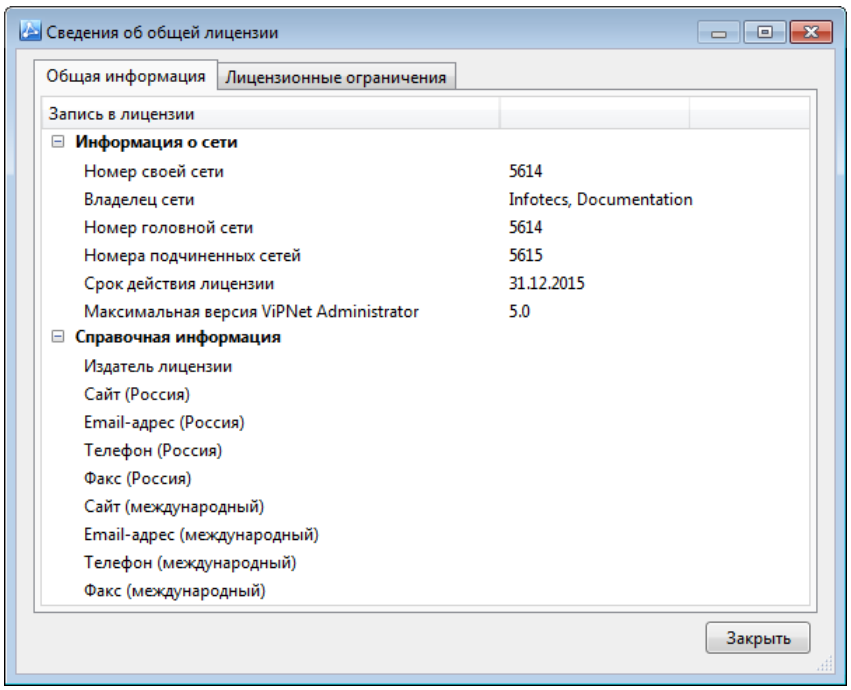

Рисунок 133. Общие сведения о лицензии для иерархической системы сетей ViPNet

Примечание. В случае использования файла лицензии `*.itcslic`, в окне **Сведения об общей лицензии** на вкладке **Общая информация** не отображаются контактные данные поставщика лицензии. Чтобы просмотреть данную информацию, в главном окне программы ViPNet Центр управления сетью перейдите в меню **Справка** > **О программе**.

3 На вкладке **Лицензионные ограничения** ознакомьтесь с общими ограничениями на структуру сетей ViPNet, входящих в иерархическую систему.

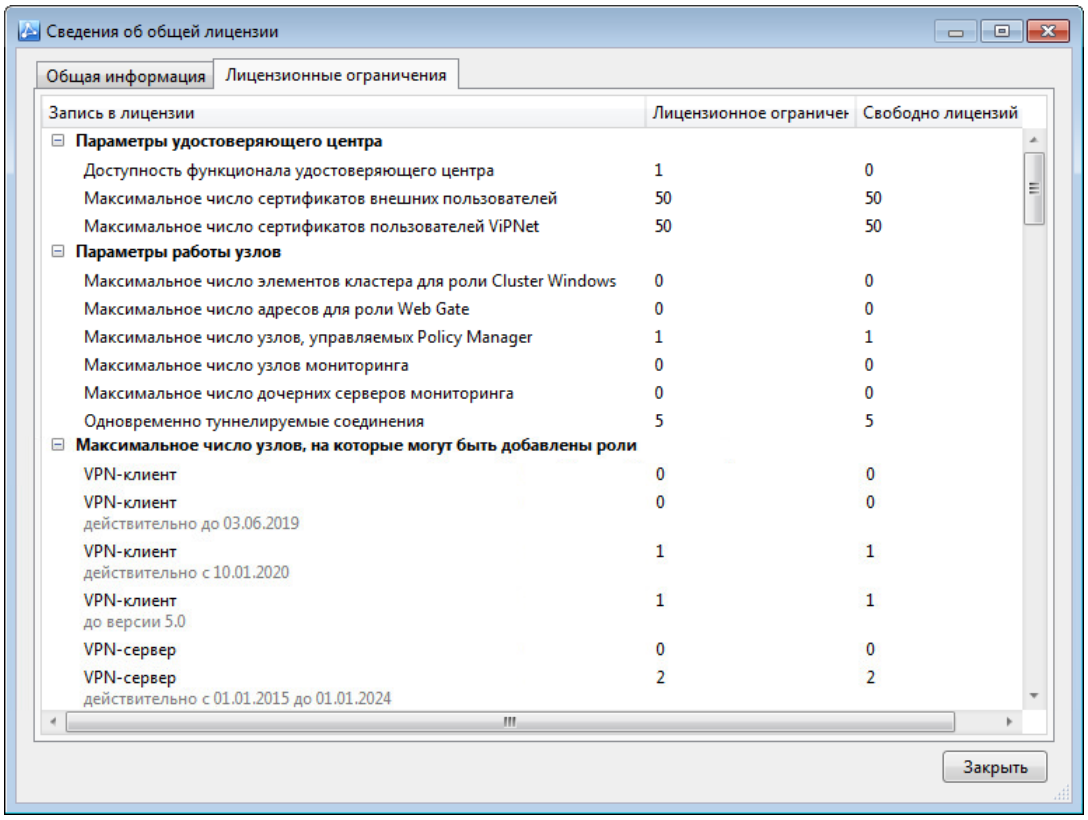

Рисунок 134. Лицензионные ограничения для иерархической системы сетей ViPNet

4 Получив необходимую информацию, нажмите кнопку **Закрыть**.

7

Межсетевое взаимодействие

Организация межсетевого взаимодействия 233

Связи с объектами доверенных сетей 242

Изменение шлюзового координатора своей сети 249

Отправка межсетевой информации 251

Прием межсетевой информации 255

Прекращение межсетевого взаимодействия 261

Организация межсетевого взаимодействия

Если требуется организовать канал для защищенного обмена информацией между двумя разными сетями ViPNet, между этими сетями следует установить межсетевое взаимодействие. Другие сети ViPNet, с которыми в вашей сети установлено межсетевое взаимодействие, называются доверенными сетями.

Для каждой доверенной сети в Удостоверяющем и ключевом центре создается межсетевой мастер-ключ, на основе которого формируются ключи для защищенного обмена информацией с данной доверенной сетью. Подробнее о создании межсетевых мастер-ключей см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Работа с мастер-ключами».

Также для каждой доверенной сети назначается шлюзовой координатор (см. глоссарий, стр. 309). Шлюзовой координатор своей сети связан с аналогичным координатором доверенной сети, и через эти координаторы направляются все транспортные конверты (см. глоссарий, стр. 308), передаваемые между двумя сетями.

Чтобы обеспечить возможность защищенного соединения между сетевыми узлами вашей и доверенной сетей, обмена письмами в программе ViPNet Деловая почта, файлами и так далее, следует создать связи между объектами вашей сети ViPNet и объектами доверенной сети. Об особенностях создания связей с объектами доверенной сети см. раздел Связи с объектами доверенных сетей (на стр. 242).

Организация межсетевого взаимодействия между сетями ViPNet состоит из следующих этапов:

1. Администратор первой сети ViPNet, инициирующий межсетевое взаимодействие (см. «Инициация межсетевого взаимодействия» на стр. 234), создает в Центре управления сетью файл межсетевой информации, а в Удостоверяющем и ключевом центре — межсетевой мастер-ключ. Затем он передает файл межсетевой информации и межсетевой мастер-ключ администратору второй сети ViPNet.
2. Администратор второй сети ViPNet принимает межсетевую информацию (см. «Прием и обработка полученной межсетевой информации» на стр. 236), затем создает файл с ответной межсетевой информацией и передает его администратору первой сети.

   Затем администратор второй сети импортирует переданный ему межсетевой мастер-ключ.
3. Администратор первой сети завершает организацию взаимодействия приемом ответной межсетевой информации (см. «Завершение организации межсетевого взаимодействия» на стр. 240).
4. Администратор каждой сети создает новые справочники и ключи и отправляет их на узлы своей сети (см. «Обновление справочников и ключей» на стр. 87).

   После этого узлы доверенных сетей, участвующие в межсетевом взаимодействии, могут обмениваться информацией друг с другом.

Инициация межсетевого взаимодействия

Для инициирования межсетевого взаимодействия с другой сетью ViPNet необходимо:

- создать файл с межсетевой информацией о своей сети;
- создать межсетевой мастер-ключ;
- сохранить файл межсетевой информации на съемный носитель;
- передать носитель с межсетевой информацией вместе с межсетевым мастер-ключом администратору другой сети ViPNet.

Чтобы инициировать межсетевое взаимодействие, выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Доверенные сети** выберите пункт **Установить взаимодействие**. Будет запущен мастер **Установка межсетевого взаимодействия**.

2 На первой странице мастера выберите вариант **Я инициатор межсетевого взаимодействия** и нажмите кнопку **Далее**.

3 На странице **Задайте информацию о другой сети ViPNet и координатор для связи с ней** укажите номер сети, с которой требуется установить взаимодействие, имя сети, которое будет отображаться в программе ViPNet Центр управления сетью, и выберите шлюзовой координатор своей сети. Затем нажмите кнопку **Далее**.

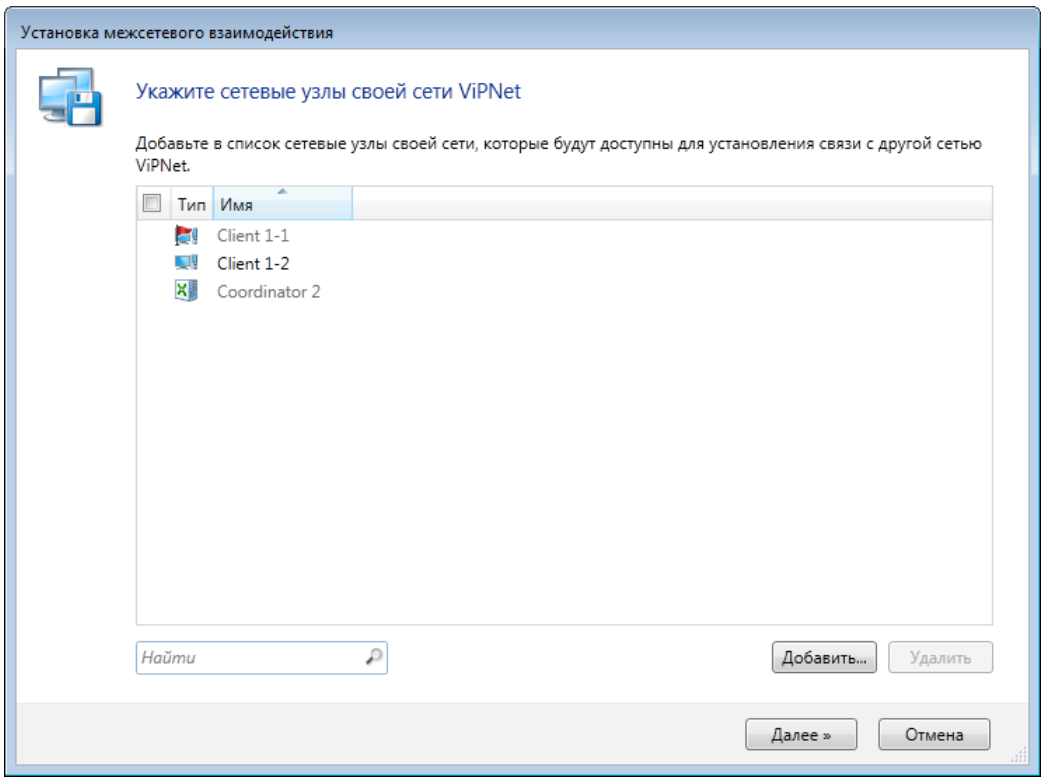

Рисунок 135. Организация межсетевого взаимодействия

4 На странице **Укажите сетевые узлы своей сети ViPNet** выберите узлы своей сети, которые будут участвовать во взаимодействии с узлами доверенной сети. Вы можете выбрать сразу все сетевые узлы с помощью флажка, расположенного в заголовке списка.

Центр управления сетью и шлюзовой координатор своей сети должны обязательно присутствовать в списке узлов для взаимодействия, их невозможно удалить.

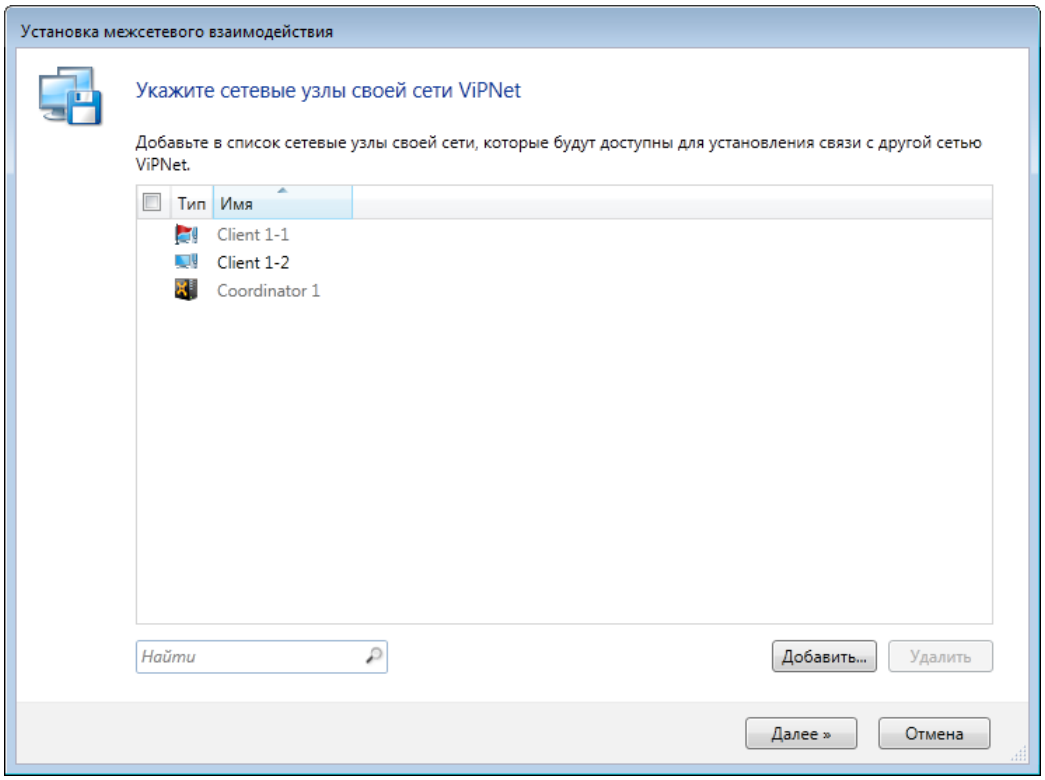

Рисунок 136. Выбор узлов своей сети для межсетевого взаимодействия

Выбрав сетевые узлы, нажмите кнопку **Далее**.

5 На странице **Укажите пользователей своей сети ViPNet** выберите пользователей для межсетевого взаимодействия. По умолчанию в список добавлены пользователи сетевых узлов, выбранных на предыдущей странице.

Примечание. Если для межсетевого взаимодействия выбран сетевой узел, но не выбран ни один пользователь этого узла, сведения об этом узле не будут включены в межсетевую информацию. Исключениями являются Центр управления сетью и шлюзовой координатор.

Выбрав пользователей, нажмите кнопку **Далее**.

6 На открывшейся странице при необходимости укажите комментарий для администратора сети, с которой устанавливается взаимодействие, и нажмите кнопку **Далее**.

7 На странице **Укажите файл для сохранения межсетевой информации** нажмите кнопку **Обзор** и укажите папку для сохранения файла межсетевой информации. Затем нажмите кнопку **Далее**.

8 На странице **Сохранение межсетевой информации** после завершения записи файла нажмите кнопку **Далее**, на следующей странице нажмите кнопку **Готово**.

9 Передайте созданный файл межсетевой информации администратору доверенной сети.

Вместе с файлом межсетевой информации передайте администратору доверенной сети межсетевой мастер-ключ, созданный для этой сети в Удостоверяющем и ключевом центре. Подробнее о создании межсетевого мастер-ключа см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Особенности создания межсетевой информации в ПО ViPNet Administrator 3.x

Для организации межсетевого взаимодействия с доверенной сетью, в которой используется ПО ViPNet Administrator версии 3.x, после формирования данных для экспорта администратору этой сети необходимо выполнить следующие дополнительные действия, чтобы создать файл межсетевой информации, поддерживаемый ПО ViPNet Administrator версии 4.x:

1 В окне **ViPNet Центр управления сетью** в меню **Службы** выбрать команду **Экспорт**.

2 В окне **Экспорт** выбрать нужную доверенную сеть и нажать кнопку **Архив**.

3 В окне **Задайте каталог назначения** указать папку, в которую будет скопирован архив (по умолчанию программа предлагает папку `\NEW\EXPORT`) и нажать кнопку **Принять**.

Файл формата LZH будет помещен в папку с именем, совпадающим с номером доверенной сети, для которой предназначен экспорт. Далее администратор сети, в которой используется ПО ViPNet Administrator 3.x, может передать его вам.

Прием и обработка полученной межсетевой информации

Если межсетевое взаимодействие было инициировано администратором другой сети ViPNet, он передает вам файл межсетевой информации и межсетевой мастер-ключ.

Чтобы принять файл с межсетевой информацией, выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Доверенные сети** выберите пункт **Установить взаимодействие**. Будет запущен мастер **Установка межсетевого взаимодействия**.

2 На первой странице мастера выберите вариант **Я принимаю файл с межсетевой информацией** и нажмите кнопку **Далее**.

3 На странице **Загрузка межсетевой информации из файла** укажите файл с межсетевой информацией, полученный от администратора сети ViPNet, который инициировал межсетевое

взаимодействие. После указания файла в окне мастера появится предупреждение, что взаимодействие с сетью не установлено.

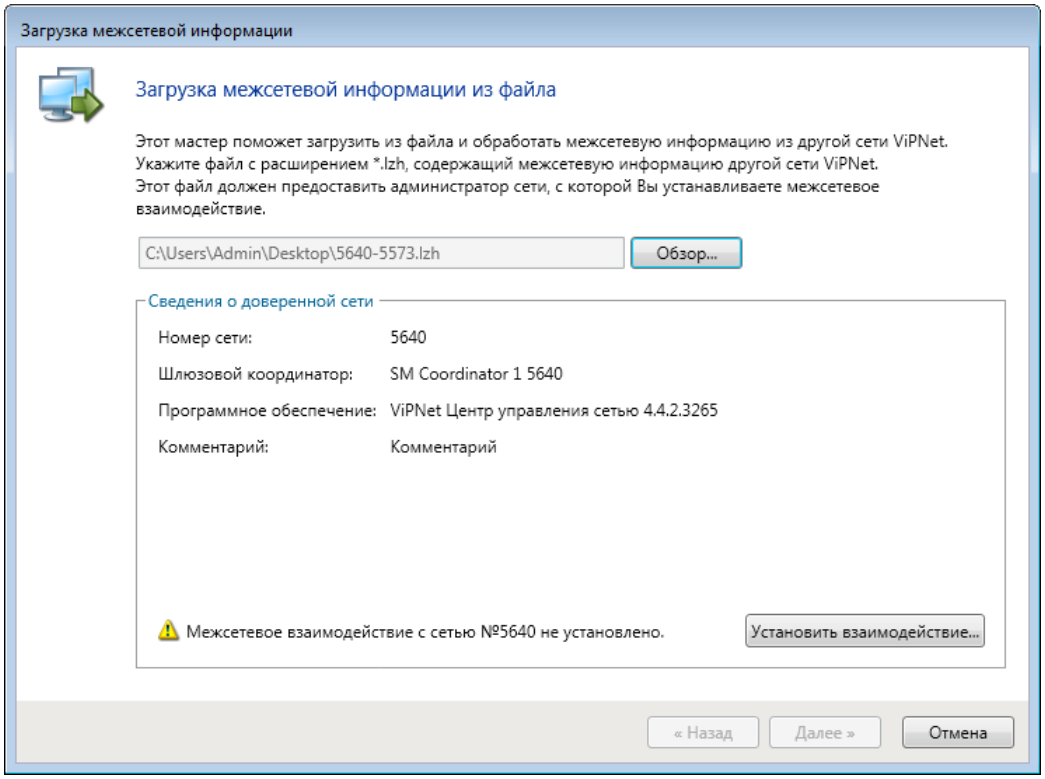

Рисунок 137. Прием и обработка полученной межсетевой информации

4 Чтобы продолжить загрузку межсетевой информации, нажмите кнопку **Установить взаимодействие**.

5 На странице **Задайте информацию о другой сети ViPNet и координатор для связи с ней** (см. рисунок на стр. 234) выберите шлюзовой координатор своей сети, затем нажмите кнопку **Далее**.

6 Если файл межсетевой информации содержит ошибки, откроется страница **Проверка межсетевой информации** со списком обнаруженных конфликтных или неполных данных.

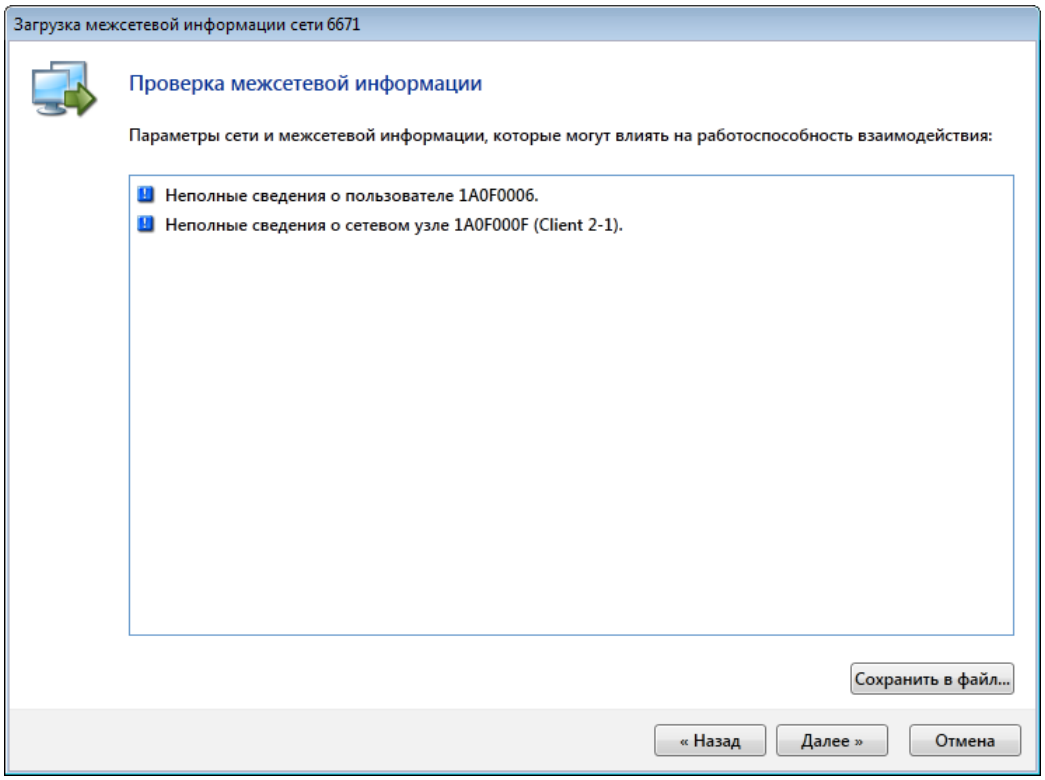

Рисунок 138. В межсетевой информации обнаружены неполные данные

При обнаружении конфликтных данных загрузка межсетевой информации будет невозможна. В этом случае обратитесь к администратору доверенной сети для устранения конфликтов.

Чтобы продолжить обработку межсетевой информации, нажмите кнопку **Далее**.

7 На странице **Изменения в межсетевой информации** ознакомьтесь со списком узлов и пользователей, которые были выбраны для межсетевого взаимодействия администратором другой сети ViPNet. Затем нажмите кнопку **Далее**.

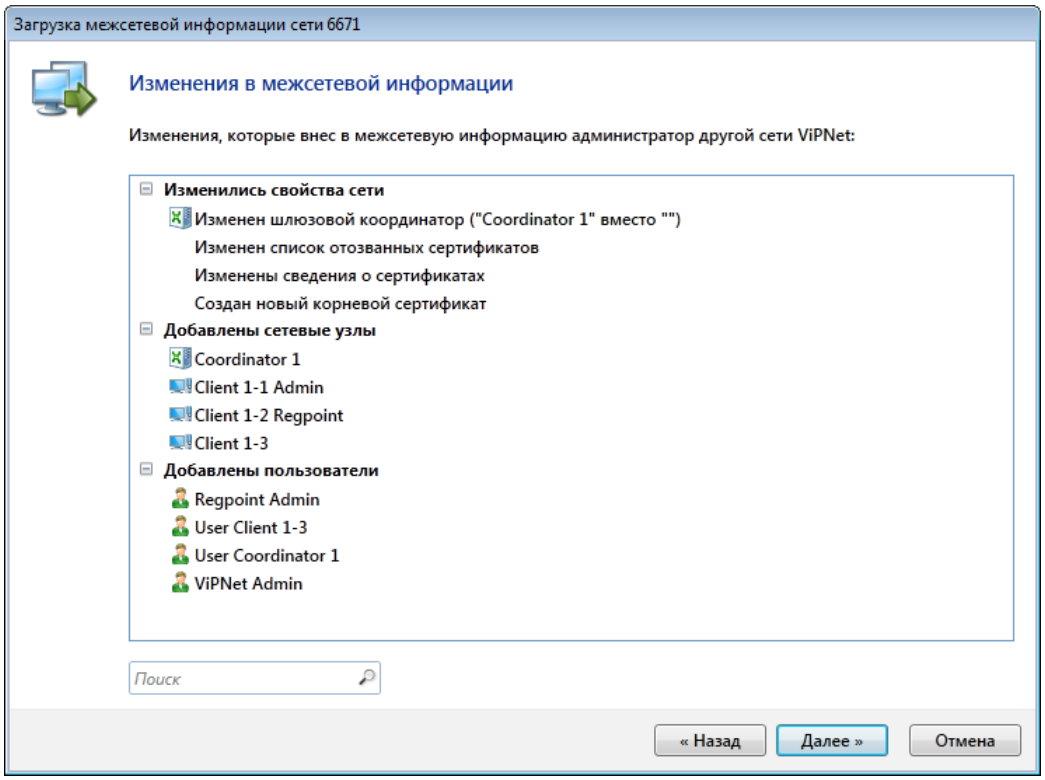

Рисунок 139. Просмотр объектов, добавленных в межсетевую информацию

8 На странице **Загрузка межсетевой информации** после завершения обработки информации нажмите кнопку **Готово**. Сеть будет добавлена в список доверенных сетей.

Примечание. Если ваша сеть является частью иерархической системы сетей ViPNet, главная сеть или подчиненные сети присутствуют в списке доверенных сетей по умолчанию.

---

9 Для пользователей новой доверенной сети задайте связи с пользователями своей сети (см. «Изменение связей с объектами доверенной сети» на стр. 245).

10 После приема и обработки полученной межсетевой информации в программе ViPNet Удостоверяющий и ключевой центр импортируйте переданный администратором другой сети ViPNet межсетевой мастер-ключ. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

11 Подготовьте сертификаты администраторов и списки аннулированных сертификатов вашей сети для передачи в доверенную сеть в составе ответной межсетевой информации. Для этого в программе ViPNet Удостоверяющий и ключевой центр в меню **Сервис** выберите пункт **Экспорт межсетевой информации**.

12 В программе ViPNet Центр управления сетью в представлении **Доверенные сети** выберите раздел **Свойства сетей**.

13 На панели просмотра щелкните правой кнопкой мыши добавленную доверенную сеть и в контекстном меню выберите пункт **Создать межсетевую информацию**.

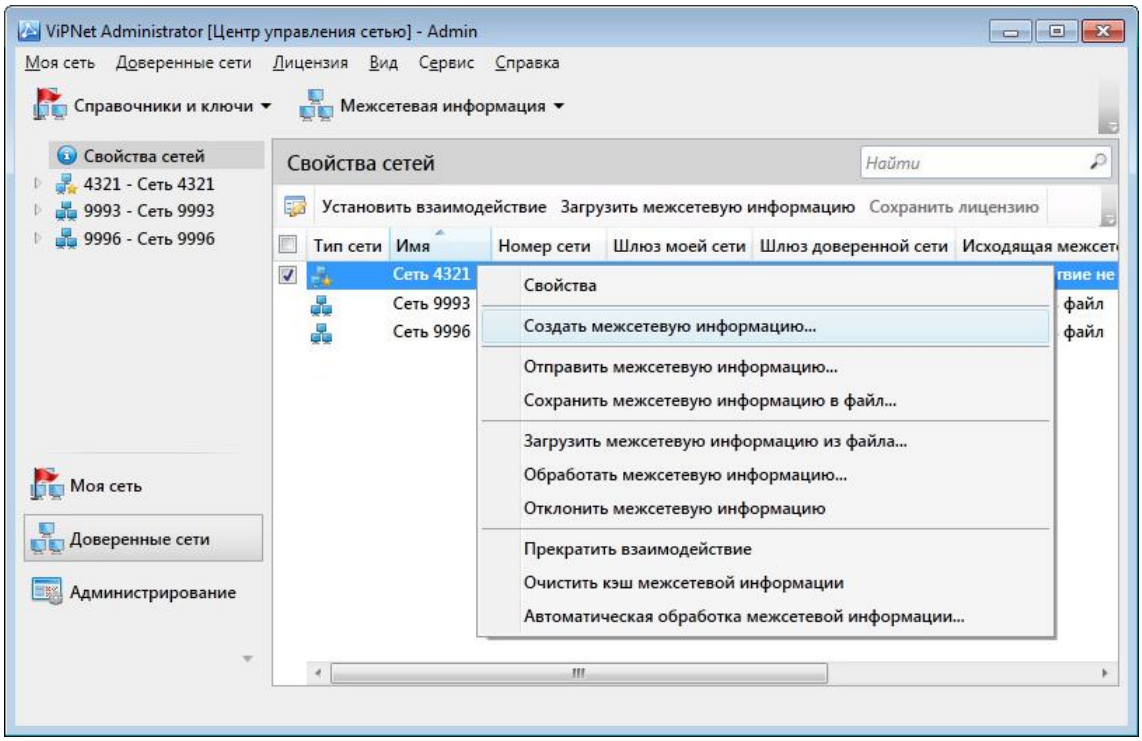

Рисунок 140. Создание межсетевой информации

14 В появившемся окне установите соответствующий флажок и нажмите кнопку **Создать**, чтобы автоматически отправить межсетевую информацию после создания.

15 После создания ответной межсетевой информации сохраните ее на съемный носитель. Для этого снова щелкните доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить межсетевую информацию в файл**, затем в окне **Сохранить как** укажите папку для сохранения межсетевой информации.

16 Передайте созданный файл администратору доверенной сети.

17 Создайте новые справочники и ключи для узлов своей сети, участвующих в межсетевом взаимодействии, и отправьте их на узлы (см. «Обновление справочников и ключей» на стр. 87).

Завершение организации межсетевого взаимодействия

Инициировав процедуру организации межсетевого взаимодействия, вы подготовили и передали администратору другой сети ViPNet файл межсетевой информации о своей сети и межсетевой мастер-ключ. Администратор другой сети принял и обработал полученную от вас межсетевую информацию, а затем передал вам файл с ответной межсетевой информацией. Теперь необходимо принять ответную информацию и обработать ее.

Чтобы завершить организацию межсетевого взаимодействия, выполните следующие действия:

1. Получите у администратора доверенной сети ViPNet файл, содержащий ответную межсетевую информацию.
2. В окне программы ViPNet Центр управления сетью в меню **Доверенные сети** выберите пункт **Загрузить межсетевую информацию из файла**.
3. В окне **Загрузка межсетевой информации** укажите файл межсетевой информации, полученной от администратора другой сети ViPNet (см. «Загрузка межсетевой информации из файла» на стр. 259).
4. Примите ответную межсетевую информацию с помощью мастера **Обработка межсетевой информации** (см. «Обработка межсетевой информации для отдельной сети» на стр. 256).

   После завершения работы мастера межсетевое взаимодействие будет установлено.
5. Для узлов вашей сети, участвующих в межсетевом взаимодействии, создайте и отправьте новые справочники и ключи (см. «Обновление справочников и ключей» на стр. 87).

Связи с объектами доверенных сетей

Связи сетевых узлов и пользователей вашей сети с сетевыми узлами и пользователями доверенной сети обеспечивают возможность взаимодействия этих объектов между собой, так же как связи между объектами одной сети ViPNet (см. «Связи между объектами сети ViPNet» на стр. 29).

Однако создание связей между объектами вашей сети и объектами доверенных сетей и управление этими связями имеет ряд особенностей:

- В межсетевом взаимодействии обязательно участвует пара объектов — пользователь и сетевой узел этого пользователя. Участие в межсетевом взаимодействии сетевого узла и пользователя по отдельности невозможно.

  

  Примечание. Исключение составляют узлы, которые являются Центром управления сетью и шлюзовым координатором вашей сети. По умолчанию пользователи этих узлов не участвуют в межсетевом взаимодействии, вы можете добавить их вручную.

- При межсетевом взаимодействии вы можете изменить только связи между пользователями. Связи между сетевыми узлами автоматически изменяются соответствующим образом.
- При изменении связей с объектами доверенной сети необходимо согласовать изменения с администратором этой доверенной сети. Для этого предназначены статусы связей между объектами доверенных сетей (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).
- При создании связи между клиентом своей сети и сетевым узлом доверенной сети создайте связь между координатором (если он не является шлюзовым), на котором зарегистрирован клиент, и одним из следующих сетевых узлов:
  - шлюзовым координатором своей сети;
  - шлюзовым координатором доверенной сети.

  При создании связи между координатором своей сети и клиентом доверенной сети, связываемый координатор должен быть шлюзовым или иметь связь с одним из следующих сетевых узлов:
  - шлюзовым координатором своей сети;
  - шлюзовым координатором доверенной сети.
- Если установлено межсетевое взаимодействие с сетью ViPNet, в которой используется версия программного обеспечения ViPNet Administrator ниже, чем 4.0:
  - Со стороны этой доверенной сети в межсетевом взаимодействии могут участвовать группы пользователей. Это происходит в том случае, если в межсетевом взаимодействии участвуют несколько пользователей из одной группы.

- Вы не можете удалить подтвержденные связи с пользователями и группами пользователей этой доверенной сети. В случае необходимости вы можете запретить такие связи (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).

При установлении межсетевого взаимодействия обязательными являются следующие связи:

- Связи между Центрами управления сетью доверенных сетей.
- Связи между шлюзовыми координаторами доверенных сетей.

Изменение списка объектов, участвующих в межсетевом взаимодействии

Для каждой доверенной сети вы можете задать список сетевых узлов и пользователей вашей сети, которые могут участвовать в межсетевом взаимодействии с определенной доверенной сетью.

Чтобы изменить список объектов, участвующих в межсетевом взаимодействии с определенной доверенной сетью, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.
2. На панели навигации выберите раздел **Свойства сетей**.
3. На панели просмотра дважды щелкните доверенную сеть, для которой требуется изменить параметры межсетевого взаимодействия. Откроется окно с названием доверенной сети.
4. Для просмотра или изменения списка узлов своей сети, участвующих во взаимодействии с доверенной сетью, на панели навигации выберите раздел **Сетевые узлы**.
   - Чтобы добавить сетевые узлы в список, нажмите кнопку **Добавить** и в окне **Выбор объектов** выберите один или несколько узлов.

     При добавлении сетевого узла в список пользователей, участвующих в межсетевом взаимодействии, будут добавлены все пользователи этого узла.
   - Чтобы исключить сетевые узлы из межсетевого взаимодействия, выберите их в списке и нажмите кнопку **Удалить**, в окне подтверждения нажмите кнопку **Удалить из списка**.

     При удалении сетевого узла из списка пользователей, участвующих в межсетевом взаимодействии, будут удалены пользователи этого узла. Связи удаленных узлов и пользователей с объектами доверенной сети будут разорваны.

Примечание. Невозможно исключить из межсетевого взаимодействия сетевые узлы, которые имеют связи с узлами доверенной сети в статусе **Предложена доверенной сетью** (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).

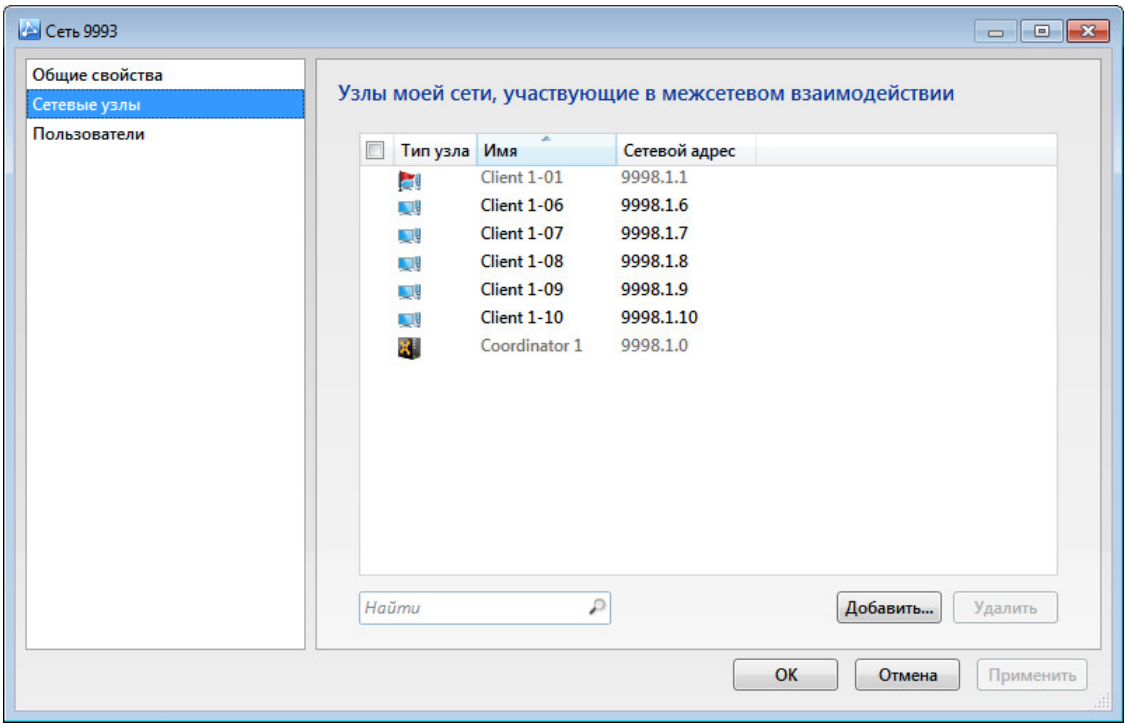

Рисунок 141. Узлы своей сети, участвующие в межсетевом взаимодействии

5 Для просмотра или изменения списка пользователей своей сети, участвующих во взаимодействии с доверенной сетью, на панели навигации выберите раздел **Пользователи**.

- В список могут быть добавлены только пользователи сетевых узлов, участвующих в межсетевом взаимодействии с данной доверенной сетью.

  Чтобы добавить пользователей в список, нажмите кнопку **Добавить** и в открывшемся окне выберите одного или несколько пользователей.

- Чтобы исключить пользователей из межсетевого взаимодействия, выберите их в списке и нажмите кнопку **Удалить**, в окне подтверждения нажмите **Да**.

  При этом связи между удаляемыми пользователями и пользователями доверенной сети будут разорваны. Если удаленный пользователь был единственным пользователем на своем сетевом узле, который участвовал в межсетевом взаимодействии с данной сетью, узел пользователя также будет исключен из межсетевого взаимодействия.

6 Для сохранения настроек нажмите кнопку **OK**.

7 После добавления узлов и пользователей своей сети в список объектов, участвующих в межсетевом взаимодействии, создайте связи с объектами доверенных сетей (см. «Изменение связей с объектами доверенной сети» на стр. 245).

Изменение связей с объектами доверенной сети

Управление связями между объектами своей сети и объектами доверенной сети осуществляется с помощью изменения связей между пользователями этих сетей. При этом создать связи между группами пользователей доверенной сети и пользователями своей сети нельзя.

Чтобы изменить связи пользователя доверенной сети с пользователями вашей сети, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети** (см. рисунок на стр. 57).
2. На панели навигации разверните список объектов нужной доверенной сети и выберите раздел **Пользователи**.
3. На панели просмотра двойным щелчком откройте окно свойств пользователя доверенной сети, связи которого требуется изменить.
4. В открывшемся окне **Свойства пользователя** на панели навигации выберите раздел **Связи с пользователями**.

Примечание. В окне свойств пользователя вашей сети вы можете изменить связи с пользователями доверенных сетей (см. «Изменение связей между пользователями» на стр. 207), а также статусы связей с пользователями доверенных сетей (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).

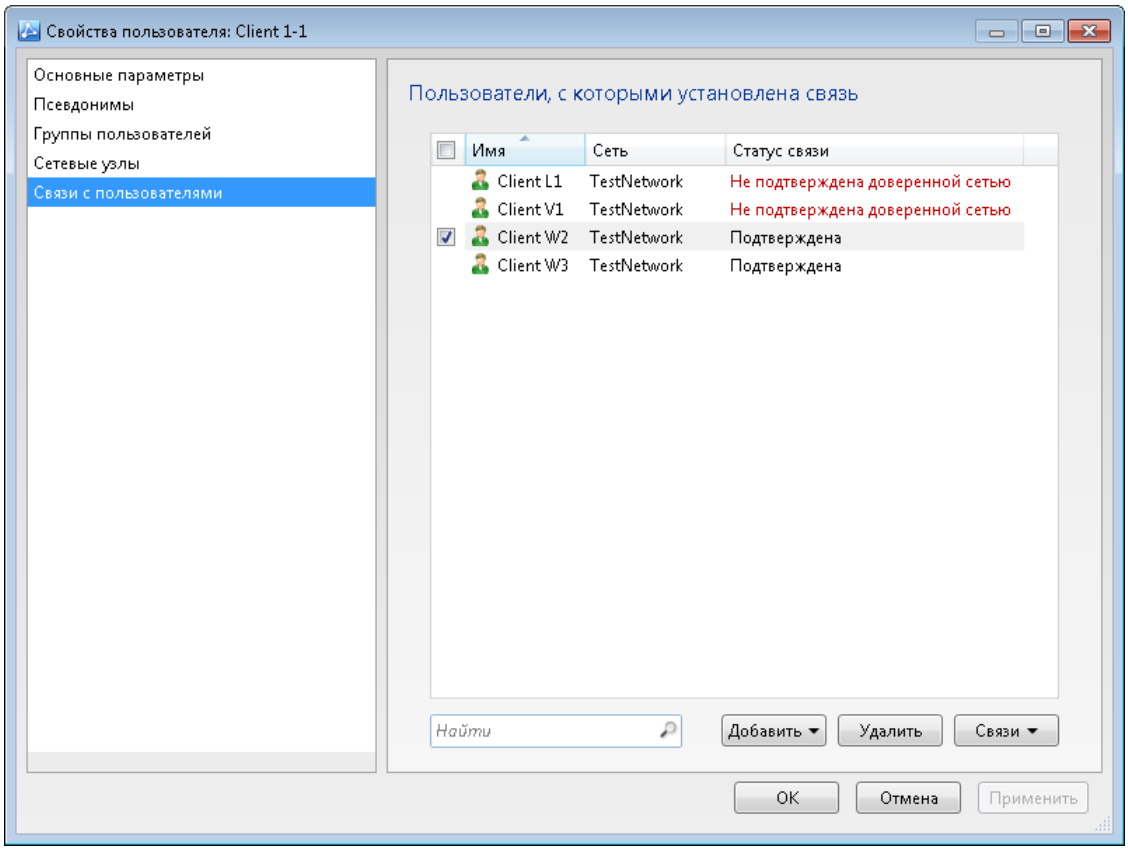

Рисунок 142. Связи пользователя доверенной сети

5 Чтобы создать связи между выбранным пользователем доверенной сети и пользователями своей сети:

- Нажмите кнопку **Добавить** и выполните одно из действий:
  - В меню выберите пункт **Связи с пользователями** и в открывшемся окне укажите пользователей своей сети, связи с которыми вы хотите создать.
  - В меню выберите пункт **Связи по образцу** и в открывшемся окне выберите пользователя той же доверенной сети, связи которого вы хотите скопировать.

При создании связей между пользователем доверенной сети и пользователями вашей сети произойдут следующие изменения:

- Будут созданы связи между сетевыми узлами связанных пользователей.
- Пользователи и сетевые узлы вашей сети, с которыми были созданы связи, будут добавлены в список объектов, участвующих в межсетевом взаимодействии (если они отсутствовали в этом списке).
- Добавленные связи между узлами и пользователями будут иметь статус **Не подтверждена доверенной сетью**.

6 Чтобы удалить связи между выбранным пользователем доверенной сети и пользователями своей сети, выберите нужных пользователей своей сети и нажмите кнопку **Удалить**.

Примечание. Невозможно удалить связи, которые имеют статус **Предложена доверенной сетью** (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).

При удалении связей между пользователем доверенной сети и пользователями вашей сети будут также удалены связи между сетевыми узлами этих пользователей.

7 После изменения связей с пользователями доверенной сети:

- Для узлов вашей сети, связи которых были изменены, создайте и отправьте справочники и ключи (см. «Обновление справочников и ключей» на стр. 87).
- Для доверенной сети, связи объектов которой были изменены, создайте и отправьте межсетевую информацию (см. «Отправка межсетевой информации» на стр. 251).

Изменение статуса связей с объектами доверенных сетей

Связь между объектом (узлом или пользователем) своей сети и объектом доверенной сети может иметь один из следующих статусов:

- **Предложена доверенной сетью** — связь между объектами создана администратором доверенной сети и пока не подтверждена и не запрещена в вашей сети.
- **Не подтверждена доверенной сетью** — связь между объектами создана в вашей сети (см. «Изменение связей с объектами доверенной сети» на стр. 245) и пока не подтверждена и не запрещена администратором доверенной сети.
- **Подтверждена** — связь между объектами подтверждена в вашей сети и в доверенной сети.
- **Запрещена доверенной сетью** — администратор доверенной сети запретил создавать связь между объектами.
- **Запрещена своей сетью** — связь запрещена в вашей сети, администратор доверенной сети не сможет создать связь между объектами.

Чтобы изменить статус связи между пользователем своей сети и пользователем доверенной сети (а также статус связи между сетевыми узлами этих пользователей), выполните следующие действия:

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

2 На панели навигации выберите раздел **Пользователи**.

3 На панели просмотра дважды щелкните запись нужного пользователя.

4 В окне свойств пользователя на панели навигации выберите раздел **Связи с пользователями**.

5 Установите флажок **Доверенных сетей** или нажмите ссылку справа от флажка, чтобы выбрать нужные доверенные сети.

6 В списке выберите связи, статус которых требуется изменить.

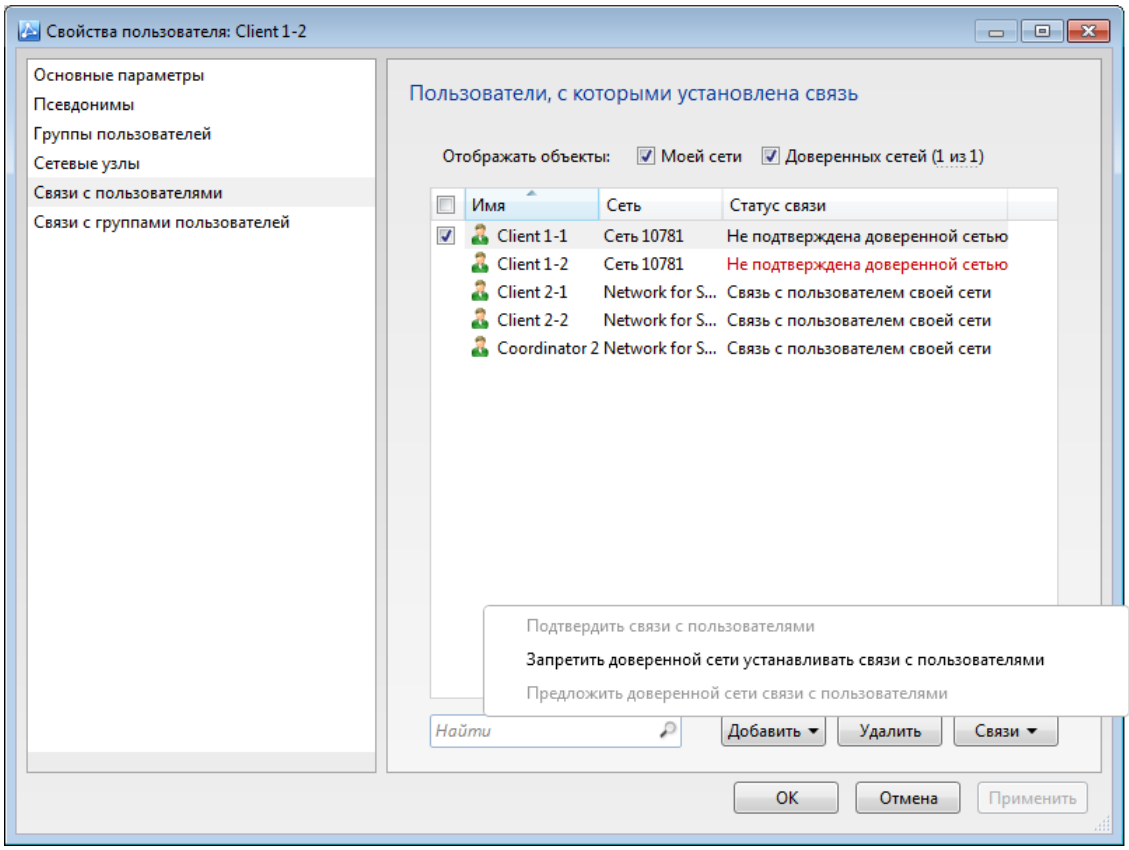

Рисунок 143. Изменение статуса связи с пользователями доверенной сети

7 Нажмите кнопку **Связи** и в меню выберите один из пунктов:

- **Подтвердить связи с пользователями** — чтобы подтвердить связи, предложенные администратором доверенной сети.
- **Запретить доверенной сети устанавливать связи с пользователями** — чтобы запретить администратору доверенной сети устанавливать связи между выбранными пользователями. В окне подтверждения нажмите кнопку **Запретить связи**.
- **Предложить доверенной сети связи с пользователями** — чтобы предложить администратору доверенной сети установить связь между пользователями, которая была ранее запрещена. В окне подтверждения нажмите кнопку **Предложить связи**.

8 После изменения статусов связей для доверенной сети, связи объектов которой были изменены, создайте и отправьте межсетевую информацию (см. «Отправка межсетевой информации» на стр. 251).

Изменение шлюзового координатора своей сети

Чтобы изменить координатор своей сети, который используется в качестве шлюзового для связи с определенной доверенной сетью, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.
2. На панели навигации выберите раздел **Свойства сетей**.
3. На панели просмотра дважды щелкните доверенную сеть, для которой вы хотите изменить шлюзовой координатор.
4. В открывшемся окне с названием доверенной сети на панели навигации выберите раздел **Общие свойства**.
5. В списке **Шлюз моей сети** выберите координатор, который будет использоваться для связи с данной доверенной сетью.

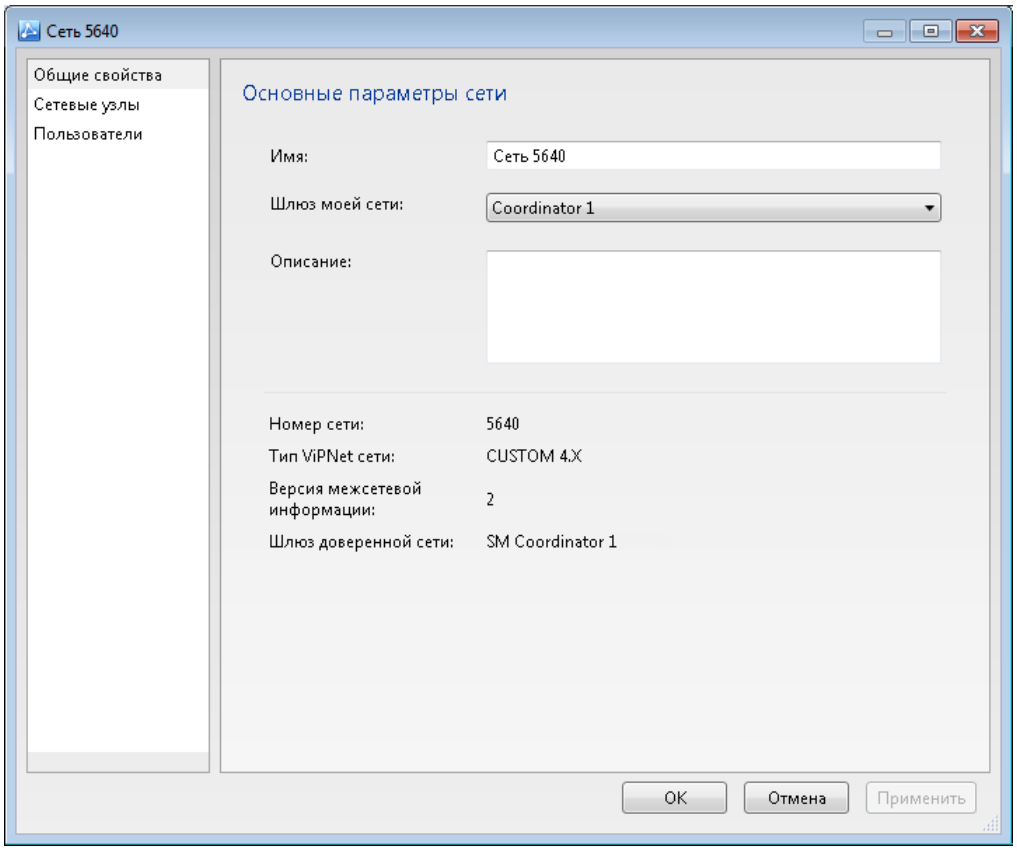

Рисунок 144. Свойства доверенной сети

6. Для сохранения настроек нажмите кнопку **OK**.

7 Для данной доверенной сети создайте и отправьте новую межсетевую информацию (см. «Отправка межсетевой информации» на стр. 251).

8 После того, как межсетевая информация будет доставлена в доверенную сеть, для прежнего шлюзового координатора и нового шлюзового координатора создайте и отправьте новые справочники и ключи (см. «Обновление справочников и ключей» на стр. 87).

Отправка межсетевой информации

При изменении параметров межсетевого взаимодействия с какой-либо доверенной сетью (например, если вы изменили связи между объектами вашей сети и объектами доверенной сети) необходимо создать и отправить новую межсетевую информацию для этой доверенной сети.

Если для какой-либо доверенной сети требуется создать или отправить межсетевую информацию, в программе ViPNet Центр управления сетью будут отображены следующие оповещения:

- Значок представления **Доверенная сеть** примет вид  .
- Рядом с именем доверенной сети на панели навигации появится значок  .
- Если требуется создать межсетевую информацию, в разделе **Свойства сетей** в столбце **Исходящая межсетевая информация** появится статус **Требуется создать**.
- Если требуется отправить межсетевую информацию, в разделе **Свойства сетей** в столбце **Исходящая межсетевая информация** появится статус **Требуется отправить**.

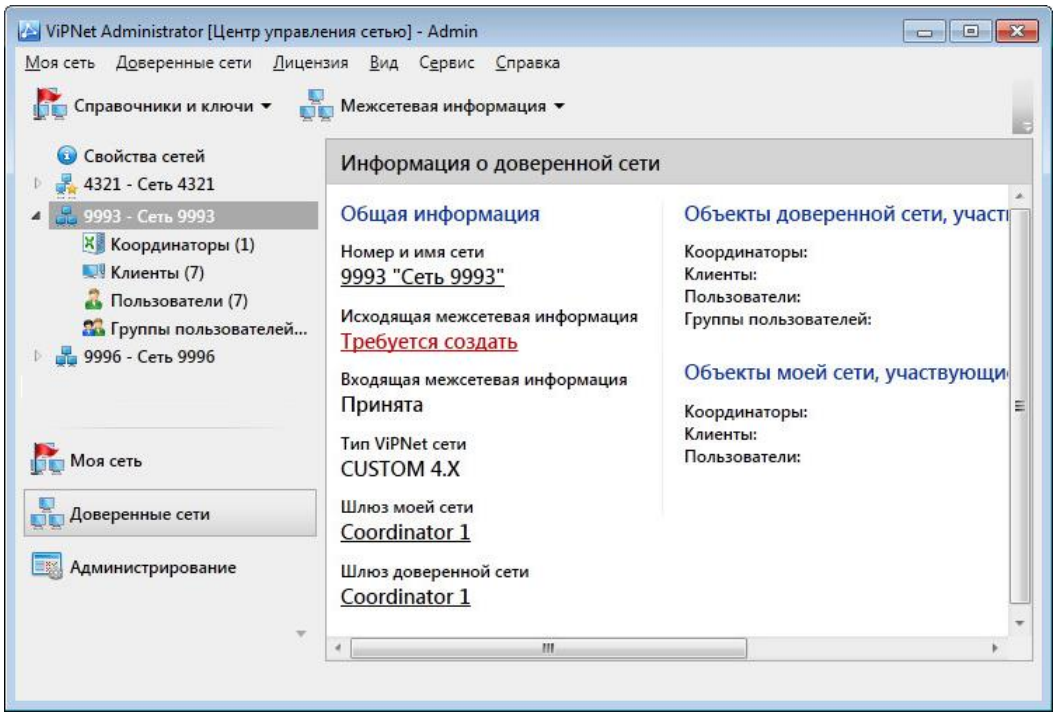

Рисунок 145. Требуется создать межсетевую информацию

Создание межсетевой информации

Чтобы создать межсетевую информацию для доверенной сети, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.
2. На панели навигации выберите раздел **Свойства сетей** (см. рисунок на стр. 57).
3. На панели просмотра щелкните нужную доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Создать межсетевую информацию**, в окне подтверждения нажмите соответствующую кнопку.

   В открывшемся окне будут отображены сведения о ходе процесса.
4. Если создание межсетевой информации завершено с ошибкой, для просмотра отчета о невыполненных операциях нажмите кнопку **Отчет**. В случае успешного создания межсетевой информации для доверенной сети окно со сведениями о ходе процесса закроется автоматически.

Отправка межсетевой информации через сеть ViPNet

Если организация межсетевого взаимодействия (на стр. 233) с доверенной сетью завершена, для отправки межсетевой информации в доверенную сеть вы можете использовать защищенный канал, установленный между вашей и доверенной сетями.

Для отправки межсетевой информации выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.
2. На панели навигации выберите раздел **Свойства сетей** (см. рисунок на стр. 57).
3. На панели просмотра щелкните нужную доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Отправить межсетевую информацию**.
4. В окне подтверждения нажмите кнопку **Отправить информацию**. Откроется окно **Отправка межсетевой информации**, в котором будут отображены сведения о ходе отправки.

Примечание. Отправка межсетевой информации осуществляется с помощью транспортного модуля ViPNet MFTP (см. глоссарий, стр. 308), который является частью программы ViPNet Client. Убедитесь, что на компьютере с серверным приложением ViPNet Центр управления сетью запущена эта программа.

---

5. Если отправка межсетевой информации завершена с ошибками, для просмотра отчета о невыполненных операциях нажмите кнопку **Отчет**. В случае успешной отправки окно **Отправка межсетевой информации** закроется автоматически.

Подробный отчет об отправке межсетевой информации и ее статусе можно просмотреть в журнале транспортных конвертов (см. «Журналы транспортных конвертов» на стр. 102).

Групповая отправка межсетевой информации

Если вы организовали межсетевое взаимодействие сразу с несколькими доверенными сетями, вы можете выполнить групповую отправку межсетевой информации. Для этого:

1 В программе ViPNet Центр управления сетью на панели инструментов нажмите кнопку **Межсетевая информация** и в меню выберите пункт **Отправить межсетевую информацию**.

2 В открывшемся окне будет представлен список доверенных сетей, для которых имеется неотправленная межсетевая информация.

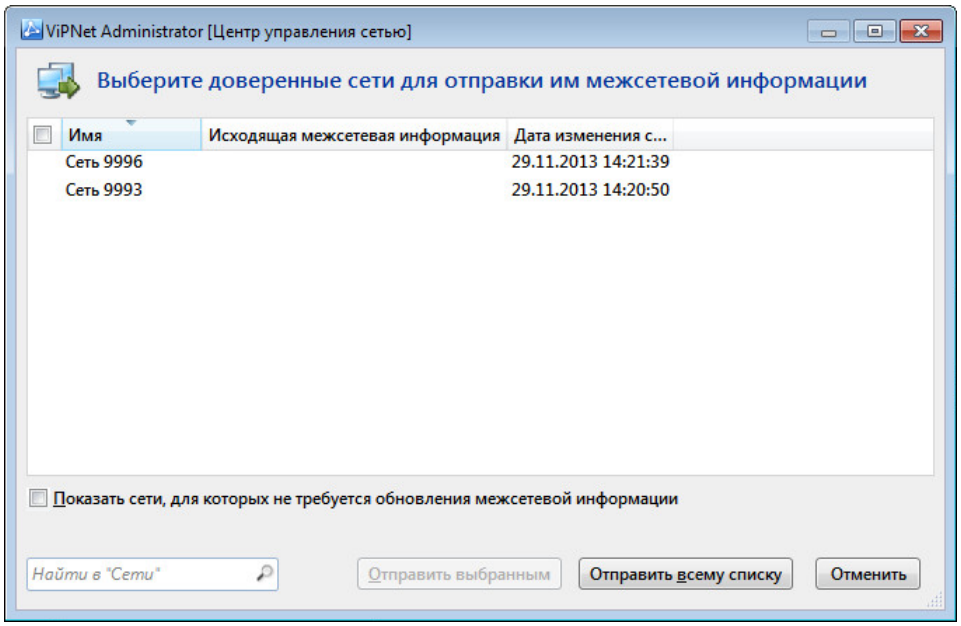

Рисунок 146. Групповая отправка межсетевой информации

При необходимости выберите в списке доверенные сети, в которые требуется отправить межсетевую информацию. Для поиска доверенных сетей в списке введите часть имени сети в строку поиска, расположенную внизу окна.

Если перед отправкой вы хотите просмотреть список сетей, для которых не требуется обновление межсетевой информации, установите соответствующий флажок.

3 Чтобы отправить межсетевую информацию, выполните одно из действий:

- Чтобы отправить межсетевую информацию в выбранные доверенные сети, нажмите кнопку **Отправить выбранным**.
- Чтобы отправить межсетевую информацию во все доверенные сети, отображаемые в списке, нажмите кнопку **Отправить всему списку**.

Передача межсетевой информации в виде файла

Если по какой-либо причине вы не можете отправить межсетевую информацию через сеть ViPNet, передайте информацию в доверенную сеть в виде файла. Для этого выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.
2. На панели навигации выберите раздел **Свойства сетей** (см. рисунок на стр. 57).
3. На панели просмотра щелкните нужную доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить межсетевую информацию в файл**, затем в окне **Сохранить как** укажите папку для сохранения межсетевой информации.
4. Передайте сохраненный файл администратору доверенной сети каким-либо надежным способом.

Прием межсетевой информации

Если администратор одной из доверенных сетей изменит параметры межсетевого взаимодействия с вашей сетью ViPNet, ему потребуется отправить в вашу сеть новую межсетевую информацию. Межсетевая информация может быть передана в вашу сеть по защищенному каналу ViPNet (см. ниже в этом разделе) или в виде файла (см. «Загрузка межсетевой информации из файла» на стр. 259).

Когда транспортный модуль ViPNet MFTP (см. глоссарий, стр. 308) на сетевом узле с серверным приложением ViPNet Центр управления сетью принимает новую межсетевую информацию, в программе ViPNet Центр управления сетью отображаются следующие оповещения:

- Значок представления **Доверенная сеть** принимает вид  .
- Рядом с именем доверенной сети, от которой поступила межсетевая информация, на панели навигации появляется значок  .
- В разделе **Свойства сетей** в столбце **Входящая межсетевая информация** появляется статус **Готова к обработке**.

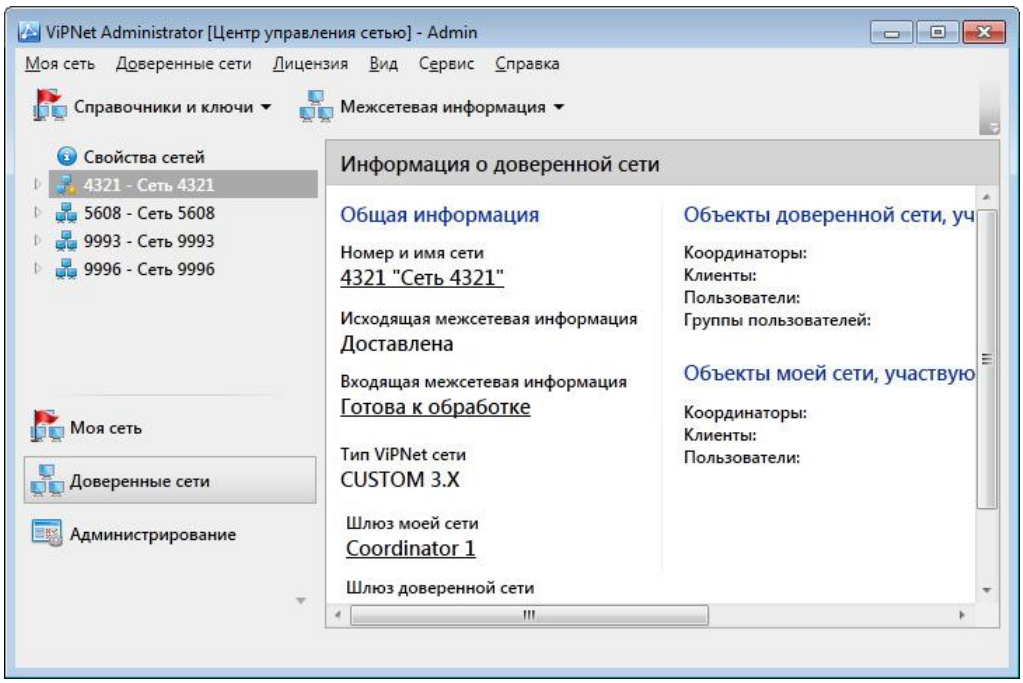

Рисунок 147. Поступила входящая межсетевая информация

Чтобы обработать или отклонить входящую межсетевую информацию, выполните одно из действий:

- Чтобы просмотреть изменения в межсетевой информации для отдельной доверенной сети и принять либо отклонить их, в разделе **Свойства сетей** щелкните нужную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Обработать межсетевую информацию** (см. «Обработка межсетевой информации для отдельной сети» на стр. 256).

- Чтобы выполнить автоматическую обработку межсетевой информации, поступившей из нескольких доверенных сетей, на панели инструментов нажмите кнопку **Межсетевая информация**  и в меню выберите пункт **Обработать межсетевую информацию** (см. «Групповая обработка межсетевой информации» на стр. 257).
- Чтобы немедленно отклонить поступившую межсетевую информацию, в разделе Свойства сетей щелкните нужную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Отклонить межсетевую информацию**.

Обработка межсетевой информации для отдельной сети

Чтобы обработать межсетевую информацию для отдельной доверенной сети, выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.
2. На панели навигации выберите раздел **Свойства сетей**.
3. На панели просмотра щелкните нужную доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Обработать межсетевую информацию**. Будет запущен мастер **Обработка межсетевой информации**.
4. На первой странице мастера выполните следующие действия:
   - Чтобы подтвердить все связи, предложенные администратором доверенной сети, установите соответствующий флажок. В этом случае всем предложенным связям будет присвоен статус **Подтверждена**.

     Если вы не установите флажок **Подтвердить все связи, предложенные доверенной сетью**, вам потребуется изменить статус связей для каждого пользователя (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).
   - Для продолжения нажмите кнопку **Далее**.
5. Если межсетевая информация содержит ошибки, откроется страница **Проверка межсетевой информации** (см. рисунок на стр. 238) со списком обнаруженных конфликтных или неполных данных.

   При обнаружении конфликтных данных загрузка межсетевой информации будет невозможна. В этом случае обратитесь к администратору доверенной сети для устранения конфликтов.

   Чтобы продолжить обработку межсетевой информации, нажмите кнопку **Далее**.
6. На странице **Изменения в межсетевой информации** просмотрите список изменений, внесенных администратором доверенной сети:
   - Чтобы отклонить предложенные администратором другой сети изменения, нажмите кнопку **Отклонить изменения**. В этом случае обработка межсетевой информации будет прекращена.

- Чтобы принять изменения и продолжить обработку межсетевой информации, нажмите кнопку **Далее**.

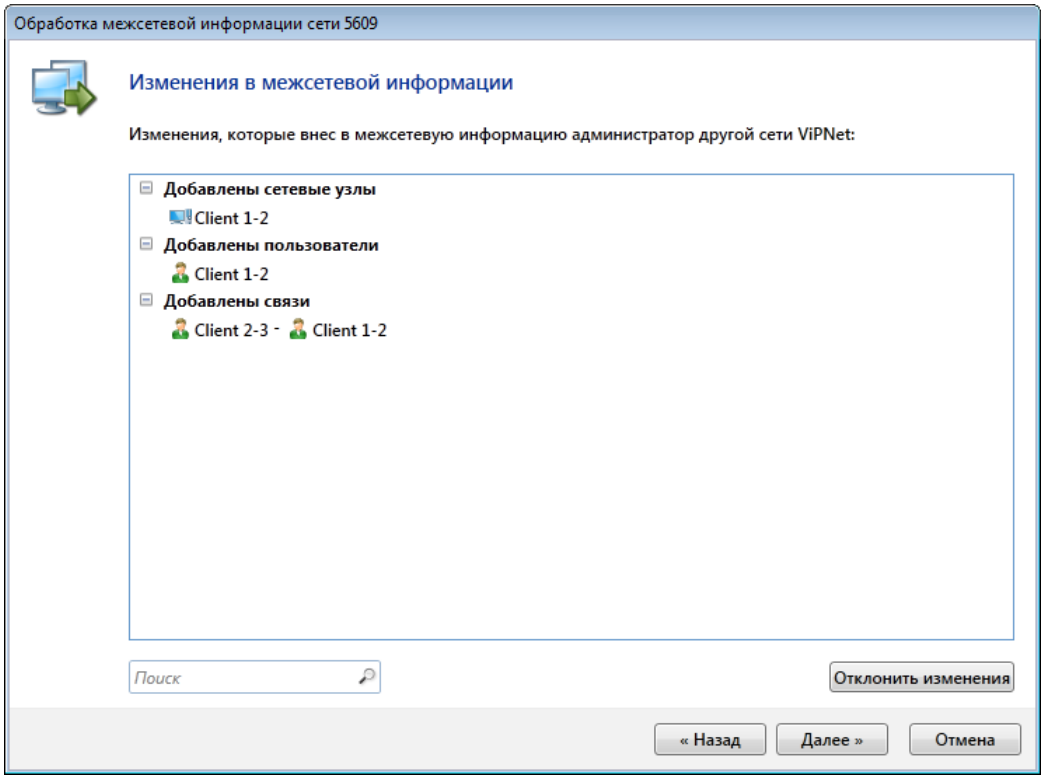

Рисунок 148. Список изменений в межсетевой информации

7 После успешной обработки межсетевой информации на странице **Загрузка межсетевой информации** нажмите кнопку **Готово**.

8 В случае необходимости создайте новые справочники и ключи и отправьте их на узлы своей сети (см. «Обновление справочников и ключей» на стр. 87).

Групповая обработка межсетевой информации

Для автоматической обработки межсетевой информации, поступившей из нескольких доверенных сетей, вы можете использовать окно групповой обработки или контекстное меню в списке доверенных сетей.

Чтобы выполнить групповую обработку межсетевой информации с возможностью предварительного просмотра списка сетей, для которых имеется необработанная межсетевая информация, выполните следующие действия:

1 В программе ViPNet Центр управления сетью на панели инструментов нажмите кнопку **Межсетевая информация** и в меню выберите пункт **Обработать межсетевую информацию**.

2 В открывшемся окне будет представлен список доверенных сетей, для которых имеется необработанная межсетевая информация.

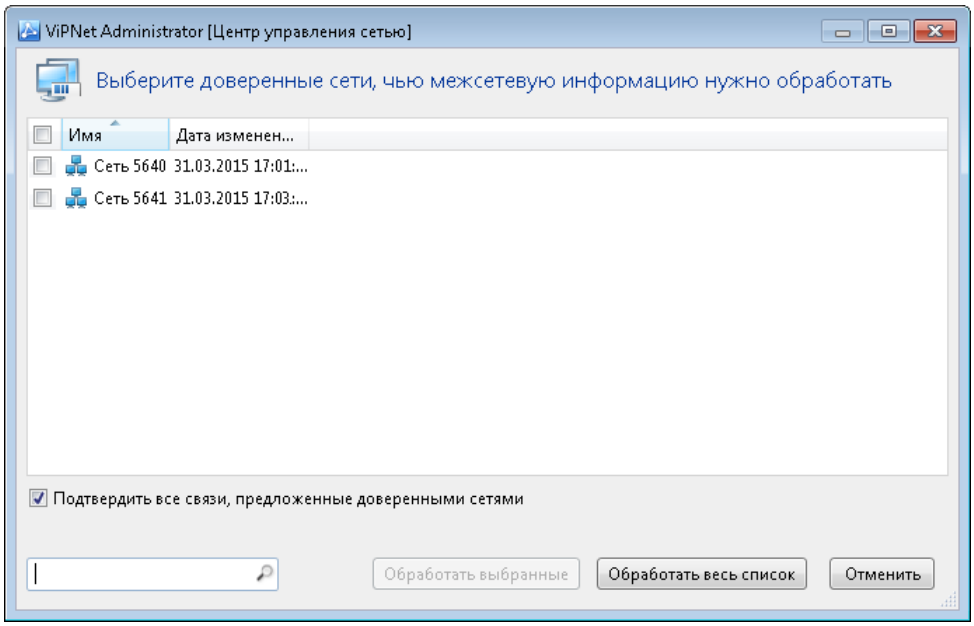

Рисунок 149. Групповая обработка межсетевой информации

При необходимости выберите в списке доверенные сети, для которых требуется обработать межсетевую информацию. Для поиска доверенных сетей в списке введите часть имени сети в строку поиска, расположенную внизу окна.

3 Чтобы подтвердить все связи, предложенные администраторами доверенных сетей, установите соответствующий флажок. В этом случае всем предложенным связям будет присвоен статус **Подтверждена**.

Если вы не установите флажок **Подтвердить все связи, предложенные доверенными сетями**, вам потребуется изменить статус связей для каждого пользователя (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).

4 Чтобы начать обработку межсетевой информации, выполните одно из действий:

- Чтобы обработать межсетевую информацию для выбранных доверенных сетей, нажмите кнопку **Обработать выбранные**.
- Чтобы обработать межсетевую информацию для всех доверенных сетей, отображаемых в списке, нажмите кнопку **Создать для всего списка**.

Откроется окно **Межсетевая информация** с индикатором выполнения операции.

5 Когда обработка межсетевой информации будет завершена, для просмотра отчета о выполненных операциях нажмите кнопку **Отчет**. Чтобы закрыть окно **Межсетевая информация**, нажмите соответствующую кнопку.

Чтобы запустить автоматическую обработку межсетевой информации с помощью контекстного меню, выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.

2 На панели навигации выберите раздел **Свойства сетей**.

3 На панели просмотра выберите одну или несколько доверенных сетей, щелкните выбранные сети правой кнопкой мыши и в контекстном меню выберите пункт **Автоматическая обработка межсетевой информации**.

4 В открывшемся окне выполните следующие действия:

- Чтобы подтвердить все связи, предложенные администраторами доверенных сетей, установите соответствующий флажок. В этом случае всем предложенным связям будет присвоен статус **Подтверждена**.
- Чтобы начать обработку межсетевой информации, нажмите кнопку **Обработать**. Откроется окно **Межсетевая информация** с индикатором выполнения операции.

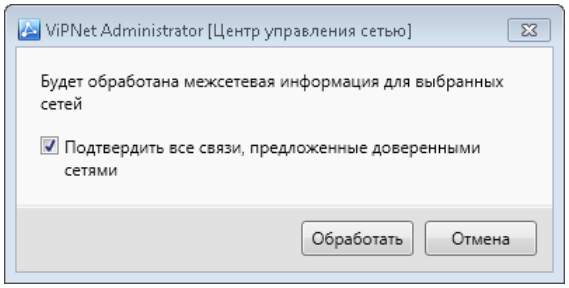

Рисунок 150. Автоматическая обработка межсетевой информации

5 Когда обработка межсетевой информации будет завершена, для просмотра отчета о выполненных операциях нажмите кнопку **Отчет**. Чтобы закрыть окно **Межсетевая информация**, нажмите соответствующую кнопку.

Загрузка межсетевой информации из файла

Если по какой-либо причине невозможно отправить межсетевую информацию из доверенной сети в вашу сеть по защищенному каналу ViPNet, администратор доверенной сети может передать межсетевую информацию в виде файла.

Чтобы загрузить межсетевую информацию из файла, выполните следующие действия:

1 В окне программы ViPNet Центр управления сетью в меню **Доверенные сети** выберите пункт **Загрузить межсетевую информацию из файла**.

2 В окне **Загрузка межсетевой информации** нажмите кнопку **Обзор** и укажите файл межсетевой информации, полученный от администратора доверенной сети.

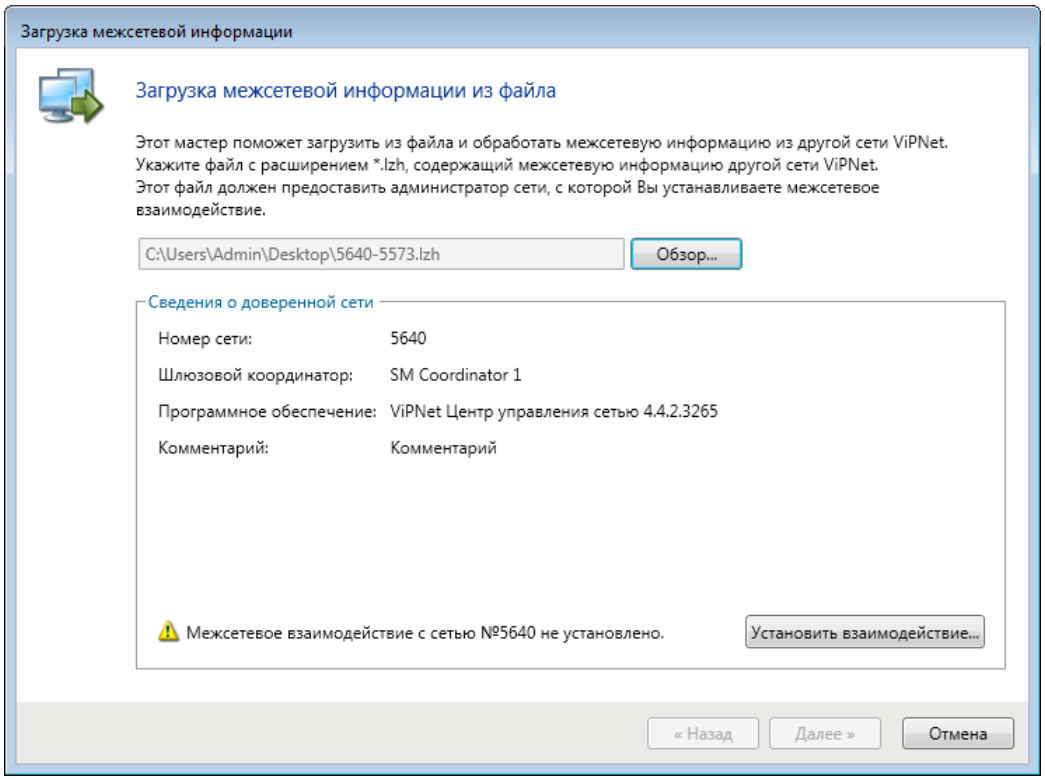

Рисунок 151. Загрузка межсетевой информации из файла

3 Чтобы подтвердить все связи, предложенные доверенной сетью, установите соответствующий флажок. В этом случае всем предложенным связям будет присвоен статус **Подтверждена**.

Если вы не установите флажок **Подтвердить все связи, предложенные доверенной сетью**, вам потребуется изменить статус связей для каждого пользователя (см. «Изменение статуса связей с объектами доверенных сетей» на стр. 247).

4 Для продолжения нажмите кнопку **Далее**. Будет запущен мастер **Загрузка межсетевой информации**.

5 Выполните обработку межсетевой информации с помощью мастера (см. «Обработка межсетевой информации для отдельной сети» на стр. 256).

6 В случае необходимости создайте новые справочники и ключи и отправьте их на узлы своей сети (см. «Обновление справочников и ключей» на стр. 87).

Прекращение межсетевого взаимодействия

Если больше нет необходимости во взаимодействии с какой-либо доверенной сетью, вы можете прекратить межсетевое взаимодействие. Для этого выполните следующие действия:

1. В окне программы ViPNet Центр управления сетью выберите представление **Доверенные сети**.
2. На панели навигации выберите раздел **Свойства сетей** (см. рисунок на стр. 57).
3. На панели просмотра щелкните правой кнопкой мыши доверенную сеть, межсетевое взаимодействие с которой требуется прекратить, и в контекстном меню выберите пункт **Прекратить взаимодействие**.
4. В окне подтверждения установите флажок **Прекратить взаимодействие**, затем нажмите кнопку **Прекратить взаимодействие**.

   В открывшемся окне **Прекращение взаимодействия с выбранными сетями** будет отображен процесс удаления данных об объектах доверенной сети и их связях с объектами вашей сети. Также информация о доверенной сети будет удалена в программе ViPNet Удостоверяющий и ключевой центр.
5. Если удаление данных о доверенной сети завершено с ошибкой, для просмотра отчета о невыполненных операциях нажмите кнопку **Отчет**. В случае успешного удаления данных о доверенной сети окно **Прекращение межсетевого взаимодействия** закроется автоматически.

A

Возможные неполадки и способы их устранения

Не удается установить соединение с сервером ViPNet Центр управления сетью

Если не удается установить соединение с сервером ViPNet Центр управления сетью, это может быть вызвано следующими причинами:

- На компьютере с серверным приложением ViPNet Центр управления сетью не запущены службы `NccService` и `NccFilewatcherService`.

  Для решения проблемы запустите указанные службы (см. «Запуск и завершение работы программы ViPNet Центр управления сетью» на стр. 49).

- Серверное приложение ViPNet Центр управления сетью установлено на удаленном компьютере, и в клиентском приложении неверно указан IP-адрес или DNS-имя этого компьютера.

  Для решения проблемы в окне сообщения о неудачной попытке соединения с сервером укажите верный IP-адрес или DNS-имя сервера (см. «Запуск и завершение работы программы ViPNet Центр управления сетью» на стр. 49).

- Серверное приложение ViPNet Центр управления сетью установлено на удаленном компьютере, и закрыты порты 9000, 9100, 9200, 9300, 9400, 9500, 9600, 9700, которые используются для подключения клиентского приложения к серверному приложению по протоколу TCP.

  Для решения проблемы убедитесь, что указанные порты открыты.

- Серверное приложение ViPNet Центр управления сетью установлено на удаленном защищенном узле (см. глоссарий, стр. 302). В то же время компьютер с клиентским приложением является открытым узлом (см. глоссарий, стр. 305) или защищенным узлом, который не имеет связи с узлом серверного приложения.

  Для решения проблемы рекомендуется установить клиентское приложение ViPNet Центр управления сетью на защищенном узле, связанном с узлом, на котором находится сервер.

- Серверное и клиентское приложения ViPNet Центр управления сетью установлены на двух разных компьютерах, на которых отличаются настройки даты и времени.

  Для решения проблемы на компьютере с серверным приложением и на компьютере с клиентским приложением ViPNet Центр управления сетью рекомендуется сделать одинаковые настройки даты, времени и часового пояса.

Не удается установить соединение с SQL-сервером

Если не удается подключиться к SQL-серверу, это может быть вызвано тем, что на компьютере, на котором установлено серверное приложение ЦУСа, было установлено какое-либо обновление Windows.

Для решения проблемы выполните одно из действий:

- Восстановите или обновите установленные компоненты программы ViPNet CSP.
- Внесите изменения в системный реестр Windows. Для этого:
  - В меню **Пуск** выберите пункт **Выполнить**.
  - В окне **Выполнить** в поле **Открыть** введите `regedit` и нажмите кнопку **OK**. Откроется окно **Редактор реестра**.

    

    Внимание! Неправильное редактирование реестра может привести к возникновению неполадок в работе операционной системы, поэтому обязательно создайте резервную копию реестра. Это позволит восстановить реестр при возникновении неполадок.

  - В разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\Default\00010002` щелкните **Functions** и в окне **Редактирование мультистроки** перенесите строки, содержащие «GOST» в конец списка, не изменяя порядок и состав остальных строк. Затем нажмите **OK**.
  - В разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002` щелкните **Functions** и в окне **Редактирование мультистроки** перенесите строки, содержащие «GOST» в конец списка, не изменяя порядок и состав остальных строк. Затем нажмите **OK**.

- Выполните перезагрузку компьютера.

Ошибка при вводе имени администратора и пароля

Если при входе в клиентское приложение ViPNet Центр управления сетью вы ввели правильное имя пользователя и пароль, но в результате появилось сообщение о вводе неверных данных пользователя, это может быть вызвано сбоем серверного приложения.

Для решения проблемы остановите службу `NccService`, затем снова запустите ее.

Некорректная обработка межсетевой информации

Если при обработке межсетевой информации из определенной доверенной сети возникают ошибки, например, неверно отображаются изменения параметров межсетевого взаимодействия, выполните следующие действия:

1. Удалите данные о межсетевой информации, загруженной для этой доверенной сети ранее. Для этого:
   - В разделе **Свойства сетей** (см. «Представление „Доверенные сети“» на стр. 56) щелкните доверенную сеть правой кнопкой мыши и в контекстном меню выберите пункт **Очистить кэш межсетевой информации**.
   - В окне подтверждения нажмите кнопку **Да**.
2. Снова обработайте поступившую межсетевую информацию. В результате все параметры межсетевого взаимодействия с доверенной сетью будут определены на основе последней версии межсетевой информации.

Ошибки при загрузке структуры сети из программы ViPNet Центр управления сетью версии 3.x

Если при загрузке структуры сети, созданной в программе ViPNet Центр управления сетью версии 3.x, возникли ошибки, ознакомьтесь с документом «ViPNet Administrator. Руководство по обновлению с версии 3.x на версию 4.0». Рекомендации по устранению ошибок приведены в разделе «Возможные проблемы при миграции» этого документа.

Истекает срок действия лицензии на сеть ViPNet

Если при запуске клиентского приложения ViPNet Центр управления сетью появляется предупреждение об окончании срока действия лицензии на сеть ViPNet, выполните следующие действия:

1. Обратитесь к представителю ОАО «ИнфоТеКС» для продления срока действия лицензии.
2. Получите новый файл лицензии и загрузите его в программу ViPNet Центр управления сетью (см. «Обновление лицензии» на стр. 108).

Превышено максимальное число узлов, на которые добавлена роль

После обновления лицензии на сеть ViPNet (см. «Обновление лицензии» на стр. 108) может возникнуть ситуация, когда новая лицензия позволяет создать меньшее количество узлов с определенной ролью, чем в старая. Также возможно изменение формата лицензии, в результате чего поддержка определенных ролей может быть прекращена.

В этом случае при создании справочников появится сообщение: «Превышено максимальное число узлов, на которые добавлена роль <имя роли>».

Чтобы решить проблему, выполните следующие действия:

1. В программе ViPNet Центр управления сетью в представлении **Моя сеть** выберите раздел **Роли**.
2. На панели просмотра найдите роль, для которой были превышены лицензионные ограничения, и откройте окно свойств роли.
3. Из списка узлов, на которые добавлена роль, удалите необходимое число узлов, чтобы устранить превышение лицензионных ограничений.

Ошибки при сохранении отчета о структуре сети

Если вы сохраняете отчет о структуре сети ViPNet с количеством сетевых узлов больше 1000 в файл с расширением `*.html`, отчет о структуре сети может быть сохранен некорректно. В этом случае рекомендуется сохранять структуру сети в файл с расширением `*.xml`.

B

Роли сетевых узлов

В следующей таблице перечислены роли сетевых узлов, которые могут быть добавлены на сетевые узлы при наличии разрешений в лицензии на сеть ViPNet. Для каждой роли приведены описание и информация о совместимости с другими ролями.

Таблица 9. Возможные роли сетевых узлов

Идентификатор	Название роли	Описание	Ограничения
0000	Business Mail	Позволяет использовать на клиенте программу ViPNet Деловая почта. При добавлении данной роли можно задать уровень полномочий пользователя в программе ViPNet Деловая почта.	Может быть добавлена только на клиент.
0004	Network Control Center	Позволяет установить на клиенте серверное приложение ViPNet Центр управления сетью.	Автоматически добавляется на первый клиент сети ViPNet и не может быть добавлена на другие клиенты.
0005	Dispatcher	Позволяет использовать на клиенте программу ViPNet Dispatcher.	Может быть добавлена только на клиент.
000C	Policy Manager	Позволяет использовать на клиенте программу ViPNet Policy Manager для централизованного управления политиками безопасности сетевых узлов. При добавлении данной роли вы можете задать список контролируемых узлов.	Автоматически добавляется на клиент с ролью «Network Control Center».

Идентификатор	Название роли	Описание	Ограничения
0017	VPN-клиент	Позволяет использовать на клиенте программное обеспечение ViPNet Client для работы в защищенной сети ViPNet. При добавлении данной роли вы можете задать уровень полномочий пользователя в программе ViPNet Монитор.	Может быть добавлена только на клиент.
0018	Программный VPN-координатор	Позволяет использовать на координаторе программное обеспечение ViPNet Coordinator для Windows или Linux для работы в качестве сервера защищенной сети ViPNet. При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Несовместима с ролями, предназначенными для программно-аппаратных комплексов: • ViPNet Coordinator HW; • ViPNet Coordinator KB; • ViPNet Coordinator IG.
001D	Registration Point	Позволяет использовать на клиенте программу ViPNet Registration Point для регистрации пользователей ViPNet. При добавлении данной роли можно ограничить число создаваемых в программе запросов на сертификаты и дистрибутивы для пользователей.	Может быть добавлена только на клиент.
001E	SafeDisk	Позволяет использовать на сетевом узле программу ViPNet SafeDisk-V.	Может быть добавлена на клиент или координатор.
0020	CryptoService	Позволяет использовать на сетевом узле программу ViPNet CryptoService. При добавлении данной роли можно задать уровень полномочий пользователя в программе ViPNet CryptoService.	Может быть добавлена на клиент или координатор.
0025	Failover	Позволяет развернуть кластер горячего резервирования на базе координатора с программным обеспечением ViPNet Coordinator for Linux или программно-аппаратного комплекса ViPNet Coordinator HW.	Может быть добавлена только на координатор с ролью «Программный VPN-координатор», «Coordinator HW-VA», «Coordinator HW-VPNM», «Coordinator HW-MCM» .
0029	SDK	Позволяет встраивать криптографические функции ViPNet во внешние приложения.	Может быть добавлена на клиент или координатор.

Идентификатор	Название роли	Описание	Ограничения
002C	Web Gate	Позволяет использовать координатор с программным обеспечением ViPNet Coordinator for Linux в качестве веб-шлюза. При добавлении данной роли можно задать число адресов для шлюза.	Может быть добавлена только на координатор.
002D	Coordinator KB1000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator KB1000.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер». При этом для ViPNet CSP должна быть установлена самая последняя версия программного обеспечения.
0032	Cluster Windows	Позволяет использовать на координаторе программное обеспечение ViPNet Cluster для объединения нескольких компьютеров в отказоустойчивый кластер.	Может быть добавлена только на координатор с ролью «Программный VPN-координатор».
0038	Publication Service	Позволяет использовать на клиенте программу ViPNet Publication Service для публикации сертификатов.	Может быть добавлена только на клиент.
003B	Клиент SGA	Позволяет использовать на клиенте апплет ViPNet SGA для удаленного мониторинга и управления координатором под управлением операционной системы Linux.	Может быть добавлена только на клиент.
003C	Сервер TLS	Позволяет использовать сетевой узел в качестве сервера для соединений по протоколу TLS.	Может быть добавлена на клиент или координатор.
003E	Интеграция с СОЗ	Позволяет экспортировать на сетевом узле данные в Систему оценки защищенности производства (СОЗ ЦБИ).	Может быть добавлена на клиент или координатор.

Идентификатор	Название роли	Описание	Ограничения
0040	Coordinator HW100 A	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW100. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер». Координатор с данной ролью не может выполнять функцию транспортного сервера. Имеет ограничение на количество туннелируемых соединений — 2.
0041	Coordinator HW100 B	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW100. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер». Имеет ограничение на количество туннелируемых соединений — 5.
0042	Coordinator HW100 C	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW100. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер». Имеет ограничение на количество туннелируемых соединений — 10.

Идентификатор	Название роли	Описание	Ограничения
0044	Coordinator HW1000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW1000. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер».
0045	Coordinator HW2000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW2000. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «Failover2000», «DNS-Сервер» и «WINS-Сервер».
0047	StateWatcher	Позволяет развернуть на клиенте сервер системы мониторинга ViPNet StateWatcher. При добавлении данной роли можно задать число узлов мониторинга и дочерних серверов.	Может быть добавлена только на клиент.
0048	CryptoService Linux	Позволяет использовать криптографические функции ViPNet на узлах с операционной системой Linux.	Может быть добавлена на клиент или координатор.
0049	Terminal	Позволяет использовать на клиенте программное обеспечение ViPNet Terminal.	Может быть добавлена только на клиент. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер».
004B	Coordinator HW-VPNM	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW-VPNM. При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «Failover», «DNS-Сервер» и «WINS-Сервер».

Идентификатор	Название роли	Описание	Ограничения
004C	Coordinator HW100 CU	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW100.	Может быть добавлена только на координатор. Совместима только с ролями «Failover100», «DNS-Сервер» и «WINS-Сервер».
004D	Coordinator HW100 AU	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW100.	Может быть добавлена только на координатор. Совместима только с ролями «Failover100», «DNS-Сервер» и «WINS-Сервер».
004F	VPN Client для мобильных устройств	Позволяет использовать на мобильных устройствах программное обеспечение ViPNet Client для операционных систем Android, iOS и macOS. При добавлении данной роли можно задать уровень полномочий пользователя в приложении ViPNet Client для указанных операционных систем.	Может быть добавлена только на клиент. Несовместима с ролями «DNS-Сервер» и «WINS-Сервер».
0054	Coordinator KB100	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator KB100.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер». При этом для ViPNet CSP должна быть установлена самая последняя версия программного обеспечения.
0055	Coordinator HW-VA	Позволяет развернуть координатор на виртуальной машине с помощью программного обеспечения ViPNet Coordinator HW-VA. При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «Failover», «DNS-Сервер» и «WINS-Сервер». Количество туннелируемых соединений определяется лицензией.
0058	Coordinator HW-MCM	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW-MCM. При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «Failover», «DNS-Сервер» и «WINS-Сервер».

Идентификатор	Название роли	Описание	Ограничения
0059	Обмен сообщениями и файлами	Позволяет использовать на узле встроенные в ПО ViPNet средства коммуникации — обмен защищенными сообщениями и файловый обмен.	Может быть добавлена на неограниченное количество клиентов или координаторов с ролью «VPN-клиент» или «Программный VPN-координатор».
005A	DNS-Сервер	Эту роль следует добавлять на сетевые узлы, которые являются DNS-серверами или туннелируют DNS-серверы.	Может быть добавлена на неограниченное количество клиентов или координаторов.
005B	WINS-Сервер	Эту роль следует добавлять на сетевые узлы, которые являются WINS-серверами или туннелируют WINS-серверы.	Может быть добавлена на неограниченное количество клиентов или координаторов.
0065	Connect	Позволяет использовать на клиенте программу ViPNet Connect.	Может быть добавлена только на клиент с ролью «VPN-клиент» или «VPN Client для мобильных устройств».
006E	Coordinator HW1000 C	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW1000. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер», «WINS-сервер».
006F	Coordinator HW1000 D	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW1000. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер», «WINS-сервер».

Иденти-фикатор	Название роли	Описание	Ограничения
0070	Coordinator HW5000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW5000. Информация о поддерживаемых исполнениях приведена в документе «ViPNet Coordinator HW. Общее описание». При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер», «WINS-сервер».
0071	Coordinator IG10	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG10. При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 5. Не поддерживает выбор типа межсетевого экрана (ФСТЭК).
0074	Coordinator KB2000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator KB2000.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер». При этом для ViPNet CSP должна быть установлена самая последняя версия программного обеспечения.
0075	StateWatcher SHW1000	Позволяет развернуть сервер системы мониторинга на базе программно-аппаратного комплекса ViPNet StateWatcher SHW1000. При добавлении данной роли можно задать число узлов мониторинга и дочерних серверов.	Может быть добавлена только на клиент.

Идентификатор	Название роли	Описание	Ограничения
0076	StateWatcher SHW2000	Позволяет развернуть сервер системы мониторинга на базе программно-аппаратного комплекса ViPNet StateWatcher SHW2000. При добавлении данной роли можно задать число узлов мониторинга и дочерних серверов.	Может быть добавлена только на клиент.
0077	StateWatcher VA	Позволяет развернуть сервер системы мониторинга на базе виртуального устройства ViPNet StateWatcher VA. При добавлении данной роли можно задать число узлов мониторинга и дочерних серверов.	Может быть добавлена только на клиент.
0078	Coordinator HW50 AU	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator HW50. При добавлении данной роли можно назначить координатор защищенным интернет-шлюзом (см. «Функции координатора в защищенной сети ViPNet» на стр. 33).	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер».
0081	ConServer	Позволяет установить серверное ПО ViPNet Connect для организации групповых чатов.	Может быть добавлена только на клиент.
0082	CPNs	Customer Push Notification Server (CPNs) позволяет развернуть серверное ПО для рассылки push-уведомлений на устройства с клиентским ПО ViPNet Connect.	Может быть добавлена только на клиент.
0083	xF100	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet xFirewall 100.	Может быть добавлена на координатор без функций VPN-сервера. Совместима только с ролью «DNS-Сервер».
0084	xF1000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet xFirewall 1000.	Может быть добавлена на координатор без функций VPN-сервера. Совместима только с ролью «DNS-Сервер».
0085	xF2000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet xFirewall 2000.	Может быть добавлена на координатор без функций VPN-сервера. Совместима только с ролью «DNS-Сервер».

Идентификатор	Название роли	Описание	Ограничения
0086	xF5000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet xFirewall 5000.	Может быть добавлена на координатор без функций VPN-сервера. Совместима только с ролью «DNS-Сервер».
0088	Coordinator IG10 A0	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG10 A0.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 5.
0089	Coordinator IG10 B0	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG10 B0.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 65535.
008A	Coordinator IG10 A1	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG10 A1.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 5.
008B	Coordinator IG10 B1	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG10 B1.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 65535.

Идентификатор	Название роли	Описание	Ограничения
008C	Coordinator IG100 A0	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG100 A0.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 5.
008D	Coordinator IG100 B0	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG100 B0.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 65535.
008E	Coordinator IG100 A1	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG100 A1.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 5.
008F	Coordinator IG100 B1	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator IG100 B1.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-сервер» и «WINS-сервер». Имеет ограничение на количество туннелируемых соединений — 65535.
0090	xF-VA	Позволяет развернуть координатор на базе сетевого узла с ПО ViPNet xFirewall-VA.	Может быть добавлена на координатор без функций VPN-сервера. Совместима только с ролью «DNS-Сервер».
0091	Client for Linux	Позволяет использовать на клиенте ПО ViPNet Client for Linux, предназначенное для установки на компьютеры с ОС Linux.	Может быть добавлена только на клиент. Для корректной работы ViPNet Client for Linux также необходимо добавить роль «VPN-клиент».

Иденти-фикатор	Название роли	Описание	Ограничения
0093	Coordinator KB5000	Позволяет развернуть координатор на базе программно-аппаратного комплекса ViPNet Coordinator KB5000.	Может быть добавлена только на координатор. Совместима только с ролями «DNS-Сервер» и «WINS-Сервер». При этом для ViPNet CSP должна быть установлена самая последняя версия программного обеспечения.

C

История версий

Что нового в версии 4.6.3

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью по сравнению с версией 4.6.2.

- **Добавление координатора без функций сервера IP-адресов и транспортного сервера**

  Теперь для уменьшения нагрузки на вычислительные ресурсы координатора вы можете использовать координатор с отключенными функциями сервера IP-адресов и транспортного сервера. Такой координатор не рассылает информацию о других узлах, его необходимо регистрировать на другом координаторе и на него нельзя добавить клиенты. Вы можете использовать его для туннелирования и в качестве межсетевого экрана. Новый координатор называется координатором без функций VPN-сервера и отображается значком  в списке координаторов.

- **Управление доменными зонами, обслуживаемыми выделенными защищенными DNS-серверами**

  Мобильные клиенты ViPNet и другие узлы могут одновременно использовать публичные и корпоративные DNS-серверы. При нахождении пользователя в публичной сети DNS-запрос о разрешении доменного имени корпоративного ресурса мог быть отправлен на незащищенные публичные DNS-серверы, создавая возможность атак, направленных на подмену запрашиваемых ресурсов. Теперь, чтобы запросы корпоративных ресурсов отправлялись только на защищенные DNS-серверы, вы можете настроить доменные зоны, которые будут обслуживаться только выделенными защищенными DNS-серверами. В этом случае запросы корпоративных ресурсов, отправленные на публичные DNS-серверы, будут блокироваться. Чтобы создать список защищенных DNS-серверов и доменных зон, в представлении **Моя Сеть** выберите новый раздел **DNS-серверы и DNS-зоны**.

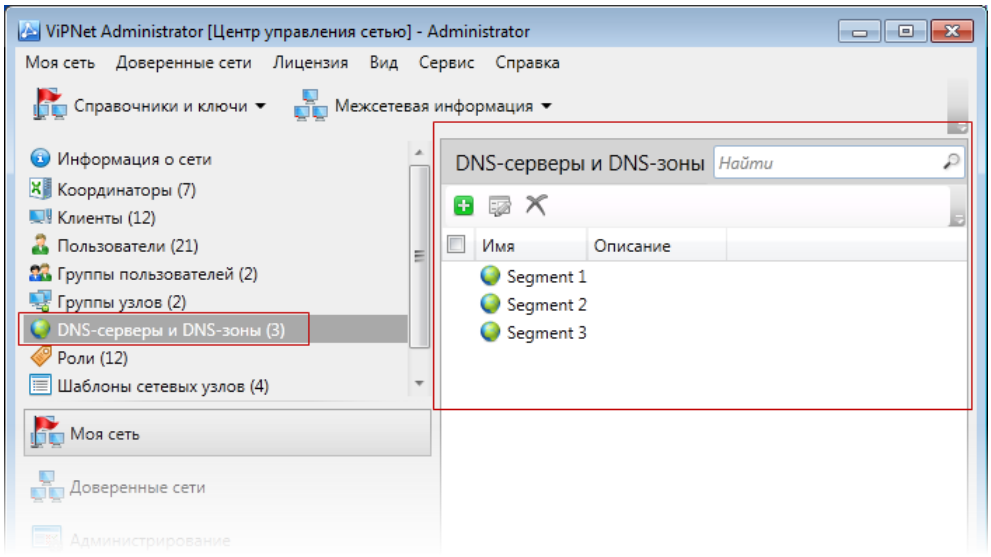

Рисунок 152. Управление списком защищенных DNS-серверов и доменных зон

- **Добавление новых ролей**

  В программу ViPNet Центр управления сетью были добавлены новые роли:

  - «xF100», «xF1000», «xF2000», «xF5000», «xF-VA» — позволяют развернуть координатор на базе соответствующих модификаций ПАК ViPNet xFirewall.
  - «Coordinator IG10 A/B», «Coordinator IG100 A/B» — позволяют развернуть координатор на базе соответствующих модификаций ПАК ViPNet Coordinator IG10 и ПАК ViPNet Coordinator IG100.
  - «ConServer» — позволяет установить серверное ПО для организации групповых чатов с помощью клиентского приложения ViPNet Connect.
  - «CPNs» (Customer Push Notification Server) — позволяет развернуть серверное ПО для рассылки push-уведомлений на устройства с ViPNet Connect.
  - Роль «VPN-сервер» переименована в роль «Программный VPN-координатор».
  - Роль «ThinClient» переименована в роль «Terminal».

- **Изменения в настройке параметров роли «Terminal» (ранее «ThinClient»)**

  Теперь с помощью ПО ViPNet Центр управления сетью вы можете задавать следующие настройки узла с ролью «Terminal»:

  - подключение пользователя к виртуальному рабочему столу IBS, использующему технологию Parallels VDI;
  - подключение USB-модема к узлу (см. «Настройка параметров подключения USB-модема в терминальной сессии» на стр. 155);
  - параметры доступа к веб-ресурсам через прокси-сервер в терминальной сессии (см. «Настройка параметров прокси-сервера для веб-браузера» на стр. 157);
  - перенаправление USB-устройств на сервер из терминальной сессии (см. «Настройка параметров подключения к терминальному серверу» на стр. 160).

- **Использование TCP-туннеля в настройках подключения к внешней сети для координатора**

Теперь вы можете установить TCP-туннель для каждого из выбранных координаторов в окне свойств координатора в разделе **Межсетевой экран**. Использование TCP-туннеля может быть настроено при подключении через межсетевой экран со статической трансляцией адресов или без использования межсетевого экрана.

- **Управление временем хранения записей журналов транспортных конвертов**

  Теперь вы можете задать время хранения записей для журналов транспортных конвертов (см. «Параметры журналов» на стр. 81).

- **Переименование параметра функции сервера открытого Интернета**

  В свойствах ролей для различных модификаций координаторов флажок **Координатор является сервером открытого Интернета** переименован в флажок **Координатор является защищенным интернет-шлюзом**.

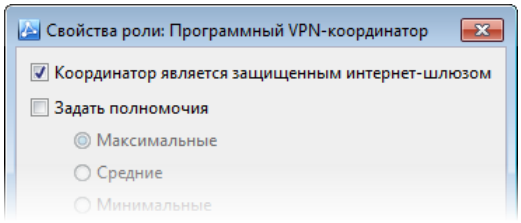

Рисунок 153. Переименование функции открытого Интернета

- **Добавлена возможность поиска по маске с использованием специальных символов**

  Теперь в любой строке поиска вы можете использовать символы подстановки, см. подробнее в разделе Интерфейс программы ViPNet Центр управления сетью (на стр. 54).

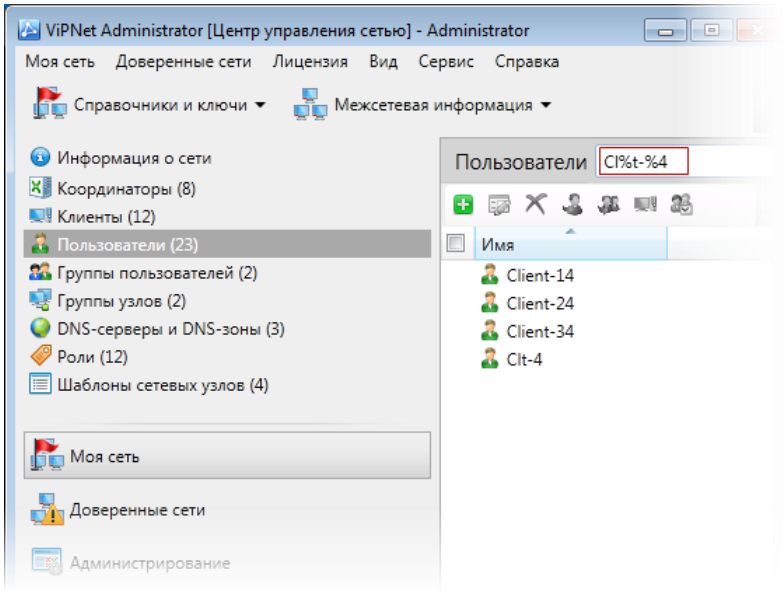

Рисунок 154. Поиск по маске при помощи специальных символов

Что нового в версии 4.6.2

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью по сравнению с версией 4.5.

- **Управление списком DNS- и WINS-серверов узлов**

  В качестве защищенного DNS- или WINS-сервера на сетевых узлах ViPNet можно использовать любой узел своей или доверенной сети ViPNet, на который добавлена соответствующая роль (см. «Добавление ролей „DNS-Сервер" и «WINS-Сервер»» на стр. 148). Раньше информация обо всех имеющихся в сети узлах с ролями «DNS-сервер» и «WINS-сервер» помещалась в справочники в виде файла `dns.txt` и передавалась на сетевые узлы, поэтому на каждом узле мог оказаться довольно большой список защищенных DNS- и WINS-серверов. Теперь для каждого сетевого узла вы можете задать собственный список DNS- и WINS-серверов и настроить приоритет их использования (см. «Настройка списков DNS- и WINS-серверов сетевого узла» на стр. 172), чтобы записи о наиболее приоритетных DNS- и WINS-серверах не оказались в конце списка и не были проигнорированы или же узел не использовал недоступные ему DNS- и WINS-серверы.

- **Добавление новых ролей**

  В программу ViPNet Центр управления сетью были добавлены новые роли (см. «Роли сетевых узлов» на стр. 266):

  - «Coordinator HW50 AU», «Coordinator HW1000 C», «Coordinator HW1000 D», «Coordinator HW5000» — позволяют развернуть координаторы на базе соответствующих модификаций ПАК ViPNet Coordinator HW.
  - «Coordinator IG10» — позволяет развернуть координатор на базе ПАК ViPNet Coordinator IG10.
  - «StateWatcher SHW1000», «StateWatcher SHW2000» — позволяет развернуть сервер системы мониторинга ViPNet StateWatcher на базе соответствующих модификаций ПАК ViPNet Statewatcher SHW.
  - «StateWatcher VA» — позволяет развернуть сервер системы мониторинга ViPNet StateWatcher на базе виртуального устройства StateWatcher VA.

- **Создание отчетов о структуре сети**

  В программе ViPNet Центр управления сетью реализована функция создания отчетов о структуре сети (см. «Создание отчета о структуре сети» на стр. 85). С помощью нее администраторы могут сохранять информацию об имеющейся структуре сети ViPNet в формат XML или HTML для последующего использования в сторонних программах или для встраивания в другие информационные системы, например системы управления предприятием. В данных отчетах информация о сети представлена в иерархическом виде, отображены все имеющиеся координаторы, клиенты и пользователи, а также информация о связях узлов и пользователей и назначенных ролях.

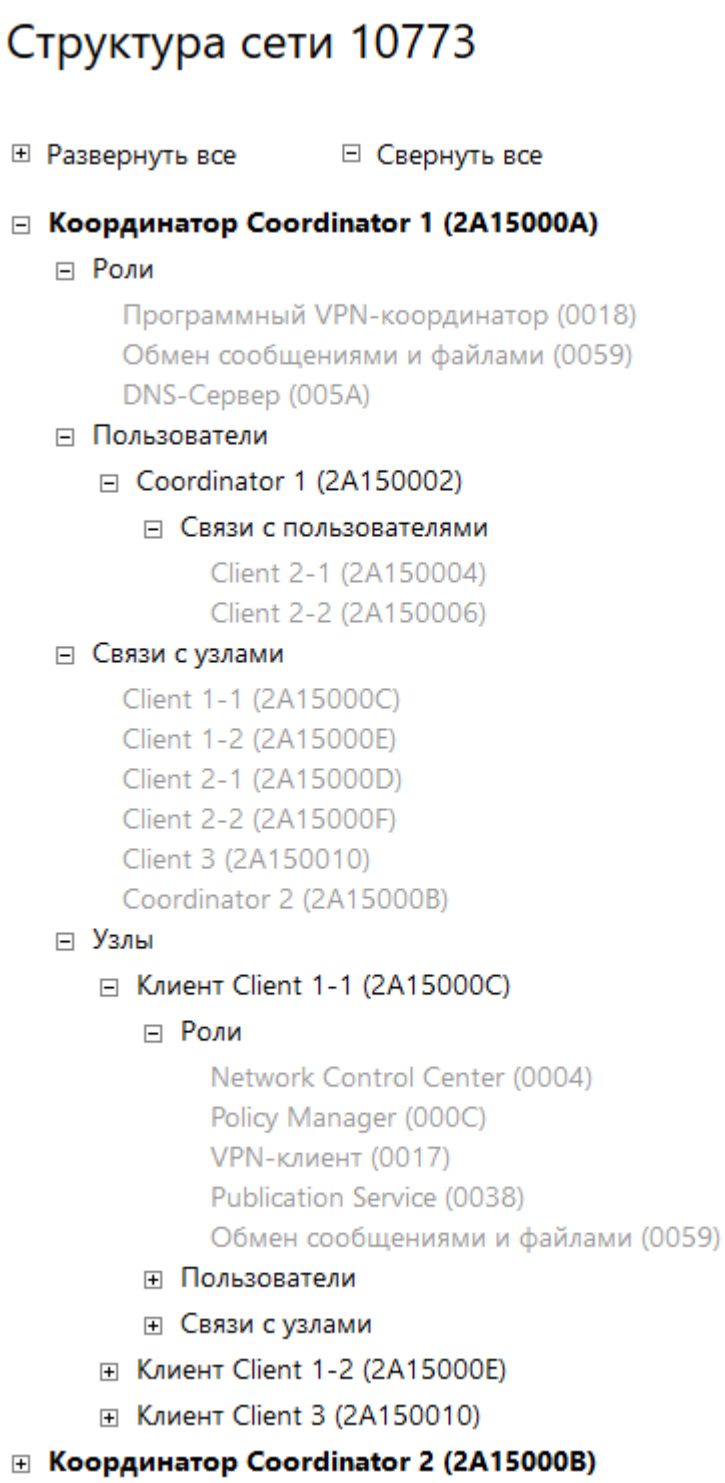

Рисунок 155. Просмотр отчета о структуре сети ViPNet в формате HTML

- **Создание отчетов о лицензионных ограничениях и их распределении**

  В программе ViPNet Центр управления сетью теперь можно создавать следующие отчеты о лицензии на сеть ViPNet (см. «Создание отчетов о лицензии на сеть» на стр. 110):

- Отчет о лицензионных ограничениях, в котором содержатся сведения об общем количестве лицензий на различные компоненты сети ViPNet, а также о количестве свободных и использованных лицензий на эти компоненты.
- Отчет о распределении лицензионных ограничений, в котором содержатся сведения о том, сколько лицензий на различные компоненты сети используется в главной и подчиненных сетях ViPNet. Создание отчетов данного типа доступно, только если в вашей организации развернута иерархическая система сетей ViPNet (на стр. 220).

Отчеты о лицензии на сеть ViPNet сохраняются в файлы формата CSV, затем вы можете использовать их в сторонних программах или распечатывать на принтере.

- **Изменения в системе лицензирования**

  Раньше в лицензии на сеть ViPNet были предусмотрены ограничения на используемые в сети роли и количество узлов с различными ролями. Ограничения на версии устанавливаемых компонентов ViPNet определялись общими ограничениями, заданными в лицензии для узлов сети ViPNet.

  В новой системе лицензирования добавлена возможность управления версиями отдельных компонентов ViPNet. Теперь файл лицензии может включать в себя дополнительные ограничения для ролей по версии и периоду использования устанавливаемого программного обеспечения (см. «Роли сетевых узлов» на стр. 31).

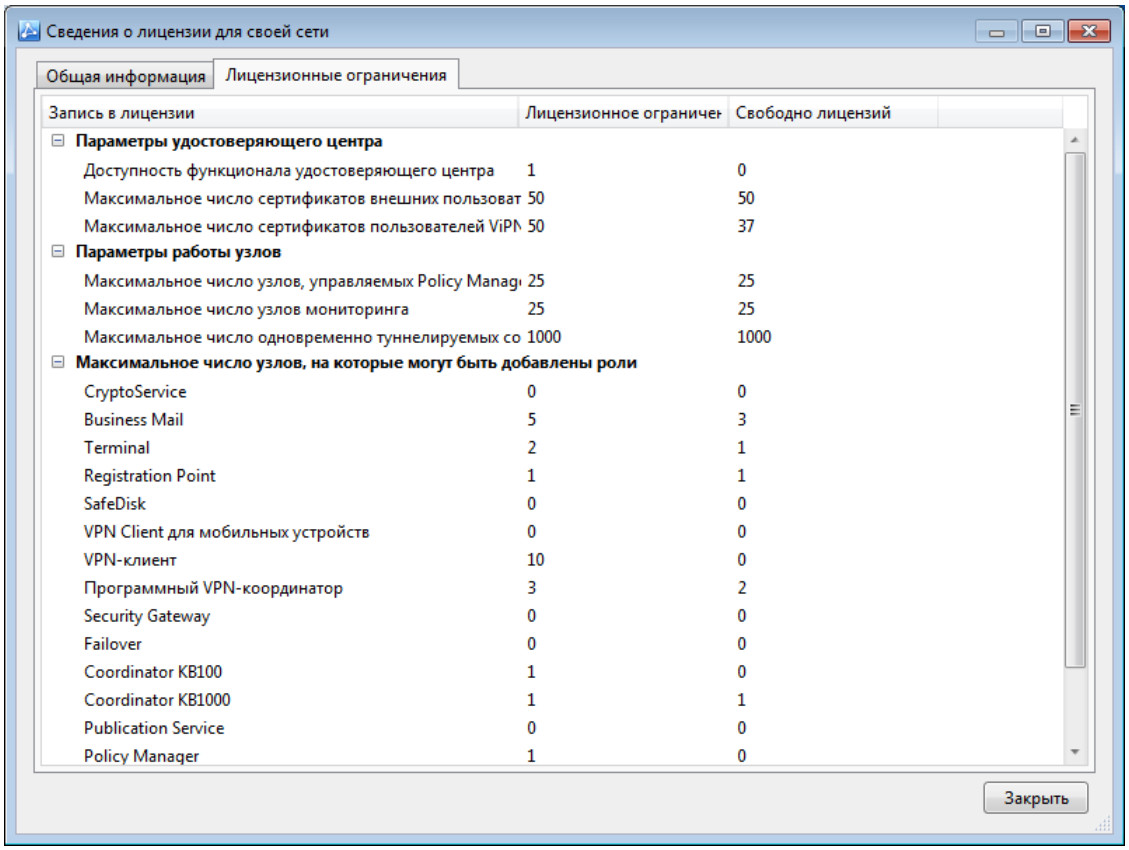

Рисунок 156. Просмотр информации о лицензионных ограничениях

- **Настройка подключения к базе данных**

В программе ViPNet Центр управления сетью реализована возможность настройки подключения к конкретной базе данных на SQL-сервере. Данная функция может понадобиться, если в организации имеется несколько сетей ViPNet и для каждой из них используется отдельная база данных ПО ViPNet Administrator на общем SQL-сервере.

- **Задание уровня полномочий для роли «VPN-сервер»**

  Раньше для настройки уровня полномочий пользователя координатора (узла с добавленной ролью «VPN-сервер») нужно было дополнительно добавлять на этот узел роль «VPN-клиент» и в ее свойствах указывать нужный уровень полномочий. Теперь вы можете задать уровень полномочий непосредственно в свойствах роли «VPN-сервер» (см. «Изменение уровня полномочий пользователя» на стр. 146).

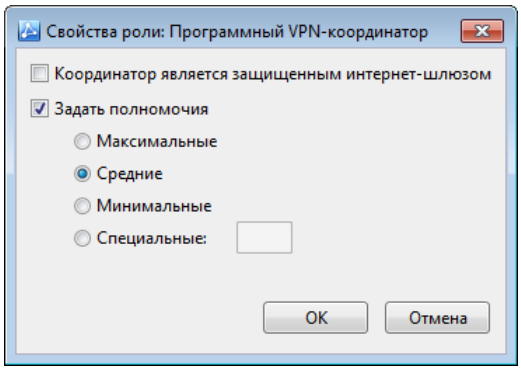

Рисунок 157. Настройка уровня полномочий для роли «Программный VPN-координатор»

- **Изменения в настройке параметров роли «ThinClient»**

  Раньше с помощью ПО ViPNet Administrator можно было задать только несколько стандартных параметров узла с ролью «ThinClient». Остальные настройки выполнялись непосредственно на узле в программе ViPNet ThinClient.

  Теперь с помощью ПО ViPNet Administrator вы можете задавать все параметры узла с ролью «ThinClient», которые поддерживаются программным обеспечением ViPNet ThinClient (см. «Настройка дополнительных параметров терминала» на стр. 159).

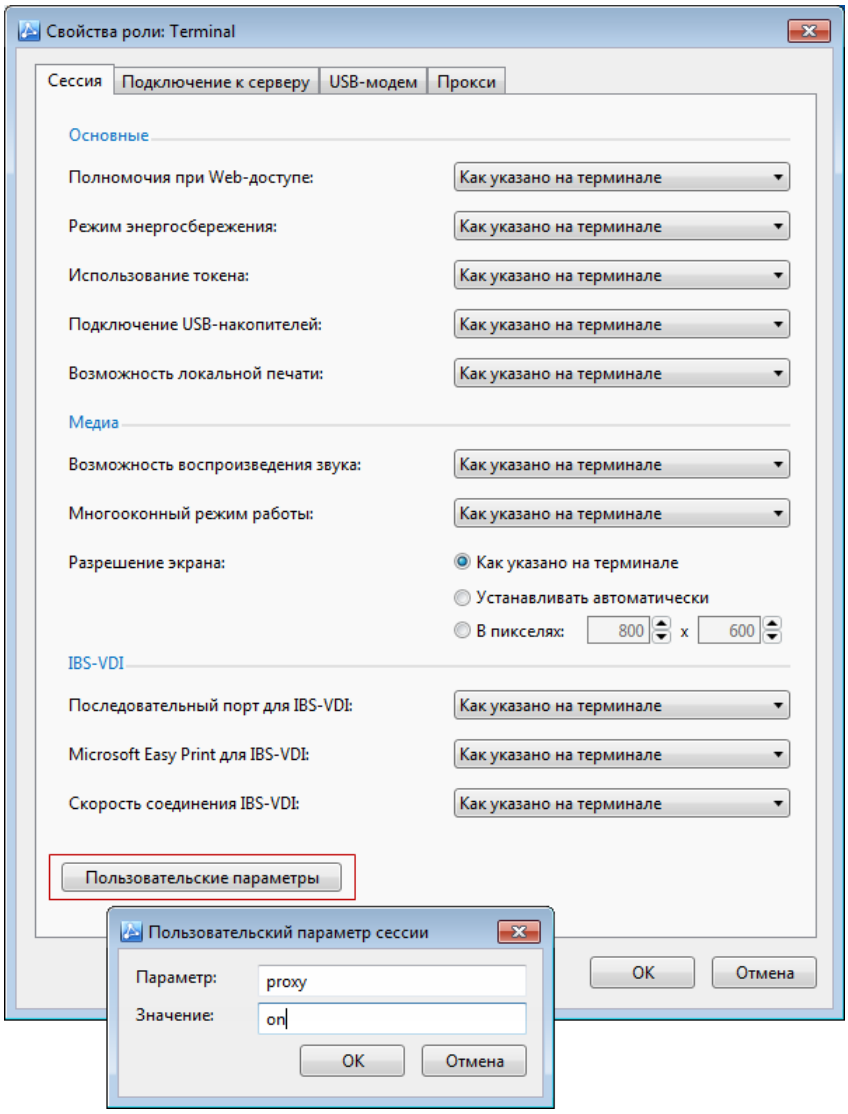

Рисунок 158. Настройка дополнительных параметров терминала

Что нового в версии 4.5

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью по сравнению с версией 4.4.

- **Добавление новых ролей**

  Добавлены следующие роли для сетевых узлов:

  - «Coordinator VA500» — позволяет вам развернуть координатор на базе виртуального устройства ViPNet Coordinator VA500.
  - «Failover500» — позволяет вам развернуть кластер горячего резервирования на базе виртуального устройства ViPNet Coordinator VA500.

- **Сведения о доверенных сетях в окне свойств шлюзового координатора**

Сведения о том, для каких доверенных сетей тот или иной координатор вашей сети является шлюзовым, вы можете просмотреть в свойствах доверенных сетей. Теперь имя, номер и шлюз доверенной сети, для которой координатор вашей сети является шлюзовым, вы можете также просмотреть в окне свойств этого координатора, выбрав раздел **Межсетевые каналы**.

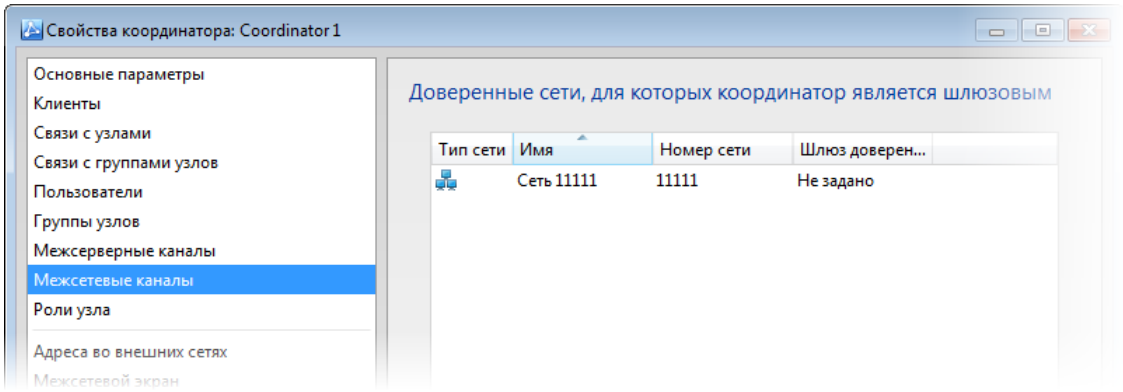

Рисунок 159. Сведения о доверенной сети в свойствах шлюзового координатора

Что нового в версии 4.4

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью версии 4.4.

- **Добавление новых ролей**

  Добавлены следующие роли для сетевых узлов:

  - «Connect» — позволяет использовать на клиенте программу ViPNet Connect, с помощью которой вы можете обмениваться текстовыми сообщениями с другими пользователями.
  - «Coordinator HW100-D», «Coordinator HW50-A» и «Coordinator HW50-B» — позволяют вам развернуть координаторы на базе соответствующих программно-аппаратного комплексов.
  - «Failover100», «Failover1000» и «Failover2000» — позволяют вам развернуть кластеры горячего резервирования на базе соответствующих программно-аппаратных комплексов ViPNet Coordinator HW.

- **Изменение названий ролей**

  Таблица 10. Старые и новые названия ролей сетевых узлов в ЦУСе

Старое название	Новое название
Деловая почта	Business Mail
Центр управления сетью	Network Control Center
ViPNet Cluster	Cluster Windows
ViPNet Terminal	ThinClient

- **Изменение логики проверки лицензии**

Теперь файл, содержащий информацию о лицензионных ограничениях, требуется указывать не при установке программы ViPNet Центр управления сетью, а при ее первом запуске. Это позволяет упростить и ускорить процесс установки программы.

- **Настройка параметров безопасности сетевых узлов**

  Теперь в программе ViPNet Центр управления сетью вы можете централизованно настроить следующие параметры безопасности сетевых узлов:

  - Шифрование данных.

    Теперь администратор сети ViPNet может централизованно задавать алгоритм шифрования исходящего IP-трафика сетевых узлов и писем, отправляемых пользователями сетевых узлов с помощью программы ViPNet Деловая почта.

  - Отключение брандмауэра Windows при запуске программ ViPNet Client и ViPNet Coordinator.

    Если для фильтрации IP-трафика, который проходит через узлы ViPNet, используются сетевые экраны, встроенные в программы ViPNet Client и ViPNet Coordinator, на данных узлах необходимо отключить брандмауэр Windows. В противном случае между встроенным сетевым экраном и брандмауэром Windows могут возникнуть конфликты, влекущие за собой проблемы с доступом в сеть. Раньше отключение брандмауэра Windows происходило автоматически при запуске программ ViPNet Client и ViPNet Coordinator, и администратор не мог изменить данную настройку. Теперь в случае необходимости использования брандмауэра Windows администратор может отменить его автоматическое отключение.

  - Сохранение пароля пользователя программы ViPNet Client и ViPNet Coordinator.

    Раньше данный параметр администратор сети ViPNet настраивал в программах ViPNet Client и ViPNet Coordinator. Теперь его можно задать в программе ViPNet Центр управления сетью и передать сразу на все узлы, на которых используются программы ViPNet Client или ViPNet Coordinator, в составе дистрибутива ключей или обновления справочников.

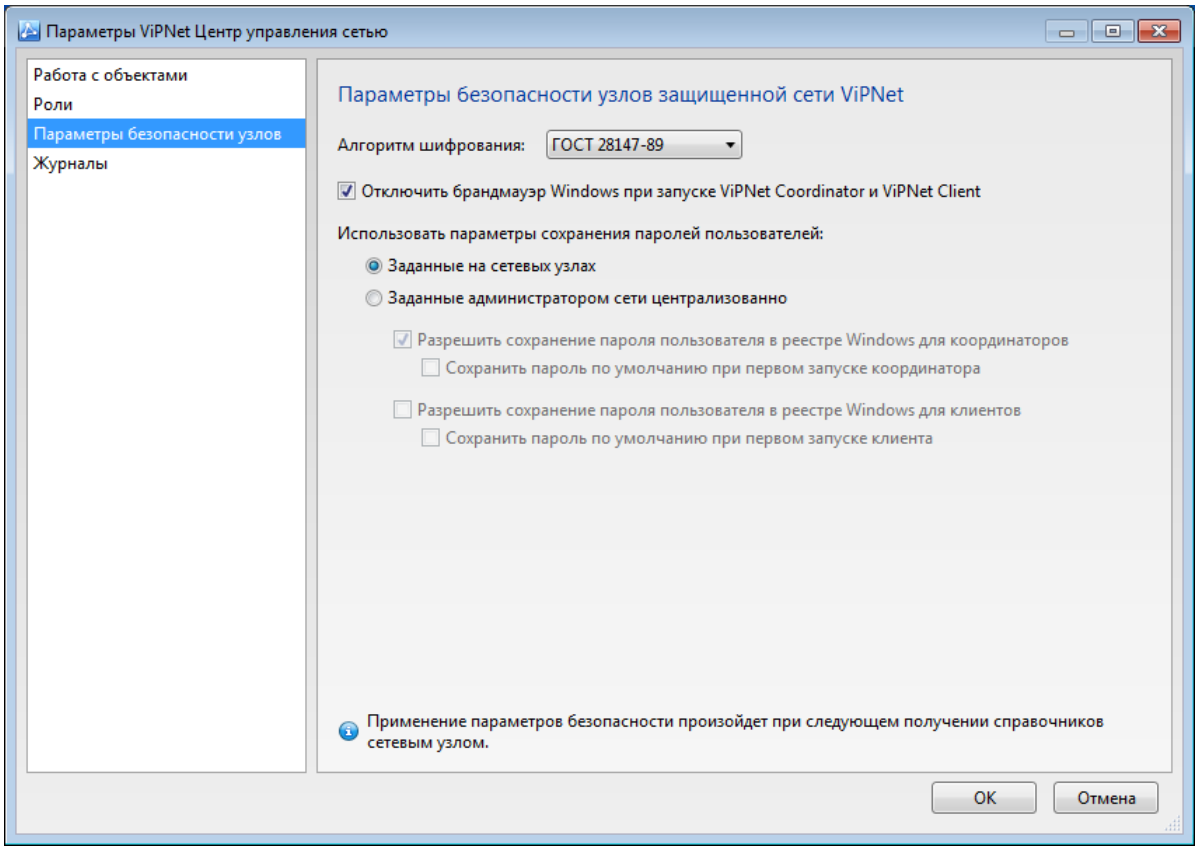

Рисунок 160. Настройка параметров безопасности сетевых узлов

- **Повышение быстродействия**
  - Увеличена скорость создания справочников.
  - Ускорен процесс загрузки данных из программы ViPNet Центр Управления сетью версии 3.2.x.
- **Улучшение внутренней функциональности**

  Исправлены незначительные ошибки, выявленные в процессе эксплуатации версии 4.4.0.
- **Обновление документации и справки**

  Доработаны документация и справка для программы ViPNet Центр управления сетью.

Более подробную информацию о новых возможностях программы см. в документе «Новые возможности ViPNet Administrator. Приложение к документации ViPNet».

Что нового в версии 4.3

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью версии 4.3.

- **Использование шаблонов сетевых узлов**

В программе ViPNet Центр управления сетью появилась возможность использовать шаблоны, в которых можно задавать различные настройки сетевых узлов. Данная функциональность облегчает задачу создания и редактирования параметров большого количества сетевых узлов (см. «Работа с шаблонами сетевых узлов» на стр. 191). Теперь при создании узлов вы можете назначить им необходимые шаблоны, настройки из которых буду применены к этим узлам.

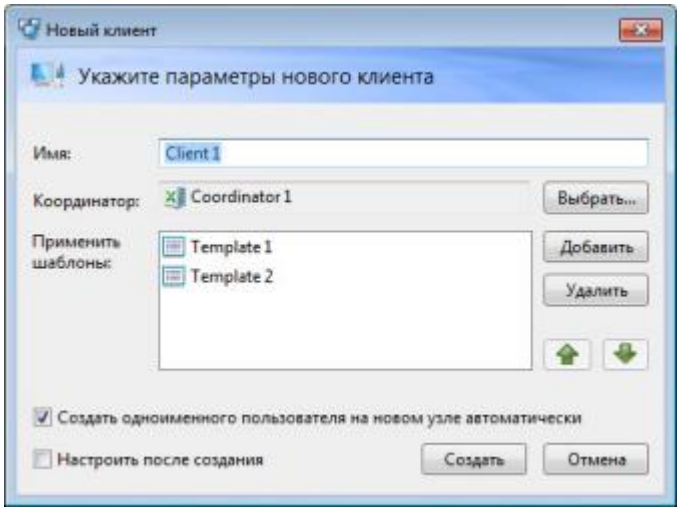

Рисунок 161. Применение шаблонов к создаваемому узлу

- **Расширены возможности работы с группами узлов**

  Раньше группы узлов использовались только для задания паролей администраторов узлов ViPNet. Теперь с помощью групп можно быстро создавать связи между сетевыми узлами, не тратя время на настройку связей для каждого узла по отдельности (см. «Работа с группами узлов» на стр. 196). Также вы можете осуществлять отправку справочников, ключей и обновлений ПО ViPNet на отдельные группы узлов.

- **Возможность переноса сетевого узла, на котором развернута программа ViPNet Центр управления сетью, на другой координатор**

  В предыдущей версии сменить координатор можно было только для обычных клиентов сети. Теперь реализована возможность переноса клиента, являющегося Центром управления сетью, на другой координатор, например, если нужно включить ЦУС в сегмент сети, который относится к другому координатору (см. «Перенос клиента, являющегося Центром управления сетью, на другой координатор» на стр. 132).

- **Изменения интерфейса программы**

  Интерфейс главного окна программы ViPNet Центр управления был изменен — в представлении **Моя сеть** на панель навигации был добавлен раздел **Шаблоны сетевых узлов**. Также в окнах создания клиентов, координаторов, пользователей и групп пользователей было удалено поле для ввода описания объекта.

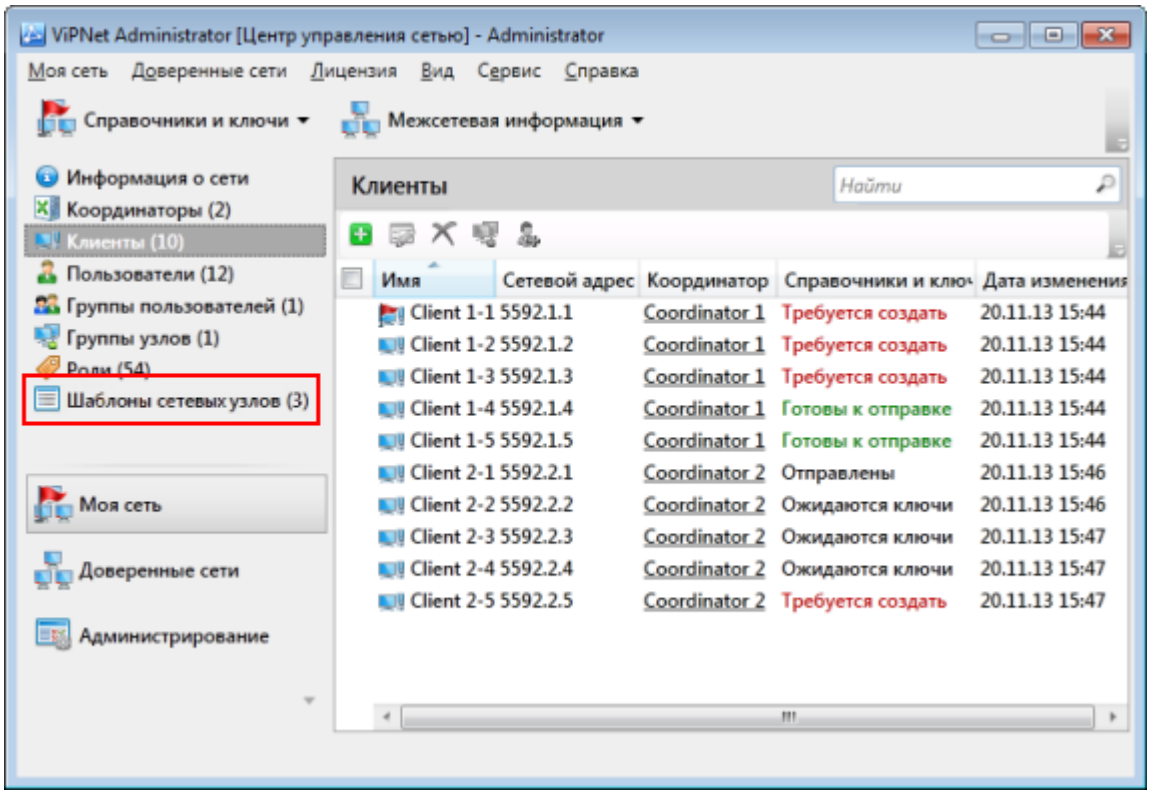

Рисунок 162. Изменения в интерфейсе

- **Новые принципы лицензирования**

  Отменены лицензионные ограничения, накладываемые на общее количество клиентов и координаторов сети ViPNet. Теперь файл лицензии ограничивает лишь число ролей, которое вы можете добавить на узлы вашей сети. Таким образом ограничивается число программ ViPNet, которое вы можете установить на сетевые узлы.

  Лицензия теперь может не только ограничивать количество сертификатов, которое может быть издано в УКЦ, но и полностью исключать функции удостоверяющего центра, скрывая при этом соответствующие элементы интерфейса. Впоследствии вы можете разблокировать функции удостоверяющего центра. Для этого необходимо обновить лицензию.

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины, в соответствии с Федеральным законом 06.04.2011 №63-ФЗ «Об электронной подписи»**

Старый термин	Новый термин	Название элемента интерфейса
Подпись	Электронная подпись	ЭП
Закрытый ключ	Ключ электронной подписи	Ключ ЭП
Открытый ключ	Ключ проверки электронной подписи	Ключ проверки ЭП
Сертификат открытого ключа подписи пользователя	Сертификат ключа проверки электронной подписи	Сертификат

Владелец сертификата	Владелец сертификата ключа проверки электронной подписи	Владелец сертификата
Список отозванных сертификатов (COC)	Список аннулированных сертификатов (CRL)	CRL
Отзыв сертификата	Аннулирование сертификата	—

В связи с изменениями переработан интерфейс программы.

- **Локализация интерфейса программы**

  Новые версии серверного и клиентского приложений ViPNet Центр управления сетью доступны на русском и английском языках. Язык интерфейса серверного приложения ЦУСа выбирается при установке программы. При установке клиентского приложения пользователем выбирается язык только для программы установки. Язык интерфейса клиентского приложения определяется автоматически при подключении к серверному приложению ЦУСа и совпадает с языком, выбранным для серверного приложения. Чтобы изменить язык клиентского приложения, необходимо переустановить серверное приложение ЦУСа и выбрать нужный язык.

Что нового в версии 4.2

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью версии 4.2.

- **Новая роль «Обмен сообщениями и файлами»**

  В версии 4.2 реализована возможность ограничить использование на сетевых узлах встроенных средств коммуникации — обмена сообщениями и обмена файлами. Для этого используются параметры новой роли «Обмен сообщениями и файлами». Ограничение коммуникации позволяет защитить сетевые узлы от получения нежелательных сообщений и файлов, а также запретить отдельным сетевым узлам обмен сообщениями или файлами.

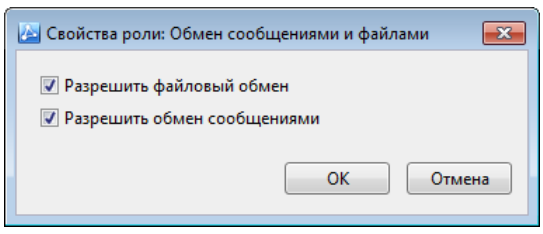

Рисунок 163. Задание разрешений на обмен сообщениями и файлами

По умолчанию роль «Обмен сообщениями и файлами» разрешает обмен сообщениями и обмен файлами и автоматически добавляется на сетевые узлы при их создании. Это соответствует отсутствию ограничений на использование средств коммуникации, как было принято в предыдущих версиях сети ViPNet. На сетевых узлах, которым эта роль не назначена, обмен сообщениями и файлами будет недоступен.

- **Новый порядок загрузки файлов обновления программного обеспечения**

  Изменен порядок загрузки файлов обновления программного обеспечения для отправки на сетевые узлы. В мастере обновления появилась одна кнопка для загрузки вместо множества отдельных ссылок для загрузки обновлений для разных типов программного обеспечения. Теперь для загрузки файла сначала нажмите кнопку, а затем выберите тип программного обеспечения и файл с обновлением. Новый порядок загрузки позволяет отображать в мастере обновления только загруженные в базу данных файлы, а также удалять из базы данных ненужные файлы обновления.

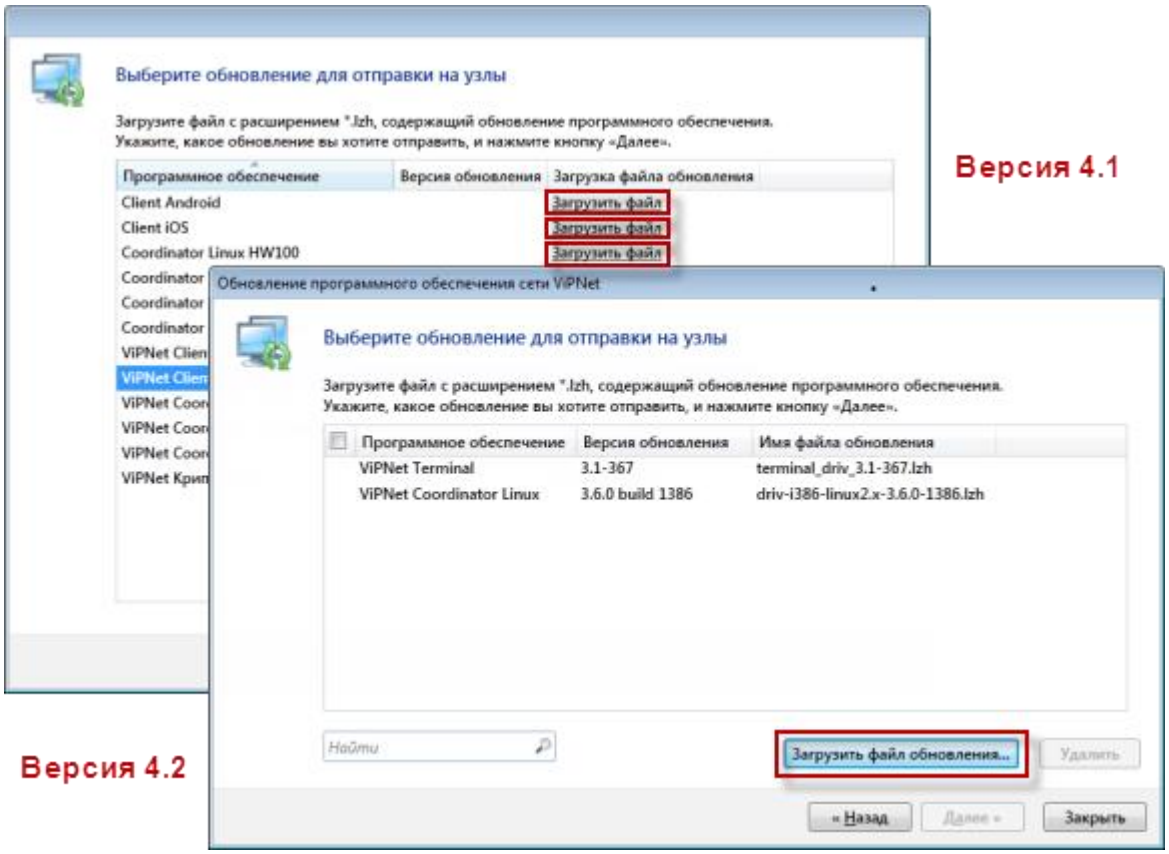

Рисунок 164. Новый порядок загрузки файлов обновления программного обеспечения

- **Выбор элементов в списках с помощью флажков**

  Реализована возможность выбора элементов в списках с помощью флажков. Для этого в списки добавлен первый столбец, содержащий флажки. Теперь вы можете выбрать или отменить выбор сразу всех элементов списка с помощью флажка, расположенного в заголовке списка.

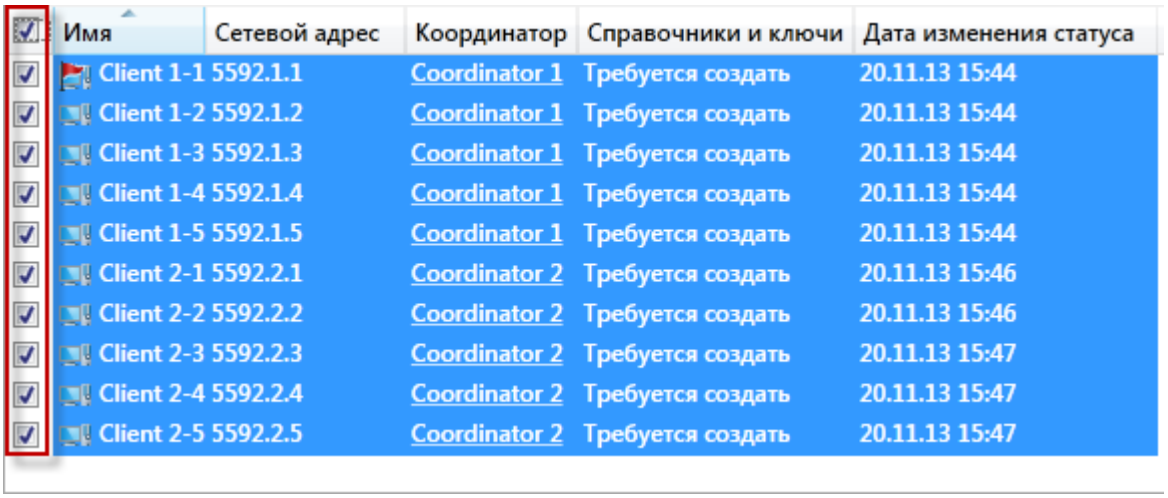

Рисунок 165. Выбор элементов в списке с помощью флажков

- **Настройка параметров журналов аудита**

  Реализована возможность настройки времени хранения записей в журналах аудита. Теперь вы можете задать требуемое время в диапазоне от 7 до 365 дней.

- **Групповая отправка межсетевой информации**

  Реализована возможность отправки межсетевой информации сразу в несколько доверенных сетей. Теперь вы можете сначала создать межсетевую информацию для разных сетей, а затем в одно действие отправить ее во все доверенные сети. Эта возможность избавляет вас от необходимости выбора доверенных сетей при отправке — межсетевая информация будет отправлена во все сети, для которых требуется ее обновление.

- **Ограничение на использование роли «Policy Manager»**

  В версии 4.2 управление политиками безопасности сетевых узлов с помощью программы ViPNet Policy Manager возможно исключительно из Центра управления сетью. Теперь роль «Policy Manager», которая определяет возможность управления политиками безопасности, можно добавить только на один сетевой узел — тот, который является Центром управления сетью.

- **Автоматическая доставка обновления при смене транспортного сервера клиента**

  Реализована автоматическая доставка обновления справочников и ключей на клиент при смене его транспортного сервера. Теперь вам не надо выполнять обновление вручную с помощью дистрибутива ключей. Доставку обновления обеспечивает старый транспортный сервер клиента, который используется еще в течение некоторого времени после смены. Время использования старого транспортного сервера задается в настройках программы.

- **Возможность размещения базы данных на существующем SQL-сервере**

  В версии 4.2 реализована возможность использовать для размещения базы данных существующий именованный экземпляр SQL-сервера. Теперь при установке серверного приложения ЦУСа вы можете не только установить SQL-сервер, входящий в комплект поставки, но также указать экземпляр SQL-сервера, ранее установленный на локальный или удаленный компьютер.

- **Изменение интерфейса**

Графический интерфейс программы приведен к более компактному виду. Теперь на панели навигации нет заголовка текущего представления, а панель инструментов содержит всего две кнопки. Изменена также цветовая гамма интерфейса, которая стала более сдержанной.

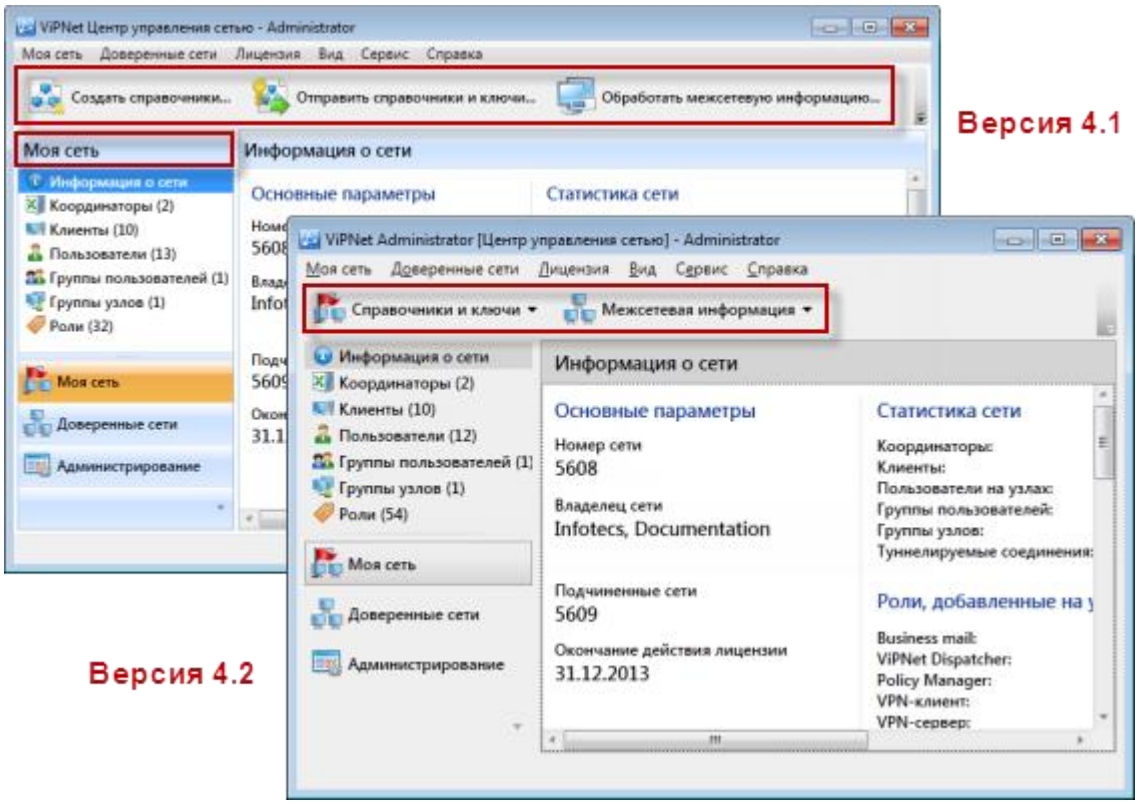

Рисунок 166. Оптимизированный интерфейс

Более подробную информацию о новых возможностях программы см. в документе «Новые возможности ViPNet Administrator версии 4.x. Приложение к документации ViPNet 4.x».

Что нового в версии 4.1

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью версии 4.1.

- **Роли «Сервер DNS» и «Сервер WINS»**

  В программе ViPNet Центр управления сетью 4.1 реализована возможность централизованного задания списка корпоративных серверов DNS (WINS). Для этого необходимо:

  - Добавить роли «Сервер DNS» и «Сервер WINS» на защищенные узлы (см. глоссарий, стр. 302), которые являются серверами DNS или WINS.
  - Добавить роли «Сервер DNS» и «Сервер WINS» на координаторы, туннелирующие серверы DNS или WINS.

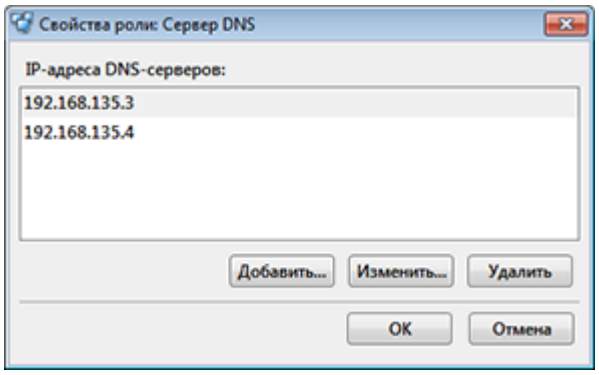

Рисунок 167. Задание адресов туннелируемых DNS-серверов

После добавления указанных ролей на защищенный узел на связанные с ним узлы в составе справочников будет передана информация о том, что узел с этой ролью или его туннелируемые узлы следует использовать в качестве серверов DNS или WINS.

- **Настройка параметров роли «ViPNet Terminal»**

  В версии 4.1 реализована возможность централизованного задания параметров термальных серверов и полномочий пользователей при работе в терминальной сессии. Для этого используются свойства роли «ViPNet Terminal», которые можно задать двумя способами:

  - Индивидуально для каждого клиента, на который добавлена роль «ViPNet Terminal», в окне свойств роли.
  - Централизованно для всех клиентов с ролью «ViPNet Terminal», которые зарегистрированы на определенном координаторе, в окне свойств координатора.

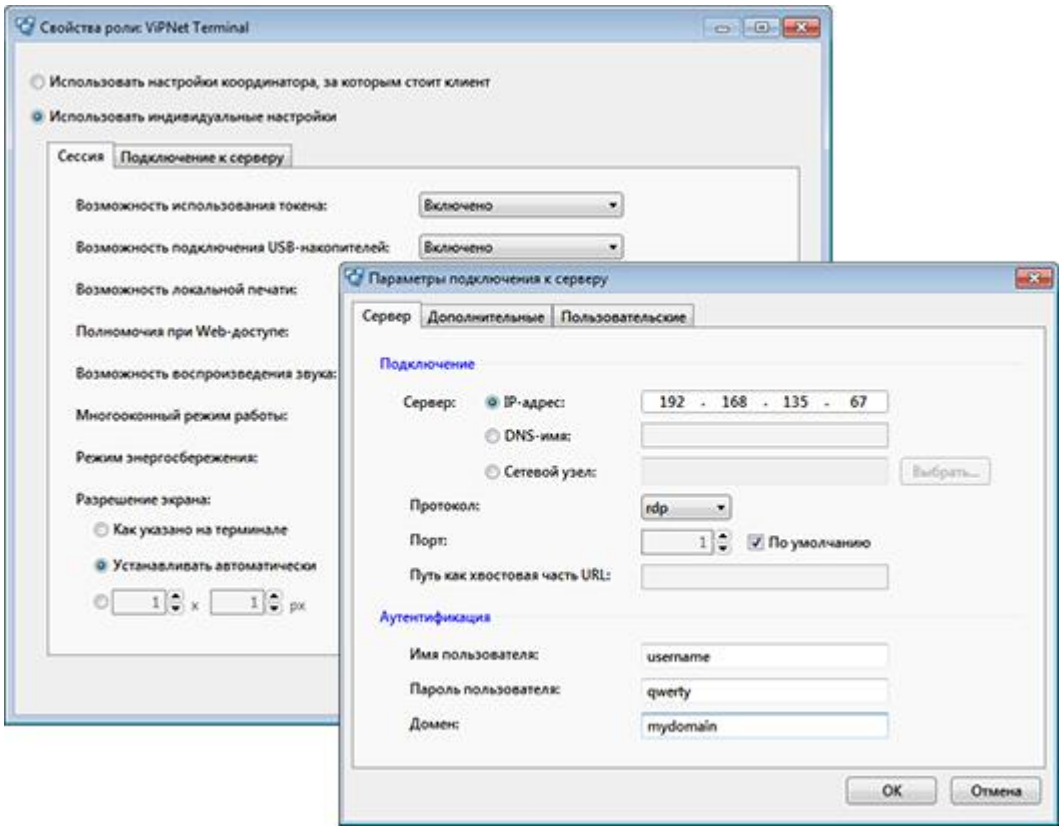

Рисунок 168. Свойства роли «ViPNet Terminal»

- **Блокировка отдельных операций со стороны ViPNet Удостоверяющий и ключевой центр**

  Программы ViPNet Удостоверяющий и ключевой центр и ViPNet Центр управления сетью при работе используют одну и ту же базу данных. Поэтому одновременное выполнение некоторых операций невозможно. В таком случае появляется предупреждение, и выполнение действия блокируется.

Более подробную информацию о новых возможностях программы см. в документе «Новые возможности ViPNet Administrator 4.x. Приложение к документации ViPNet 4.x».

Что нового в версии 4.0

В этом разделе представлен краткий обзор изменений и новых возможностей программы ViPNet Центр управления сетью версии 4.0.

- **Новая архитектура программы ViPNet Центр управления сетью**

  ViPNet Центр управления сетью 4.0 имеет клиент-серверную архитектуру и состоит из двух программных компонентов: серверного и клиентского приложений. Серверное приложение взаимодействует с базой данных SQL, в которой хранится информация об объектах сети ViPNet, ее структуре и настройках. Клиентское приложение обеспечивает интерфейс для управления сетью ViPNet.

- **Многопользовательский режим работы**

Поддерживается одновременное подключение к серверному приложению ViPNet Центр управления сетью нескольких клиентских приложений. Теперь структурой сети ViPNet и ее объектами могут управлять несколько администраторов с нескольких рабочих мест. Для аутентификации администратора в программе требуется указать имя учетной записи и пароль.

- **Новая терминология**

  В связи с изменением функциональности и логики работы Центра управления сетью были изменены некоторые термины и названия элементов интерфейса программы. Также были изменены названия некоторых ролей.

- **Появление графического интерфейса**

  Для программы ViPNet Центр управления сетью разработан новый интуитивно понятный графический интерфейс пользователя, который значительно упрощает работу с программой.

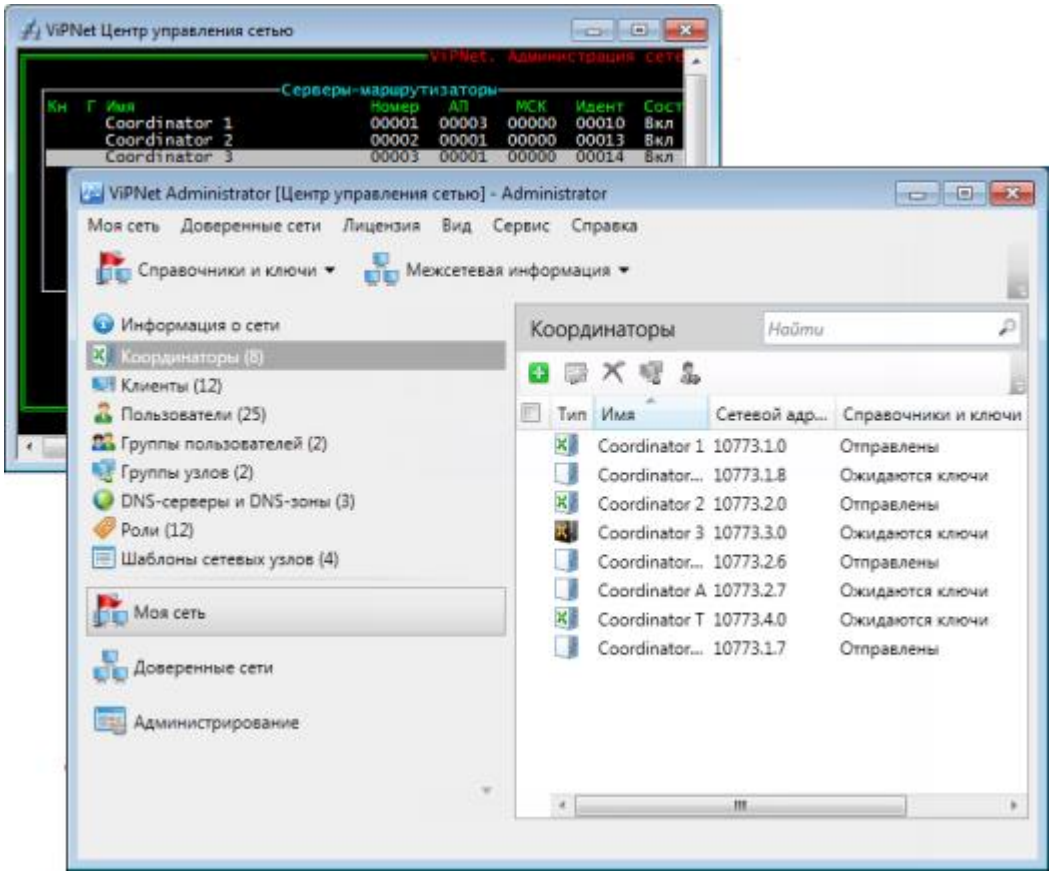

Рисунок 169. Сравнение интерфейса программы ViPNet Центр управления сетью версий 3.2.12 и 4.6.3

- **Изменение сценариев работы администратора**

  Многие сценарии работы администратора сети ViPNet были значительно изменены, например:

  - Простую структуру сети ViPNet можно создать с помощью мастера **Создание сети ViPNet**.
  - Регистрация пользователей осуществляется непосредственно на сетевых узлах.

- Установление межсетевого взаимодействия производится с помощью мастера **Установка межсетевого взаимодействия**.
- Связи между объектами задаются не на уровне типов коллективов, а между узлами, между пользователями, между пользователями и группами пользователей.
- Отправка справочников и ключей производится одновременно из одного окна.
- Для отправки обновления программного обеспечения на сетевые узлы требуется загрузить файлы обновления в базу данных. При этом проверяется тип программного обеспечения, которое содержится в загружаемом файле.

- **Конвертация данных программы ViPNet Центр управления сетью 3.x**

  Если для управления вашей сетью ViPNet использовалось программное обеспечение ViPNet Центр управления сетью 3.x, при переходе на версию 4.0 вы можете сохранить структуру и параметры сети. Для этого разработан удобный мастер, с помощью которого можно конвертировать данные программы ViPNet Центр управления сетью 3.x.

- **Усовершенствованная документация**

  Для программы ViPNet Центр управления сетью разработан полностью новый комплект документации. При разработке документации акцент был сделан на описании основных сценариев работы с программой.

D

Глоссарий

DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса серверов DNS, IP-адреса серверов WINS.

DNS-сервер

Сервер, содержащий часть базы данных DNS, используемой для доступа к именам компьютеров в интернет-домене. Например, ns.domain.net. Как правило, информация о домене хранится на двух DNS-серверах, называемых «Primary DNS» и «Secondary DNS» (дублирование делается для повышения отказоустойчивости системы).

Также DNS-сервер называют сервером доменных имен, сервером имен DNS.

DPI

DPI (Deep Packet Inspection) — технология проверки и фильтрации сетевых пакетов по их содержимому на прикладном уровне модели OSI.

IP-адрес

Адрес узла в сети, построенной на основе протокола IP.

IP-пакет

Форматированный блок информации, передаваемый в сети по протоколу IP.

PKI (инфраструктура открытых ключей)

От англ. Public Key Infrastructure — инфраструктура открытых ключей. Комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

SQL-сервер

Сервер базы данных, который работает под управлением программного обеспечения Microsoft SQL Server.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

VPN-сервер

Функция координатора, включающая в себя задачи сервера IP-адресов и транспортного сервера сети ViPNet.

Автоматизированная система управления технологическим процессом (АСУ ТП)

Группа технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях.

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

Внешние IP-адреса

Адреса внешней сети.

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Группа DNS-серверов

Совокупность списка доменных зон и списка закрепленных за ними DNS-серверов.

Группа узлов

Множество сетевых узлов ViPNet, объединенное под общим именем для удобства администрирования. Например, позволяет задать единый пароль администратора для всех сетевых узлов ViPNet, входящих в данную группу.

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Доверенная сеть

Сеть ViPNet, с узлами которой узлы своей сети ViPNet осуществляют защищенное взаимодействие.

Доменная зона (DNS-зона)

Группа имен системы DNS, входящая в конкретный домен или поддомены более низких уровней, находящаяся под одним административным управлением и обслуживаемая одним или несколькими DNS-серверами.

Защищенное соединение

Соединение между узлами, зашифрованное с помощью программного обеспечения ViPNet.

Защищенные прикладные серверы

Прикладные серверы (веб-сервер, почтовый сервер, FTP-сервер и так далее), размещенные на защищенных узлах.

Защищенный DNS-сервер

Защищенный внутренний DNS-сервер организации, который является защищенным узлом сети или туннелируется координатором ViPNet и входит в группу DNS-серверов.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Кластер (ViPNet-кластер)

Группа компьютеров (элементов кластера), объединенных высокоскоростными каналами связи и функционирующих как единое целое.

Для развертывания, настройки и управления ViPNet-кластером используется ПО ViPNet Cluster. На компьютерах, входящих в состав кластера, также должно быть установлено ПО ViPNet Coordinator.

С точки зрения сети ViPNet, кластер представлен одним сетевым узлом, является координатором и обладает всей его функциональностью.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключи пользователя ViPNet

Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Лицензия на сеть

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet. В частности, лицензия на сеть ViPNet определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешенную версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

Межсетевая информация

Информация о доверенной сети или своей сети, предназначенная для организации или изменения межсетевого взаимодействия. В состав межсетевой информации входят связи между сетевыми объектами, параметры сетевых узлов ViPNet и служебная информация (сертификаты издателей, списки аннулированных сертификатов).

Межсетевое взаимодействие

Информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Межсетевой мастер-ключ

Ключ, служащий для формирования ключей обмена между сетевыми узлами разных сетей ViPNet.

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-

трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

Модуль DPI

программный модуль ПО ViPNet xFirewall, выполняющий фильтрацию трафика на прикладном уровне модели OSI для определенного набора приложений и протоколов.

Обязательные связи

Связи между сетевыми узлами ViPNet, наличие которых является обязательным для функционирования сети ViPNet. Эти связи не могут быть удалены.

Примером обязательных связей является связь клиента с координатором, который является его транспортным сервером.

Открытый Интернет (Защищенный интернет-шлюз)

Технология, реализованная в программном обеспечении ViPNet. При подключении к Интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от Интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

Начиная с версии ПО ViPNet Administrator ЦУС 4.6.3, технология «Открытый Интернет» называется «Защищенный интернет-шлюз».

Открытый трафик

Поток незашифрованных IP-пакетов.

Открытый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

Пароль администратора сетевого узла ViPNet

Пароль для входа на сетевом узле ViPNet в режим администратора, в рамках которого становятся доступны дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр (в сетях, которые администрируются при помощи ПО ViPNet Administrator) или ViPNet Network Manager (в сетях, которые администрируются при помощи ПО ViPNet Network Manager).

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

Промышленная сеть

Сеть передачи данных, связывающая различные датчики, исполнительные механизмы, промышленные контроллеры и используемая в промышленной автоматизации.

Протокол 241

IP-протокол с идентификатором 241, специально разработанный для использования в программном обеспечении ViPNet.

Публичный адрес

IP-адрес, который может применяться в Интернете.

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сертификат ключа проверки электронной подписи

Сертификат ключа проверки — это электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN.

Сетевой объект

Сетевой узел, пользователь, группа узлов или группа пользователей.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Симметричное шифрование

Способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ, который должен сохраняться в секрете обеими сторонами.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Структура сети ViPNet

Упорядоченная совокупность связей между компонентами сети ViPNet, такими как:

- рабочее место администратора сети ViPNet;
- координаторы;
- клиенты.

Каждый клиент должен быть зарегистрирован на координаторе. Связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

Терминальный сервер

Выделенный компьютер, предоставляющий вычислительные ресурсы клиентам, которые подключаются к терминальному серверу по сети. Преимущества работы в терминальном режиме включают снижение расходов на программное и аппаратное обеспечение, уменьшение затрат времени на администрирование, повышение уровня защиты от внутренних злоумышленников.

Тип межсетевого экрана (ФСТЭК)

Совокупность особенностей межсетевых экранов в зависимости от их применения в информационных системах и технического исполнения (программное или программно-аппаратное), выделяемые классификацией ФСТЭК России. Выделены несколько типов межсетевых экранов: тип «А», тип «Б, тип „В", тип «Г», тип «Д». Подробнее см. на сайте ФСТЭК России http://www.fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1142-informatsionnoe-soobshchenie-fstek-rossii-ot-28-aprelya-2016-g-n-240-24-1986.

Тонкий клиент

Компьютер, предназначенный для доступа к приложениям и данным, которые размещаются на терминальном сервере.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на сетевые узлы ViPNet транспортным модулем ViPNet MFTP.

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Транспортный сервер

Функциональность координатора, обеспечивающая маршрутизацию транспортных конвертов между узлами сети ViPNet.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через Интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

Файл лицензии

Специальный файл `*.itcslic` или `infotecs.reg`, в котором зафиксированы ограничения для вашей сети ViPNet.

Фильтрация содержимого трафика

Функция, которая обеспечивает фильтрацию IP-трафика на прикладном уровне модели OSI с помощью технологии глубокой инспекции пакетов (Deep Packet Inspection, DPI) по типам приложений и прикладных протоколов, а также по пользователям.

Частный адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к Интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в Интернете. Чтобы выйти в Интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие.

Шлюзовые координаторы назначаются в ЦУСе каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Указатель

D

DHCP (Dynamic Host Configuration Protocol) - 299
DNS-сервер - 299
DPI - 299

I

IP-адрес - 299
IP-пакет - 299

P

PKI (инфраструктура открытых ключей) - 300

S

SQL-сервер - 300

V

ViPNet Administrator - 300
ViPNet Удостоверяющий и ключевой центр (УКЦ) - 300
ViPNet Центр управления сетью (ЦУС) - 300
VPN-сервер - 300

А

Автоматизированная система управления технологическим процессом (АСУ ТП) - 301
Администратор сети ViPNet - 301
Архитектура программы ViPNet Центр управления сетью - 24
Аутентификация - 301

В

Введение - 9
Взаимодействие с программой ViPNet Registration Point - 26
Взаимодействие с программой ViPNet Удостоверяющий и ключевой центр - 25
Виртуальная защищенная сеть - 301
Виртуальный IP-адрес - 301
Включение функции защищенного интернет-шлюза - 165
Внешние IP-адреса - 301
Внешняя сеть - 301
Возможные неполадки и способы их устранения - 262

Г

Группа DNS-серверов - 302
Группа узлов - 302
Групповая обработка межсетевой информации - 257
Групповая отправка межсетевой информации - 253
Групповое добавление ролей на сетевые узлы - 144

Д

Дистрибутив ключей - 302
Для кого предназначен документ - 10
Добавление группы пользователей - 215
Добавление группы узлов - 196
Добавление клиента - 113
Добавление координатора - 112
Добавление пользовательских параметров - 164
Добавление пользователя - 204
Добавление ролей - 148
Добавление ролей на сетевые узлы - 142
Доверенная сеть - 302
Доменная зона (DNS-зона) - 302

Ж

Журналы аудита - 100
Журналы транспортных конвертов - 102

З

Завершение организации межсетевого взаимодействия - 240
Загрузка межсетевой информации из файла - 259
Загрузка существующей структуры сети из программы версии 3.x - 67
Задание DNS-имен сетевого узла - 177
Задание IP-адресов сетевого узла - 175
Задание адреса для связи по каналу SMTP - 177
Задание адресов сетевого узла - 175
Запуск и завершение работы клиентского приложения - 49
Запуск и завершение работы программы ViPNet Центр управления сетью - 49
Запуск серверного приложения - 49
Защищенное соединение - 302
Защищенные прикладные серверы - 302
Защищенный DNS-сервер - 302
Защищенный узел - 302

И

Иерархическая система сетей ViPNet - 220
Изменение допустимого числа запросов для роли - 151
Изменение пароля учетной записи - 74
Изменение псевдонимов пользователя - 210
Изменение связей группы пользователей - 218
Изменение связей между пользователями - 207
Изменение связей между сетевыми узлами - 138
Изменение связей пользователя с группами пользователей - 212
Изменение связей с группами узлов - 199
Изменение связей с объектами доверенной сети - 245
Изменение связей с сетевыми узлами - 198
Изменение списка групп, в которые входит пользователь - 211
Изменение списка групп, в которые входит сетевой узел - 189
Изменение списка объектов, участвующих в межсетевом взаимодействии - 243
Изменение списка пользователей сетевого узла - 136
Изменение списка ролей сетевого узла - 142
Изменение списка сетевых узлов в группе - 197
Изменение списка сетевых узлов пользователя - 206
Изменение списка терминальных серверов - 160
Изменение списка узлов, зарегистрированных на координаторе - 120
Изменение списка участников группы пользователей - 216
Изменение статуса связей с объектами доверенных сетей - 247
Изменение уровня полномочий пользователя - 146
Изменение числа узлов мониторинга для роли - 150
Изменение числа элементов кластера для роли - 166
Изменение шлюзового координатора своей сети - 249
Инициация межсетевого взаимодействия - 234
Интерфейс программы ViPNet Центр управления сетью - 54
Истекает срок действия лицензии на сеть ViPNet - 265
История версий - 278

К

Кластер (ViPNet-кластер) - 303
Клиент (ViPNet-клиент) - 303
Клиентское приложение - 16
Ключ проверки электронной подписи - 303
Ключ электронной подписи - 303
Ключи пользователя ViPNet - 303
Ключи узла ViPNet - 304
Комплект поставки - 18
Контейнер ключей - 304
Координатор (ViPNet-координатор) - 304

Л

Лицензия на сеть - 304
Лицензия на сеть ViPNet - 23

М

Межсетевая информация - 304
Межсетевое взаимодействие - 232, 304
Межсетевой мастер-ключ - 304
Межсетевой экран - 304
Многопользовательская работа в программе - 72
Модуль DPI - 305

Н

Назначение лицензионных ограничений для отдельной сети - 227
Назначение программы ViPNet Центр управления сетью - 24
Настройка дополнительных параметров терминала - 159
Настройка защищенных DNS-серверов - 168
Настройка межсерверных каналов между координаторами, выполняющими функции VPN-сервера - 122
Настройка параметров клиента - 128
Настройка параметров координатора - 118
Настройка параметров межсетевого экрана клиентов на сервере IP-адресов - 186
Настройка параметров подключения USB-модема в терминальной сессии - 155
Настройка параметров подключения к внешней сети - 178
Настройка параметров подключения к терминальному серверу - 160
Настройка параметров пользователей - 202
Настройка параметров программы по умолчанию - 75
Настройка параметров прокси-сервера для веб-браузера - 157
Настройка параметров роли - 147, 152
Настройка параметров сетевых узлов - 111
Настройка подключения через координатор в качестве межсетевого экрана - 185
Настройка подключения через межсетевой экран с динамической трансляцией адресов - 182
Настройка подключения через межсетевой экран со статической трансляцией адресов - 183
Настройка полномочий пользователя ViPNet Terminal - 153
Настройка списка защищенных DNS-серверов и доменных зон - 168
Настройка списка управляемых узлов для роли - 149
Настройка списков DNS- и WINS-серверов сетевого узла - 172
Настройка типа межсетевого экрана ПАК ViPNet Coordinator IG - 166
Настройка туннелирования - 123
Настройка шаблона сетевых узлов - 192
Начало работы с программой ViPNet Центр управления сетью - 47
Не удается установить соединение с SQL-сервером - 263
Не удается установить соединение с сервером ViPNet Центр управления сетью - 262
Некорректная обработка межсетевой информации - 264
Новые возможности 4.6.4 - 13

О

О документе - 10
О программе - 12
Обновление лицензии - 108
Обновление программного обеспечения - 94
Обновление справочников и ключей - 87
Обработка межсетевой информации для отдельной сети - 256
Обратная связь - 19
Общие сведения о сетях ViPNet - 20
Обязательные связи - 305

Организация межсетевого взаимодействия - 233
Основные возможности программы ViPNet Центр управления сетью - 70
Основные параметры пользователя - 205
Особенности создания межсетевой информации в ПО ViPNet Administrator 3.x - 236
Открытый Интернет (Защищенный интернет-шлюз) - 305
Открытый трафик - 305
Открытый узел - 305
Отправка межсетевой информации - 251
Отправка межсетевой информации через сеть ViPNet - 252
Отправка обновлений на сетевые узлы - 87
Отправка справочников и ключей - 91
Ошибка при вводе имени администратора и пароля - 264
Ошибки при загрузке структуры сети из программы ViPNet Центр управления сетью версии 3.x - 264
Ошибки при сохранении отчета о структуре сети - 265

П

Папка ключей пользователя - 305
Параметры безопасности узлов - 76
Параметры журналов - 81
Параметры межсетевого экрана клиента - 180
Параметры межсетевого экрана координатора - 178
Параметры подключения защищенных узлов к внешней сети - 37
Параметры работы с объектами сети - 75
Пароль администратора сетевого узла ViPNet - 305
Первый запуск клиентского приложения - 51
Передача межсетевой информации в виде файла - 254
Перенос клиента на другой координатор - 129
Перенос клиента, являющегося Центром управления сетью, на другой координатор - 132
Перенос координатора без функций VPN-сервера на другой координатор - 125
Подключение без использования межсетевого экрана - 39
Подключение через координатор - 40
Подключение через межсетевой экран с динамической трансляцией адресов - 42
Подключение через межсетевой экран со статической трансляцией адресов - 44
Полномочия пользователя - 306
Превышено максимальное число узлов, на которые добавлена роль - 265
Представление - 55, 56, 58
Прекращение межсетевого взаимодействия - 261
Прием и обработка полученной межсетевой информации - 236
Прием межсетевой информации - 255
Применение шаблонов для редактирования свойств сетевых узлов - 194
Принцип работы иерархической системы сетей ViPNet - 221
Принцип функционирования сети ViPNet - 21
Принципы осуществления соединений в сети ViPNet - 37
Проверка конфигурации сети - 83
Программа ViPNet Центр управления сетью - 24
Промышленная сеть - 306
Просмотр журналов - 100
Просмотр и изменение основных параметров клиента - 128
Просмотр и изменение основных параметров координатора - 119
Просмотр сведений о лицензии для своей сети - 106
Просмотр сведений об общей лицензии - 230
Протокол 241 - 306
Публичный адрес - 306

Р

Работа с группами пользователей - 215
Работа с группами узлов - 196
Работа с лицензией - 106
Работа с шаблонами сетевых узлов - 191
Развертывание иерархической системы сетей ViPNet - 223
Распределение лицензии для всех сетей - 225
Распределение общей лицензии между сетями - 225
Резервное копирование и восстановление данных - 99
Роли сетевых узлов - 31, 266
Роли узлов по умолчанию - 79
Роль - 306

С

Связи между объектами сети ViPNet - 29
Связи с группами узлов - 140
Связи с объектами доверенных сетей - 242
Связи с сетевыми узлами - 138
Сервер IP-адресов - 306
Сервер соединений - 306
Серверное приложение - 15
Сертификат ключа проверки электронной подписи - 307
Сетевой интерфейс - 307
Сетевой объект - 307
Сетевой узел ViPNet - 307
Сеть ViPNet - 307
Симметричное шифрование - 307
Системные требования - 15
Смена сервера IP-адресов - 134
Соглашения документа - 10
Создание межсетевой информации - 252
Создание отчета о структуре сети - 85
Создание отчетов о лицензии на сеть - 110
Создание пользователя и настройка его параметров - 203
Создание сетевого узла - 112
Создание сети ViPNet
порядок действий - 60
Создание справочников - 88
Создание структуры сети ViPNet с помощью мастера - 62
Создание учетной записи - 72
Создание шаблона сетевых узлов - 191
Список аннулированных сертификатов (CRL) - 307
Справочники - 307
Справочники и ключи ViPNet - 32
Структура сети ViPNet - 308

Т

Терминальный сервер - 308
Тип межсетевого экрана (ФСТЭК) - 308
Тонкий клиент - 308
Трансляция сетевых адресов (NAT) - 308
Транспортный конверт - 308
Транспортный модуль (MFTP) - 308
Транспортный сервер - 309
Туннелирование - 35, 309
Туннелируемый узел - 309

У

Удаление группы пользователей - 216
Удаление группы узлов - 197
Удаление клиента - 117
Удаление координатора - 116
Удаление пользователя - 204
Удаление сетевого узла - 116
Удаление учетной записи - 73
Удаление шаблона сетевых узлов - 195
Управление сетью ViPNet - 69
Управление учетными записями администраторов - 72
Установка программы ViPNet Центр управления сетью - 48

Ф

Файл лицензии - 309
Фильтрация содержимого трафика - 309
Функции координатора в защищенной сети ViPNet - 33

Ч

Частный адрес - 309
Что нового в версии 4.0 - 296
Что нового в версии 4.1 - 294
Что нового в версии 4.2 - 291
Что нового в версии 4.3 - 288
Что нового в версии 4.4 - 286
Что нового в версии 4.5 - 285
Что нового в версии 4.6.2 - 281
Что нового в версии 4.6.3 - 278

Ш

Шлюзовой координатор - 309

Э

Электронная подпись - 310