ViPNet Policy Manager 4.3

Руководство администратора

infotecs

1991–2016 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00119-04 32 01

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС»

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

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

Сайт компании «ИнфоТеКС»: (http://www.infotecs.ru)

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение ... **7**
О документе ... 8
Для кого предназначен документ ... 8
Соглашения документа ... 8
О программе ... 9
Новые возможности версии 4.3.3 ... 9
Системные требования ... 11
Требования к SQL-серверу для развертывания базы данных ... 11
Совместимость с ПО ViPNet ... 12
Комплект поставки ... 13
Обратная связь ... 14

Глава 1. Общие сведения ... **15**
Принципы централизованного управления политиками безопасности сетевых узлов ... 16
Основные возможности ViPNet Policy Manager ... 18
Лицензирование ViPNet Policy Manager ... 20

Глава 2. Установка, обновление и удаление ViPNet Policy Manager ... **21**
Последовательность действий при установке ViPNet Policy Manager ... 22
Информация для администратора SQL ... 23
Установка ViPNet Policy Manager ... 24
Обновление ViPNet Policy Manager ... 26
Удаление ViPNet Policy Manager ... 27

Глава 3. Запуск и завершение работы с ViPNet Policy Manager ... **28**
Запуск программы ... 29
Интерфейс программы ... 30
Завершение работы с программой ... 32

Глава 4. Быстрый старт ... **33**
Начало работы ... 34
Как сменить пароль встроенной учетной записи ... 36
Как создать подразделение ... 37
Как создать шаблон политики безопасности ... 38
Как назначить шаблон политики безопасности сетевым узлам или подразделениям ... 39

Как отправить политики безопасности на сетевые узлы 40
Как посмотреть журнал отправки и применения политик безопасности 41
Как создать учетную запись 42

Глава 5. Управление учетными записями и ролями пользователей 43
Разграничение полномочий на основе ролей пользователей 44
Управление учетными записями 45
Создание и изменение учетной записи 45
Удаление учетной записи 48
Управление ролями пользователей 49
Создание и изменение роли пользователей 49
Удаление роли пользователей 51
Смена пароля пользователя 52

Глава 6. Работа с сетевыми узлами 53
Просмотр списка управляемых сетевых узлов 54
Просмотр и изменение основных параметров сетевого узла 56

Глава 7. Управление подразделениями 57
Назначение подразделений 58
Создание подразделения 59
Просмотр и изменение основных параметров подразделения 60
Добавление сетевых узлов в подразделение 61
Добавление в подразделение одного сетевого узла 61
Добавление в подразделение нескольких сетевых узлов 62
Удаление подразделения 64

Глава 8. Управление шаблонами политики безопасности 65
Общие сведения о шаблонах политики безопасности 66
Работа с группами объектов 68
Системные группы объектов 69
Создание и изменение групп объектов 70
Добавление сетевых узлов 74
Добавление IP-адресов и DNS-имен 75
Добавление идентификатора сетевого интерфейса 76
Добавление протоколов 77
Добавление расписаний 78
Вложенность групп объектов 79
Создание шаблона политики безопасности 80

Просмотр и изменение сетевых фильтров, заданных в шаблоне 81
Создание сетевых фильтров 82
Создание локальных фильтров открытой сети 83
Создание транзитных фильтров открытой сети 86
Создание фильтров для туннелируемых узлов 88
Создание фильтров защищенной сети 90
Рекомендации по созданию сетевых фильтров 92
Просмотр и изменение правил трансляции IP-адресов, заданных в шаблоне 93
Создание и изменение правила трансляции IP-адресов 94
Копирование шаблона политики безопасности 97
Удаление шаблона политики безопасности 98
Назначение шаблона сетевым узлам и подразделениям 99
Назначение шаблона одному сетевому узлу 99
Назначение шаблона нескольким сетевым узлам 100
Назначение шаблона одному подразделению 101
Назначение шаблона нескольким подразделениям 103

Глава 9. Рассылка политик безопасности на сетевые узлы 104
Правила формирования результирующей политики безопасности 105
Отправка и получение политик безопасности 107
Применение политик безопасности на сетевых узлах 108
Просмотр результирующей политики безопасности 109
Выборочная рассылка 111
Групповая рассылка 112
Журнал отправки и применения политик безопасности 113

Глава 10. Аудит действий пользователей 115
Работа в программе с полномочием «Аудит» 116
Просмотр журнала событий 117

Приложение A. Установка Microsoft SQL Server 119

Приложение B. Региональные настройки 122
Региональные настройки в ОС Windows 7, Server 2008 R2 123
Региональные настройки в ОС Windows 8, Server 2012, Windows 8.1, Server 2012 R2, Windows 10 127

Приложение C. История версий 131
Новые возможности версии 4.3.2 131
Новые возможности версии 4.3.1 132

Новые возможности версии 4.2 ... 132
Новые возможности версии 4.1 ... 132
Новые возможности версии 4.0 ... 133

Приложение D. Глоссарий ... 136

Приложение E. Указатель ... 139

Введение

О документе 8

О программе 9

Системные требования 11

Комплект поставки 13

Обратная связь 14

О документе

Для кого предназначен документ

Документ предназначен для администраторов, осуществляющих управление политиками безопасности сетевых узлов ViPNet с помощью программы ViPNet Policy Manager. В нем приведена информация об установке программы, предоставляемых ею возможностях, а также краткие указания для быстрого начала работы. Документ также содержит общие сведения о принципах организации управления политиками безопасности.

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.
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 Policy Manager используется в сетях ViPNet, управляемых с помощью ПО ViPNet Administrator или ПО ViPNet Network Manager. Она предназначена для централизованного управления политиками безопасности (см. глоссарий, стр. 137) узлов защищенной сети ViPNet. Программа ViPNet Policy Manager позволяет задавать различные политики безопасности как для отдельных сетевых узлов, так и для групп узлов и централизованно рассылать их на сетевые узлы.

Сведения об управляемых сетевых узлах и другая необходимая информация (учетные записи пользователей, политики безопасности и так далее) хранится в базе данных на SQL-сервере. Для создания базы данных необходимо наличие развернутого SQL-сервера, который может быть установлен на одном компьютере вместе с ViPNet Policy Manager или на отдельном компьютере. База данных создается автоматически при установке ПО ViPNet Policy Manager.

Новые возможности версии 4.3.3

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Policy Manager версии 4.3.3.

Информация об изменениях в предыдущих версиях содержится в приложении История версий (на стр. 131).

- **Копирование шаблона политики безопасности**

  Теперь, когда вам нужно создать несколько однотипных шаблонов политики безопасности с небольшими отличиями в составе шаблона или настройках, вы можете быстро создавать шаблоны на основе существующих с помощью функции копирования (см. «Копирование шаблона политики безопасности» на стр. 97).

- **Использование идентификатора интерфейса координатора с ПО ViPNet Coordinator for Linux при настройке параметров сетевых фильтров**

  Раньше при создании группы объектов или при настройке параметров сетевых фильтров для интерфейсов координаторов с ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW вы могли использовать только IP-адреса сетевых интерфейсов.

  Теперь в качестве объектов, используемых в сетевых фильтрах, вы также можете указывать идентификаторы интерфейсов (см. «Добавление идентификатора сетевого интерфейса» на стр. 76). Поскольку идентификаторы интерфейсов в отличие от IP-адресов не должны быть уникальными, этот тип объектов удобно использовать, когда в вашей сети используется несколько координаторов с ПО ViPNet Coordinator for Linux или ПАК ViPNet Coordinator HW, имеющих однотипные идентификаторы интерфейсов. В таком случае, например для шести координаторов при настройке параметров сетевого фильтра вам достаточно будет указать в качестве объекта только один идентификатор интерфейса вместо шести IP-адресов.

- **Исправление ошибок**

  Были исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Системные требования

Требования к компьютеру для установки ViPNet Policy Manager:

- 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 ОС Windows — не менее 2 Гбайт).
- Свободное место на жестком диске — не менее 250 Мбайт.
- Сетевой адаптер или модем.
- Операционная система — Windows Server 2008 R2 (64 разрядная), Windows Small Business Server 2008 SP2 (64-разрядная), Windows 7 (32/64 разрядная), Windows 8 (32/64 разрядная), Windows 8.1 (32/64 разрядная), Windows Small Business Server 2011 (64-разрядная), Windows Server 2012 (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 6.0 или выше.

Для установки и нормального функционирования ViPNet Policy Manager на компьютере предварительно должны быть установлены следующие приложения:

- ViPNet Client версии 4.0 или выше.
- Microsoft SQL Server (см. «Требования к SQL-серверу для развертывания базы данных» на стр. 11).

Требования к SQL-серверу для развертывания базы данных

Программа ViPNet Policy Manager использует для хранения необходимой информации базу данных, развернутую на SQL-сервере одной из следующих версий:

- Microsoft SQL Server 2008 R2 SP1
- Microsoft SQL Server 2012 SP1
- Microsoft SQL Server 2014 SP1

Редакция SQL-сервера может быть любой, в том числе Express Edition.

Примечание. Операционная система Windows 10 не поддерживает Microsoft SQL Server 2008 R2 SP1.

Совместимость с ПО ViPNet

Вы можете использовать программу ViPNet Policy Manager в сети ViPNet под управлением ПО следующих версий:

- ViPNet Administrator версии 4.4 и выше.
- ViPNet Network Manager версии 4.5 и выше.

Прием политик безопасности, сформированных в текущей версии программы ViPNet Policy Manager, поддерживается на сетевых узлах, на которых установлено одно из следующих ПО ViPNet:

- ViPNet Client for Windows версии 4.0 и выше;
- ViPNet Coordinator for Windows версии 4.0 и выше;
- ViPNet Coordinator HW версии 4.1 и выше;
- ViPNet Coordinator for Linux версии 4.0 и выше.

Комплект поставки

В комплект поставки ПО ViPNet Policy Manager входит:

- Файл установки.
- Документ в формате PDF «ViPNet Policy Manager. Руководство администратора».

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 http://www.infotecs.ru/products/line/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet http://www.infotecs.ru/forum.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.

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 http://www.infotecs.ru/support/request/.
- Регистрация продуктов и консультации по телефону для клиентов, имеющих расширенный уровень технического сопровождения:

  8 (495) 737-6196,

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

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

1

Общие сведения

Принципы централизованного управления политиками безопасности сетевых узлов 16

Основные возможности ViPNet Policy Manager 18

Лицензирование ViPNet Policy Manager 20

Принципы централизованного управления политиками безопасности сетевых узлов

Программа ViPNet Policy Manager предназначена для организации в сети ViPNet централизованного управления политиками безопасности сетевых узлов (см. глоссарий, стр. 137). Она устанавливается на один из узлов сети ViPNet, который будет использоваться в качестве центра управления. Список узлов, управляемых с помощью ViPNet Policy Manager, задается в программе ViPNet Центр управления сетью (далее — ЦУС) и может включать в себя узлы только той сети ViPNet, к которой принадлежит сетевой узел с ViPNet Policy Manager.

ViPNet Policy Manager позволяет централизованно управлять политиками безопасности узлов, на которых установлено ПО ViPNet с функцией защиты трафика (см. «Совместимость с ПО ViPNet» на стр. 12). На схеме ниже представлена схема организации централизованного управления политиками безопасности.

Рисунок 1. Схема организации централизованного управления политиками безопасности

Управление политиками безопасности осуществляется с помощью шаблонов, назначаемых управляемым сетевым узлам (см. глоссарий, стр. 138). Шаблон политики безопасности представляет собой именованный набор параметров безопасности и может содержать сетевые фильтры и правила трансляции IP-адресов. Для удобства управления узлы можно объединять в подразделения (см. глоссарий, стр. 137) и назначать шаблоны как отдельным узлам, так и подразделениям.

На основе шаблонов, назначенных узлам и подразделениям, формируются результирующие политики безопасности (см. глоссарий, стр. 137) для отправки на сетевые узлы. При формировании учитывается приоритет (порядок следования) шаблонов и автоматически исключаются повторы одного и того же шаблона. Рассылка результирующих политик на узлы происходит с помощью транспортного модуля MFTP (см. глоссарий, стр. 138). Транспортный модуль MFTP является частью

программного обеспечения ViPNet Client, которое должно быть установлено на компьютере вместе с программой ViPNet Policy Manager (см. «Системные требования» на стр. 11).

Политики безопасности, сформированные в программе ViPNet Policy Manager и полученные на управляемых узлах, имеют приоритет над политиками, заданными на самих узлах. Это означает, что все сетевые фильтры из присланной политики размещаются перед аналогичными фильтрами, заданными на узле. Полученная в результате текущая политика безопасности действительна для всех пользователей, зарегистрированных на узле, и всех конфигураций ПО ViPNet, установленного на узле.

На рисунке ниже представлена схема информационного взаимодействия различных узлов в процессе управления политиками безопасности:

1 Список узлов, управляемых с помощью ViPNet Policy Manager, может быть обновлен в ЦУСе и отправлен на сетевой узел с ViPNet Policy Manager в составе обновления справочников (см. глоссарий, стр. 137). В этом случае список управляемых узлов автоматически обновляется в ViPNet Policy Manager согласно новому списку узлов.

2 Политики безопасности, сформированные в ViPNet Policy Manager, рассылаются на сетевые узлы (см. «Отправка и получение политик безопасности» на стр. 107).

3 Каждый сетевой узел, получивший политику безопасности, пытается ее применить, после чего формирует и отправляет на сетевой узел с ViPNet Policy Manager квитанцию с результатом применения политики. Политика может быть применена или отклонена (см. «Журнал отправки и применения политик безопасности» на стр. 113).

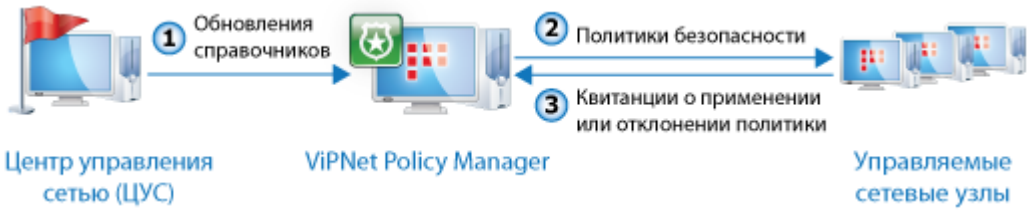

Рисунок 2. Схема взаимодействия сетевых узлов ViPNet в процессе управления политиками безопасности

Основные возможности ViPNet Policy Manager

Программа ViPNet Policy Manager предоставляет администраторам сети ViPNet следующие основные возможности:

- **Объединение сетевых узлов в подразделения и управление подразделениями**

  Сетевые узлы, к которым должна применяться одинаковая политика безопасности, можно объединять в подразделения (см. глоссарий, стр. 137). Формирование общей политики безопасности для таких узлов происходит путем назначения шаблонов не отдельным узлам, а всему подразделению. Это позволяет упростить управление политикой безопасности в сетях с большим количеством узлов. Для управления подразделениями предоставляются все необходимые функции: создание, удаление, изменение списка узлов, входящих в подразделение.

- **Управление шаблонами политики безопасности**

  Шаблоны (см. глоссарий, стр. 138) являются основным средством для задания политики безопасности. Они могут содержать сетевые фильтры и правила трансляции IP-адресов. Для управления шаблонами предусмотрены все необходимые функции: создание, настройка и удаление шаблонов.

- **Назначение шаблонов политики безопасности узлам и подразделениям в заданном порядке**

  Управление политиками безопасности сетевых узлов осуществляется путем назначения шаблонов отдельным узлам или подразделениям. Шаблон, назначенный подразделению, распространяется на все узлы, входящие в состав этого подразделения. Набор шаблонов для каждого узла состоит из шаблонов, назначенных самому узлу и подразделениям, в которые он входит. От порядка следования шаблонов зависит приоритет применения на узле параметров безопасности, заданных в шаблонах: приоритет уменьшается от первого в списке шаблона к последнему. Последовательность шаблонов можно изменять как для отдельного узла, так и в рамках подразделения.

- **Рассылка результирующих политик безопасности на сетевые узлы**

  Результирующая политика безопасности (см. глоссарий, стр. 137) сетевого узла представляет собой результат объединения шаблонов, назначенных узлу и подразделениям, в которые входит узел. Она формируется автоматически при отправке политики безопасности на узел. При формировании политики безопасности учитывается приоритет шаблонов и исключаются повторы одного и того же шаблона.

  Рассылку результирующих политик безопасности на сетевые узлы можно осуществлять выборочно (на отдельные узлы) или на все узлы подразделения (групповая рассылка). Результирующая политика отправляется в виде файла формата XML, защищенного контрольной суммой.

- **Контроль за отправкой и применением политик безопасности на сетевых узлах**

Все события, связанные с отправкой политик безопасности на сетевые узлы и их применением на узлах, записываются в журнал, который доступен для просмотра. Журнал предназначен для контроля за получением на узлах политик безопасности, отправленных из программы ViPNet Policy Manager, и за историей их применения на узлах. Для удобства просмотра можно отфильтровать события по заданным параметрам.

- **Управление учетными записями пользователей**

  Учетные записи содержат имена, пароли, персональные данные и роли пользователей программы ViPNet Policy Manager. Имя и пароль используются для аутентификации пользователя. Роли пользователя определяют действия, которые он может выполнять в программе. Для управления учетными записями предусмотрены все необходимые функции: создание, изменение и удаление.

- **Управление ролями пользователей**

  Роли пользователей (см. глоссарий, стр. 137) используются для разграничения полномочий пользователей программы ViPNet Policy Manager. Каждая роль представляет собой набор полномочий из числа допустимых и разрешает пользователям только те действия, которые предусмотрены этими полномочиями. В ViPNet Policy Manager имеется ряд предустановленных ролей пользователей. Также можно создавать свои роли пользователей, изменять их и удалять.

- **Аудит действий пользователей**

  Действия пользователей в программе ViPNet Policy Manager регистрируются в журнале событий, который можно использовать для аудита. В журнал записываются события входа в программу и выхода из программы, действия пользователей с различными объектами, факты отправки политики безопасности на сетевые узлы. При просмотре журнала можно отфильтровать события по заданным параметрам.

Лицензирование ViPNet Policy Manager

Внимание! В данном разделе используется терминология, принятая в программе ViPNet Центр управления сетью (ЦУС) версии 4.0 или выше. Начиная с указанной версии, термин «прикладная задача» изменен на термин «роль», а название прикладной задачи «Центр управления политиками» изменено на «Policy Manager».

Учитывайте эти изменения, если в вашей сети установлен ЦУС более ранней версии.

Работа с программой ViPNet Policy Manager возможна только на сетевом узле с ролью «Policy Manager». Чтобы добавить эту роль на сетевой узел, выполните следующие действия:

1. Убедитесь, что ваша лицензия на сеть ViPNet разрешает использование программы ViPNet Policy Manager. В противном случае обратитесь к представителю ОАО «ИнфоТеКС» для обновления лицензии, сообщив номер вашей сети ViPNet.
2. В программе ViPNet Центр управления роль «Policy Manager» автоматически добавляется на сетевой узел, который является Центром управления сетью.

   В программе ViPNet Network Manager разрешите использование ViPNet Policy Manager для любого клиента типа Client Windows.

   Примечание. В программе ViPNet Центр управления сетью версии 4.1 и ниже (см. «Совместимость с ПО ViPNet» на стр. 12) вы могли назначить роль «Policy Manager» любому клиенту вашей сети.

3. Задайте список узлов вашей сети, для которых вы сможете формировать политики безопасности в программе ViPNet Policy Manager:
   - В программе ViPNet Центр управления сетью задайте список управляемых узлов в свойствах роли «Policy Manager».
   - В программе ViPNet Network Manager задайте список управляемых узлов на панели свойств клиента, для которого разрешено использование ViPNet Policy Manager.

   Примечание. Связи между сетевым узлом с ролью «Policy Manager» и управляемыми сетевыми узлами будут созданы автоматически.

Наличие роли на сетевом узле проверяется при запуске программы ViPNet Policy Manager по справочникам, имеющимся на сетевом узле после установки ПО ViPNet Client. В случае успешного запуска программы в списке управляемых узлов будут присутствовать узлы, заданные в ЦУСе (см. «Просмотр списка управляемых сетевых узлов» на стр. 54).

2

Установка, обновление и удаление ViPNet Policy Manager

Последовательность действий при установке ViPNet Policy Manager 22

Информация для администратора SQL 23

Установка ViPNet Policy Manager 24

Обновление ViPNet Policy Manager 26

Удаление ViPNet Policy Manager 27

Последовательность действий при установке ViPNet Policy Manager

Чтобы установить программу ViPNet Policy Manager и компоненты, необходимые для работы программы, выполните действия из приведенного ниже списка.

Таблица 3. Установка ViPNet Policy Manager

	Действие	Ссылка
☐	Если сервер базы данных должен находиться на одном компьютере с ViPNet Policy Manager, установите программное обеспечение Microsoft SQL Server. Вы можете использовать ранее установленное программное обеспечение Microsoft SQL Server. Например, SQL-сервер, который используется для хранения данных ПО ViPNet Administrator или ViPNet Network Manager.	Требования к SQL-серверу для развертывания базы данных (на стр. 11) Установка Microsoft SQL Server (на стр. 119)
☐	Установите на компьютер программу ViPNet Client (версии 4.0 или выше) и дистрибутив ключей сетевого узла ViPNet с добавленной ролью «Policy Manager».	См. документ «ViPNet Client Монитор. Руководство пользователя»
☐	Установите программу ViPNet Policy Manager.	Установка ViPNet Policy Manager (на стр. 24)

Совет. Мы рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Информация для администратора SQL

При первой установке программы ViPNet Policy Manager на SQL-сервере, указанном в процессе установки, автоматически создается база данных, которая предназначена для хранения всей необходимой информации. Параметры созданной базы данных приведены в таблице ниже.

Таблица 4. Параметры базы данных

Параметр	Значение параметра
Параметры сортировки (collation)	Cyrillic_General_CI_AS
Модель восстановления (recovery model)	Full

Внимание! Не рекомендуется изменять настройки базы данных и осуществлять какие-либо действия по управлению структурой и информацией непосредственно в базе данных ViPNet Policy Manager. Подобные действия могут привести к серьезным неполадкам в работе ПО ViPNet Policy Manager. ОАО «ИнфоТеКС» не несет ответственности за ошибки, возникшие вследствие подобных действий.

Установка ViPNet Policy Manager

Внимание! При установке ViPNet Policy Manager на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе программы измените региональные настройки Windows (см. «Региональные настройки» на стр. 122).

Для установки ViPNet Policy Manager выполните следующие действия:

1 Запустите файл установки . Дождитесь завершения подготовки к установке ViPNet Policy Manager.

2 Следуйте указаниям программы установки ViPNet Policy Manager.

3 На странице **Установка базы на Microsoft SQL Server** укажите экземпляр SQL-сервера, имя базы данных и способ аутентификации при подключении к SQL-серверу. При выборе способа аутентификации **Встроенная в SQL Server** также укажите имя пользователя и пароль.

По умолчанию экземпляр SQL-сервера: `.\SQLEXPRESS`, имя базы данных: `ViPNetPolicyManager`, способ аутентификации: `Аутентификация Windows`. Данные для подключения к SQL-серверу, а также имя пользователя и пароль вы можете узнать у администратора SQL-сервера.

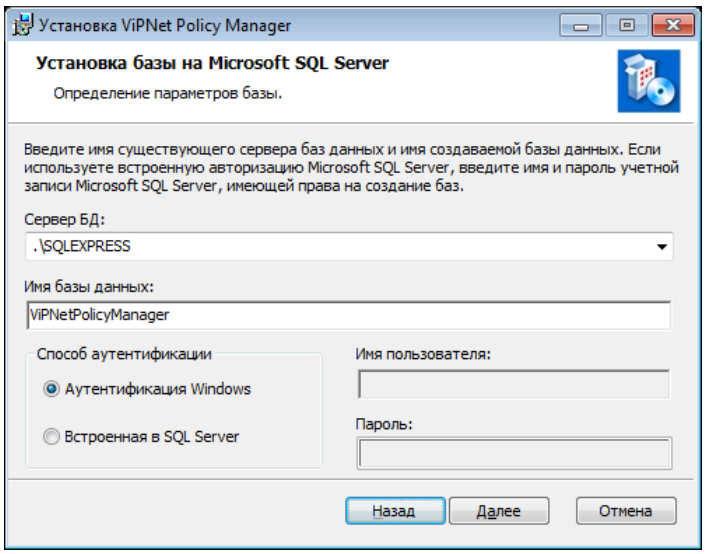

Рисунок 3. Создание базы данных

Для продолжения нажмите кнопку **Далее**.

4 Если это не первая установка программы ViPNet Policy Manager на компьютер, появится сообщение о том, что база данных уже существует. Вы можете использовать эту базу данных или создать новую под тем же именем (перезаписать).

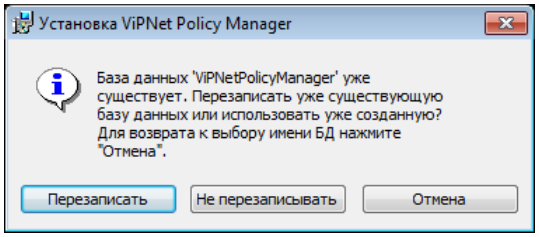

Рисунок 4. Перезапись существующей базы данных

Чтобы создать новую базу данных, нажмите кнопку **Перезаписать**, чтобы использовать существующую — кнопку **Не перезаписывать**.

5 Дождитесь окончания установки, затем нажмите кнопку **Готово**. Программа ViPNet Policy Manager готова к использованию.

Обновление ViPNet Policy Manager

Примечание. При обновлении сохраняется база данных, используемая в текущей версии программы ViPNet Policy Manager, и вся хранящаяся в ней информация. Если вы хотите создать новую базу данных, сначала удалите текущую версию программы вместе с базой данных (см. «Удаление ViPNet Policy Manager» на стр. 27), а затем установите новую версию.

Для обновления ViPNet Policy Manager вам потребуется файл установки с новой версией программы.

Чтобы обновить версию программы ViPNet Policy Manager, выполните следующие действия:

1. Завершите работу программы ViPNet Policy Manager.
2. Запустите файл установки . Дождитесь завершения подготовки к установке ViPNet Policy Manager.
3. Следуйте указаниям программы установки ViPNet Policy Manager.
4. Дождитесь окончания установки, затем нажмите кнопку **Готово**. Новая версия программы ViPNet Policy Manager готова к использованию.

Удаление ViPNet Policy Manager

При необходимости вы можете удалить с компьютера программу ViPNet Policy Manager, а также удалить с SQL-сервера используемую программой базу данных.

Внимание! Если программа ViPNet Policy Manager и сервер базы данных находятся на разных компьютерах, вы не сможете удалить базу данных с помощью файла установки ViPNet Policy Manager. В этом случае следует удалить базу данных вручную средствами SQL-сервера.

Выполните следующие действия:

1 Завершите работу программы ViPNet Policy Manager.

2 Запустите файл установки . Дождитесь завершения подготовки к удалению ViPNet Policy Manager.

3 На странице выбора операции, которую следует выполнить, нажмите кнопку **Удалить**.

4 На странице готовности к удалению установите флажок **Удалить созданную базу данных**, если вместе с программой вы хотите удалить базу данных.

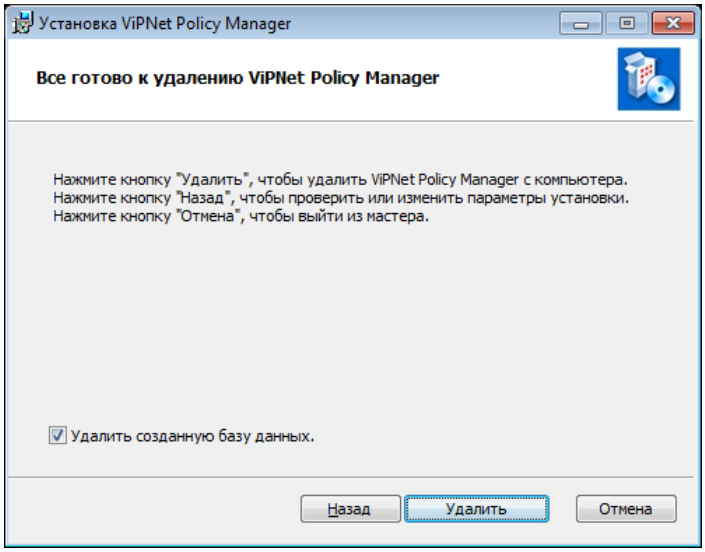

Рисунок 5. Удаление программы

5 Для продолжения нажмите кнопку **Удалить**.

6 Дождитесь завершения удаления. После удаления программы перезагрузка компьютера не требуется.

Примечание. Вы также можете удалить программу, выбрав **Все программы** > **ViPNet** > **ViPNet Policy Manager** > **Удалить** в меню **Пуск**. Однако при удалении программы этим способом нельзя удалить базу данных.

3

Запуск и завершение работы с ViPNet Policy Manager

Запуск программы 29

Интерфейс программы 30

Завершение работы с программой 32

Запуск программы

Чтобы запустить программу ViPNet Policy Manager:

1 Выполните одно из действий:

- Если вы используете операционную систему Windows 7, Windows Server 2008 R2 или более ранней версии, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Policy Manager** > **ViPNet Policy Manager** (во время установки положение программы в меню **Пуск** могло быть изменено).
- Если вы используете операционную систему Windows 8 или Windows Server 2012, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Policy Manager**.

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

Откроется окно входа в программу.

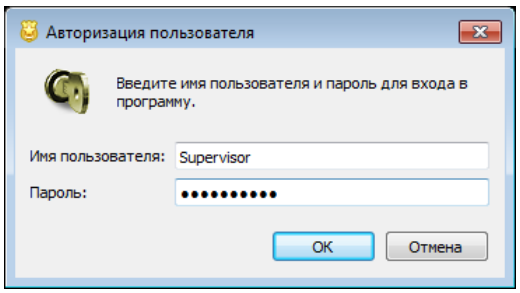

Рисунок 6. Окно входа в программу

2 В окне **Авторизация пользователя** введите имя и пароль пользователя.

Примечание. Для первого после установки входа в программу введите имя **Supervisor** и пароль **Supervisor**.

3 Нажмите кнопку **OK**.

В случае успешной аутентификации пользователя откроется главное окно программы (см. «Интерфейс программы» на стр. 30). В заголовке окна в скобках будет указано имя пользователя.

Если это первый после установки вход в программу, то сначала появится сообщение о необходимости смены пароля пользователя **Supervisor**. Это сообщение также будет появляться при входе в программу под именем **Supervisor** до тех пор, пока не будет изменен пароль.

Интерфейс программы

На рисунке ниже представлен интерфейс программы ViPNet Policy Manager.

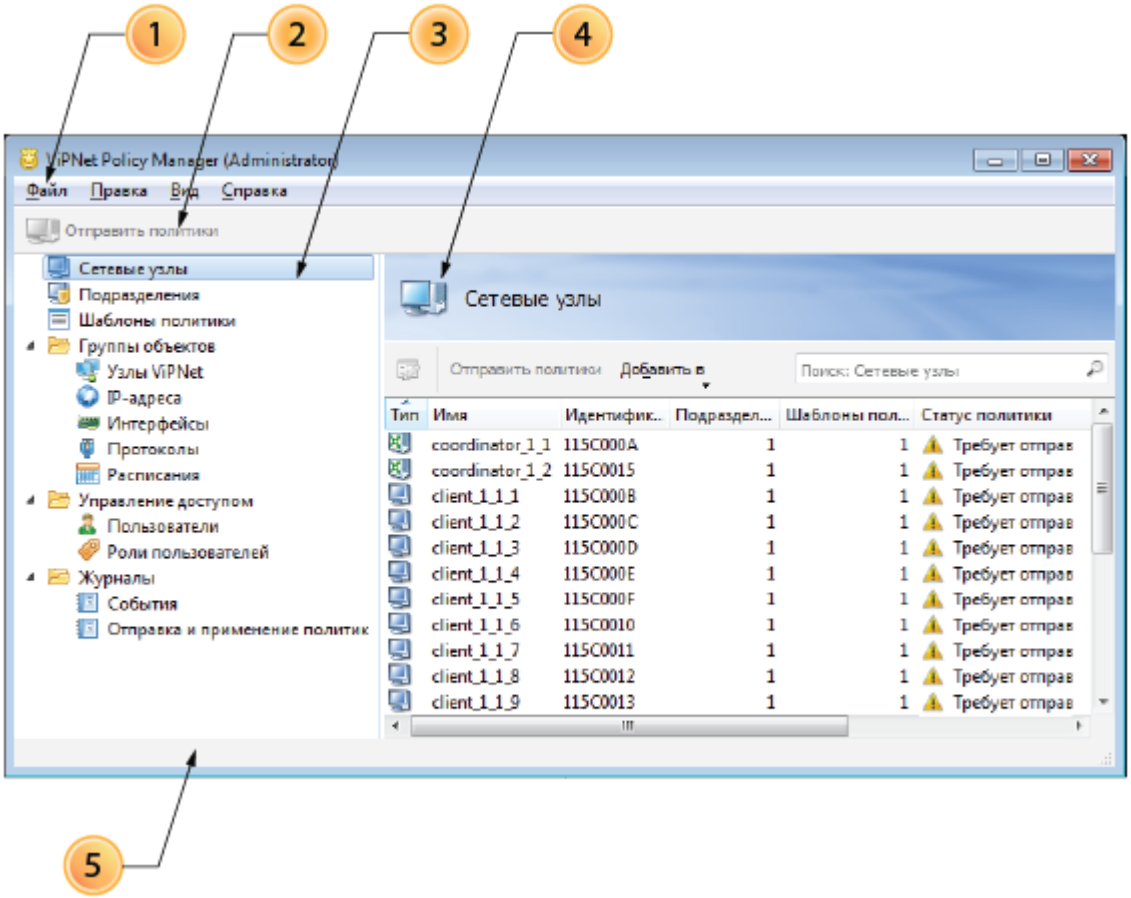

Рисунок 7. Интерфейс программы

На рисунке цифрами обозначены следующие элементы интерфейса:

1 Главное меню программы. Предоставляет доступ к различным функциям программы.

2 Панель инструментов. Содержит кнопку **Отправить политики** для отправки политик безопасности на сетевые узлы. Чтобы отобразить или скрыть панель инструментов, в меню **Вид** щелкните пункт **Панель инструментов**.

3 Панель навигации. Содержит перечень следующих разделов:

- **Сетевые узлы** — содержит список сетевых узлов, управляемых с помощью ViPNet Policy Manager (см. «Просмотр списка управляемых сетевых узлов» на стр. 54).
- **Подразделения** — предназначен для управления подразделениями, в которые объединены сетевые узлы (см. «Управление подразделениями» на стр. 57).
- **Шаблоны политики** — предназначен для управления шаблонами политики безопасности (см. «Управление шаблонами политики безопасности» на стр. 65).

- **Группы объектов** — включает в себя подразделы со списками групп объектов, предназначенных для подстановки в сетевые фильтры и правила трансляции адресов (см. «Работа с группами объектов» на стр. 68).
- **Управление доступом** — включает в себя подразделы для управления доступом и полномочиями пользователей программы:
  - **Пользователи** — предназначен для управления учетными записями пользователей (см. «Управление учетными записями» на стр. 45).
  - **Роли пользователей** — предназначен для управления ролями пользователей (см. «Управление ролями пользователей» на стр. 49).
- **Журналы** — включает в себя подразделы для просмотра журналов:
  - **События** — предназначен для просмотра журнала событий (см. «Просмотр журнала событий» на стр. 117).
  - **Отправка и применение политик** — предназначен для просмотра журнала отправки и применения на сетевых узлах политик безопасности (см. «Журнал отправки и применения политик безопасности» на стр. 113).

Примечание. Для перехода к нужному разделу выберите его на панели навигации или щелкните в меню **Вид** соответствующий пункт.

---

4 Панель просмотра. Служит для отображения списка элементов раздела или подраздела, выбранного на панели навигации (3).

5 Строка состояния. Служит для отображения сообщений. Чтобы отобразить или скрыть строку состояния, в меню **Вид** щелкните пункт **Строка состояния**.

Завершение работы с программой

Чтобы завершить работу с программой ViPNet Policy Manager:

1 Выполните одно из действий:

- В главном окне программы в меню **Файл** выберите пункт **Выход**.
- В правом верхнем углу главного окна нажмите кнопку .

2 При наличии неотправленных политик безопасности появится сообщение об этом.

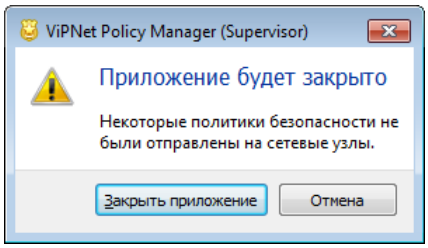

Рисунок 8. Закрытие программы

Чтобы завершить работу, несмотря на сообщение, нажмите кнопку **Закрыть приложение**. Неотправленные политики безопасности можно будет отправить на сетевые узлы в следующем сеансе работы с программой.

Примечание. Если база данных программы расположена на удаленном SQL-сервере, то в случае отсутствия соединения с сервером при выполнении операции, требующей обращения к базе данных, появится сообщение о невозможности выполнить операцию, и программа автоматически завершит свою работу.

4

Быстрый старт

Начало работы 34

Как сменить пароль встроенной учетной записи 36

Как создать подразделение 37

Как создать шаблон политики безопасности 38

Как назначить шаблон политики безопасности сетевым узлам или подразделениям 39

Как отправить политики безопасности на сетевые узлы 40

Как посмотреть журнал отправки и применения политик безопасности 41

Как создать учетную запись 42

Начало работы

Этот раздел содержит краткие указания для начала работы с программой ViPNet Policy Manager. Приведенная информация поможет приступить к работе без подробного изучения данного руководства.

Для начала работы запустите программу ViPNet Policy Manager (см. «Запуск программы» на стр. 29). Первый запуск программы возможен только под встроенной учетной записью с именем **Supervisor** и паролем **Supervisor**. После входа в программу смените пароль пользователя **Supervisor** (см. «Как сменить пароль встроенной учетной записи» на стр. 36).

Пользователь **Supervisor** имеет все полномочия, то есть может работать с любыми объектами. За подробной информацией о полномочиях пользователей обратитесь к разделу Разграничение полномочий на основе ролей пользователей (на стр. 44).

В таблице ниже приведен порядок работы с программой ViPNet Policy Manager сразу после установки. Этот порядок подразумевает работу одного пользователя **Supervisor**, имеющего максимальные полномочия. Если с программой будут работать несколько пользователей с разными полномочиями, то каждый из них сможет выполнять только те действия, которые ему разрешены. Например, функции по управлению шаблонами и по назначению шаблонов сетевым узлам могут быть разделены между пользователями. В этом случае сначала один пользователь создает нужные шаблоны, затем другой пользователь назначает шаблоны сетевым узлам.

Таблица 5. Порядок действий для начала работы

	Действие	Ссылка
☐	Запустите ViPNet Policy Manager под учетной записью **Supervisor** и смените пароль этой учетной записи.	Как сменить пароль встроенной учетной записи (на стр. 36)
☐	Создайте подразделения для объединения сетевых узлов с одинаковой политикой безопасности (если в сети есть такие узлы).	Как создать подразделение (на стр. 37)
☐	Создайте шаблон (шаблоны), реализующий требуемую политику безопасности.	Как создать шаблон политики безопасности (на стр. 38)
☐	Назначьте шаблон политики безопасности сетевым узлам.	Как назначить шаблон политики безопасности сетевым узлам или подразделениям (на стр. 39)
☐	Отправьте политики безопасности на сетевые узлы.	Как отправить политики безопасности на сетевые узлы (на стр. 40)
☐	С помощью журнала проконтролируйте получение и применение политик безопасности на сетевых узлах.	Как посмотреть журнал отправки и применения политик безопасности (на стр. 41)

	Действие	Ссылка
☐	Создайте, если это необходимо, учетные записи пользователей с нужными полномочиями.	Как создать учетную запись (на стр. 42)

Как сменить пароль встроенной учетной записи

Чтобы сменить пароль встроенной учетной записи, выполните следующие действия:

1. В окне программы ViPNet Policy Manager в меню **Файл** выберите пункт **Сменить пароль пользователя**.
2. В окне **Смена пароля пользователя** в поле **Текущий пароль** введите **Supervisor**, затем в соответствующих полях введите и подтвердите новый пароль.
3. Нажмите кнопку **Сменить пароль**. Для следующего входа в программу под именем **Supervisor** используйте новый пароль.

Как создать подразделение

Чтобы создать подразделение (см. глоссарий, стр. 137), выполните следующие действия:

1 Запустите программу ViPNet Policy Manager под учетной записью, имеющей полномочие **Управление подразделениями**.

2 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.

> **Примечание.** В списке подразделений на панели просмотра будет присутствовать подразделение с именем **Сетевые узлы**. Это подразделение всегда находится наверху иерархии подразделений, и в нем по умолчанию размещаются подразделения, создаваемые пользователями.

3 На панели просмотра нажмите кнопку **Создать**.

4 В окне **Свойства подразделения** задайте параметры нового подразделения:

- В разделе **Основные параметры** задайте имя и описание подразделения.
- В разделе **Сетевые узлы** с помощью кнопки **Добавить** сформируйте список сетевых узлов подразделения.
- В разделе **Шаблоны политик** с помощью кнопки **Добавить** сформируйте список шаблонов политики безопасности, назначенных подразделению.

> **Примечание.** До создания собственных шаблонов политики безопасности подразделению можно назначить только типовые шаблоны, входящие в состав ViPNet Policy Manager.

5 В окне **Свойства подразделения** нажмите кнопку **OK**. В иерархии подразделений появится новое подразделение, в которое будут включены выбранные узлы и назначены выбранные шаблоны.

> **Примечание.** Первое созданное подразделение размещается в корневом подразделении **Сетевые узлы**, содержащем все управляемые сетевые узлы. При создании следующих подразделений можно указать их место в иерархии, выбрав одно из существующих подразделений.

После создания подразделения и назначения ему шаблонов можно отправить политику безопасности на все узлы подразделения (см. «Как отправить политики безопасности на сетевые узлы» на стр. 40). Работа с подразделениями подробно описана в главе Управление подразделениями (на стр. 57).

Как создать шаблон политики безопасности

В общем случае шаблон политики безопасности может содержать несколько сетевых фильтров и правил трансляции IP-адресов. Подробнее о возможных компонентах шаблона см. раздел Общие сведения о шаблонах политики безопасности (на стр. 66). Далее приводится пример создания простого шаблона с одним фильтром, который разрешает любые соединения со всеми защищенными узлами.

Чтобы создать такой шаблон политики безопасности, выполните следующие действия:

1. Запустите программу ViPNet Policy Manager под учетной записью, имеющей полномочие **Управление шаблонами**.
2. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.
3. На панели просмотра нажмите кнопку **Создать**.
4. В окне **Свойства шаблона политики** выберите раздел **Основные параметры** и задайте имя и описание нового шаблона.
5. В окне **Свойства шаблона политики** выберите раздел **Фильтры защищенной сети** и добавьте в шаблон фильтр:
   - **5.1** Нажмите кнопку **Создать**.
   - **5.2** В окне **Свойства фильтра защищенной сети** задайте имя фильтра и установите переключатель **Действие** в положение **Пропускать трафик**.
   - **5.3** Нажмите кнопку **OK**.
6. В окне **Свойства шаблона политики** нажмите кнопку **OK**. В списке шаблонов появится новый шаблон, содержащий заданный фильтр.

Созданный шаблон политики безопасности можно назначить отдельным сетевым узлам или подразделениям (см. «Как назначить шаблон политики безопасности сетевым узлам или подразделениям» на стр. 39). Подробные сведения о шаблонах содержатся в главе Управление шаблонами политики безопасности (на стр. 65).

Как назначить шаблон политики безопасности сетевым узлам или подразделениям

Чтобы назначить шаблон политики безопасности отдельным сетевым узлам или подразделениям, выполните следующие действия:

1. Запустите программу ViPNet Policy Manager под учетной записью, имеющей полномочие **Назначение шаблонов**.
2. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.
3. На панели просмотра выберите шаблон и нажмите кнопку **Свойства** или дважды щелкните шаблон.
4. Чтобы назначить шаблон сетевым узлам:
   - **4.1** В окне **Свойства шаблона политики** на левой панели выберите раздел **Сетевые узлы** и нажмите кнопку **Добавить**.
   - **4.2** Выберите в списке один или несколько узлов и нажмите кнопку **OK**.
5. Чтобы назначить шаблон подразделениям:
   - **5.1** В окне **Свойства шаблона политики** на левой панели выберите раздел **Подразделения**.
   - **5.2** Установите флажки напротив тех подразделений, которым требуется назначить шаблон.
6. Чтобы сохранить список узлов и подразделений, которым назначен шаблон, нажмите кнопку **OK**.

После назначения шаблона сетевым узлам и (или) подразделениям можно отправить политики безопасности на сетевые узлы (см. «Как отправить политики безопасности на сетевые узлы» на стр. 40).

Как отправить политики безопасности на сетевые узлы

Чтобы отправить политики безопасности на отдельные сетевые узлы, выполните следующие действия:

1. Запустите программу ViPNet Policy Manager под учетной записью, имеющей полномочие **Отправка политик**.
2. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Сетевые узлы**.
3. На панели просмотра выберите один или несколько узлов со статусом политики безопасности **Требует отправки**.
4. Нажмите кнопку **Отправить политики**.
5. В окне **Отправка политики** задайте время применения политик на узлах и нажмите кнопку **OK**. Политики безопасности будут отправлены на выбранные узлы и применены в указанное время.

Политики безопасности можно отправить сразу на все узлы подразделения. Для этого:

1. Запустите программу ViPNet Policy Manager под учетной записью, имеющей полномочие **Отправка политик**.
2. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.
3. На панели просмотра выберите одно или несколько подразделений или выберите **Сетевые узлы**.
4. Нажмите кнопку **Отправить политики**.
5. В окне **Отправка политики** задайте время применения политик на узлах и нажмите кнопку **OK**. Политики безопасности будут отправлены на узлы выбранных подразделений (или на все управляемые узлы) и применены в указанное время.

Подробнее об отправке политик на сетевые узлы см. главу Рассылка политик безопасности на сетевые узлы (на стр. 104).

Как посмотреть журнал отправки и применения политик безопасности

Чтобы посмотреть журнал отправки и применения политик безопасности, выполните следующие действия:

1. Запустите программу ViPNet Policy Manager под учетной записью, имеющей полномочие **Аудит**.
2. В окне программы ViPNet Policy Manager на панели навигации в разделе **Журналы** выберите подраздел **Отправка и применение политик**.
3. На панели просмотра ознакомьтесь с записями в журнале. Запись с событием **Доставлена на узел** указывает на то, что политика безопасности была получена на узле, запись с событием **Применена** — что политика безопасности была применена на узле.

Подробнее о работе с журналом см. раздел Журнал отправки и применения политик безопасности (на стр. 113).

Как создать учетную запись

Чтобы создать учетную запись, выполните следующие действия:

1. Запустите программу ViPNet Policy Manager под учетной записью, имеющей полномочие **Управление пользователями**.
2. В окне программы ViPNet Policy Manager на панели навигации в разделе **Управление доступом** выберите подраздел **Пользователи**.
3. На панели просмотра нажмите кнопку **Создать**.
4. В окне **Свойства учетной записи** задайте параметры новой учетной записи:
   - В разделе **Основные параметры** задайте учетные данные пользователя: имя пользователя (логин), пароль и его подтверждение.

     Примечание. Имя учетной записи может содержать только символы латинского алфавита и цифры.

     Пароль должен содержать не менее девяти символов.

     Для ограничения срока действия пароля установите соответствующий флажок и задайте дату окончания действия пароля.
   - В разделе **Дополнительные параметры** введите персональные данные пользователя.
   - В разделе **Роли пользователей** задайте полномочия пользователя: нажмите кнопку **Добавить**, выберите в списке роли, содержащие необходимые полномочия, и нажмите кнопку **OK**.
5. В окне **Свойства учетной записи** нажмите кнопку **OK**. В списке учетных записей появится новая запись.

Созданную учетную запись можно использовать для входа в программу, чтобы выполнять действия, предусмотренные заданными в ней полномочиями. Подробнее о возможных полномочиях пользователей см. раздел Разграничение полномочий на основе ролей пользователей (на стр. 44).

5

Управление учетными записями и ролями пользователей

Разграничение полномочий на основе ролей пользователей 44

Управление учетными записями 45

Управление ролями пользователей 49

Смена пароля пользователя 52

Разграничение полномочий на основе ролей пользователей

Для разграничения полномочий пользователей при работе с программой ViPNet Policy Manager используются роли пользователей (см. глоссарий, стр. 137). Каждая роль определяет действия, которые разрешено выполнять пользователю в программе, и может состоять из одного или нескольких допустимых полномочий:

- **Управление пользователями** — создание, настройка и удаление учетных записей.
- **Управление ролями** — создание, настройка и удаление ролей пользователей.
- **Управление подразделениями** — создание, настройка и удаление подразделений.
- **Управление шаблонами** — создание, настройка и удаление шаблонов политики безопасности и групп объектов.
- **Назначение шаблонов** — назначение шаблонов политики безопасности сетевым узлам и подразделениям.
- **Отправка политик** — рассылка результирующих политик безопасности.
- **Аудит** — просмотр подразделений, шаблонов, групп объектов, результирующих политик безопасности и журналов.

В программе ViPNet Policy Manager имеется ряд предустановленных ролей пользователей:

- **Супервизор** — имеет все полномочия.
- **Аудитор** — имеет полномочие **Аудит**.
- **Администратор рассылки** — имеет полномочия **Назначение шаблонов** и **Отправка политик**.
- **Администратор политик** — имеет полномочия **Управление подразделениями**, **Управление шаблонами** и **Назначение шаблонов**.

Управление полномочиями пользователей осуществляется путем назначения ролей при задании свойств учетных записей (см. «Создание и изменение учетной записи» на стр. 45). Каждому пользователю может быть назначена одна или несколько ролей. Полномочия пользователя, которому назначено несколько ролей, определяются как совокупность полномочий всех его ролей.

Распределение ролей между пользователями зависит от количества персонала, ответственного за управление сетью ViPNet, и его квалификации. В случае нехватки подготовленных администраторов можно использовать встроенную учетную запись **Supervisor** с ролью **Супервизор**, которая имеет все полномочия.

Управление учетными записями

Учетные записи содержат имена и пароли пользователей, их персональные данные, а также роли пользователей.

После установки программы ViPNet Policy Manager для входа используется встроенная учетная запись с именем **Supervisor** и паролем **Supervisor**. Она позволяет создавать другие учетные записи, управлять учетными записями и ролями пользователей, а также работать с другими объектами. Встроенную учетную запись нельзя удалить.

Внимание! После установки программы настоятельно рекомендуется изменить пароль встроенной учетной записи (см. «Смена пароля пользователя» на стр. 52).

В программе ViPNet Policy Manager список учетных записей отображается в подразделе **Пользователи** раздела **Управление доступом**. Этот подраздел будет присутствовать на панели навигации только в случае, если текущий пользователь программы имеет полномочие **Управление пользователями**.

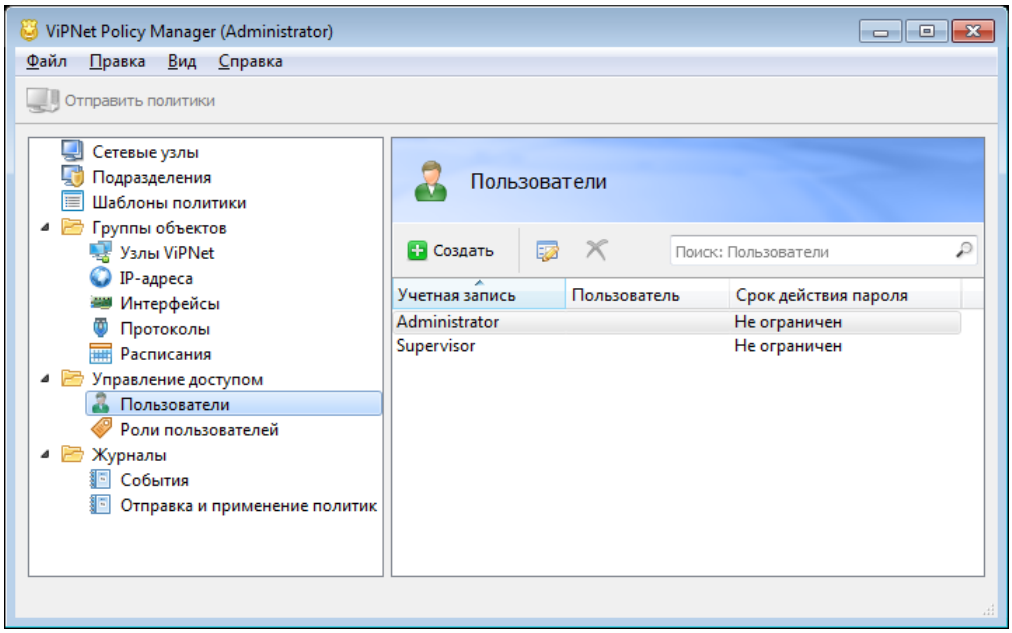

Рисунок 9. Список учетных записей пользователей

Создание и изменение учетной записи

Для возможности управлять подразделениями и шаблонами, назначать шаблоны и отправлять политики безопасности на сетевые узлы необходимо создать учетные записи с соответствующими полномочиями. Первоначальное создание учетных записей осуществляется под встроенной

учетной записью **Supervisor**. В дальнейшем создавать и изменять учетные записи сможет пользователь, имеющий полномочие **Управление пользователями**.

Чтобы создать новую учетную запись:

1 В окне программы ViPNet Policy Manager на панели навигации выберите в разделе **Управление доступом** подраздел **Пользователи**.

2 На панели просмотра (см. Рисунок 9 на стр. 45) нажмите кнопку **Создать**.

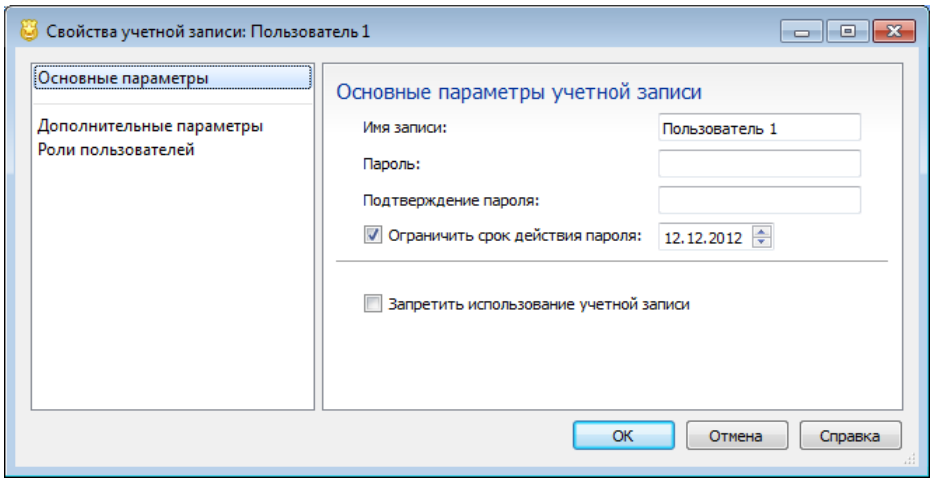

Рисунок 10. Окно создания новой учетной записи

3 В окне **Свойства учетной записи** в разделе **Основные параметры** выполните следующие действия:

- Задайте имя учетной записи. Имя учетной записи может содержать только символы латинского алфавита и цифры.
- Задайте пароль и подтвердите пароль. Пароль должен содержать не менее девяти символов.
- Если необходимо ограничить срок действия пароля, установите соответствующий флажок и задайте дату окончания действия пароля.

4 В окне **Свойства учетной записи** в разделе **Дополнительные параметры** введите в соответствующих полях персональные данные пользователя.

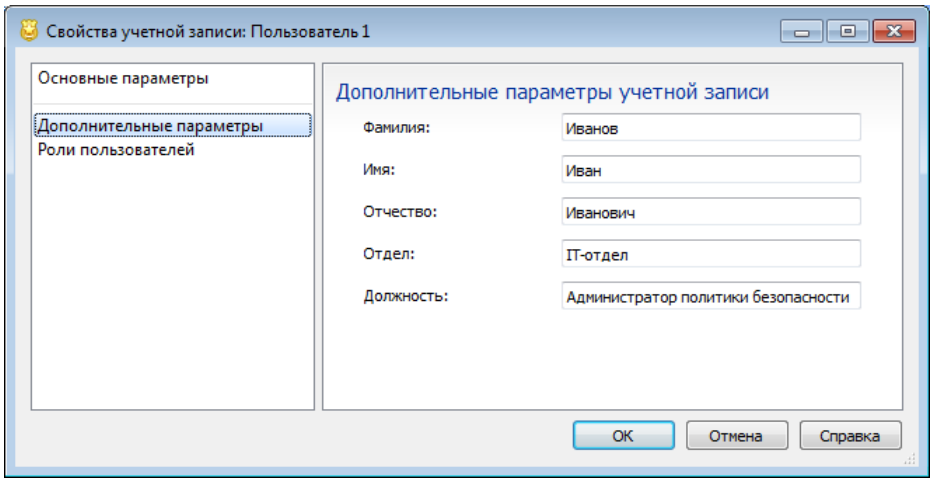

Рисунок 11. Дополнительные параметры учетной записи

5 В окне **Свойства учетной записи** в разделе **Роли пользователей** с помощью кнопок **Добавить** и **Удалить** сформируйте список ролей пользователя.

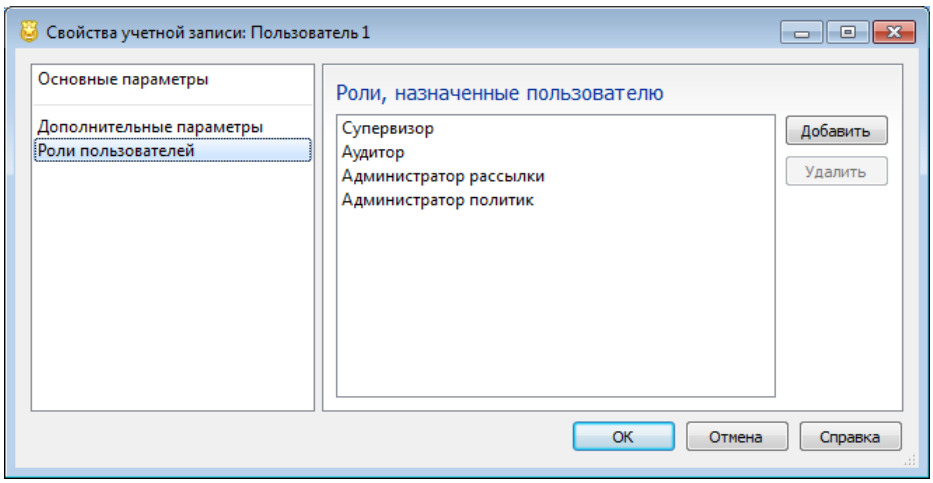

Рисунок 12. Список ролей, назначенных пользователю

Внимание! Необходимо назначить пользователю хотя бы одну роль, иначе сохранение учетной записи будет невозможно.

---

6 Нажмите кнопку **OK**. В списке учетных записей появится новая запись.

Чтобы изменить существующую учетную запись (кроме встроенной записи **Supervisor**):

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Пользователи**.

2 На панели просмотра (см. Рисунок 9 на стр. 45) выберите учетную запись и нажмите кнопку **Свойства** или дважды щелкните запись.

3 В окне **Свойства учетной записи** измените параметры или список ролей пользователя таким же образом, как при создании записи.

Примечание. Нельзя изменить учетную запись текущего пользователя программы. Если необходимо изменить именно эту учетную запись, закройте программу и снова запустите ее под другой учетной записью, имеющей полномочие **Управление пользователями**.

Удаление учетной записи

Неиспользуемую или ненужную учетную запись можно удалить. Например, учетную запись следует удалять в случае увольнения пользователя, если это предписано правилами безопасности. Для удаления требуются полномочия на управление учетными записями.

Чтобы удалить учетную запись:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Пользователи**.
2. На панели просмотра (см. Рисунок 9 на стр. 45) выберите одну или несколько учетных записей и нажмите кнопку **Удалить**.
3. В окне подтверждения нажмите кнопку **Удалить**. Выбранные учетные записи будут удалены.

Управление ролями пользователей

Роли пользователей (см. глоссарий, стр. 137) предназначены для управления полномочиями в программе ViPNet Policy Manager. Роль может соответствовать одному из полномочий или объединять несколько полномочий (см. «Разграничение полномочий на основе ролей пользователей» на стр. 44). Действия, которые может выполнять пользователь в программе, определяются назначенными ему ролями.

В программе ViPNet Policy Manager список ролей пользователей отображается в подразделе **Роли пользователей** раздела **Управление доступом**. Этот подраздел будет присутствовать на панели навигации только в случае, если текущий пользователь программы имеет полномочие **Управление ролями**.

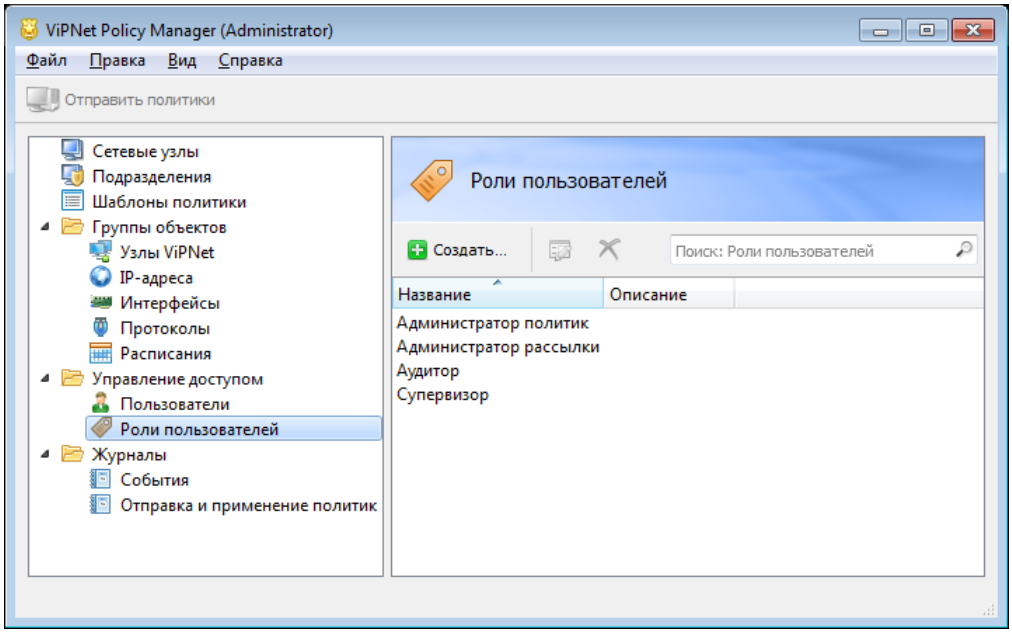

Рисунок 13. Список ролей пользователей

Создание и изменение роли пользователей

В программе ViPNet Policy Manager имеется ряд предустановленных ролей пользователей (см. «Разграничение полномочий на основе ролей пользователей» на стр. 44), а также есть возможность создавать свои роли пользователей с любой комбинацией полномочий.

Чтобы создать новую роль пользователей:

1 В окне программы ViPNet Policy Manager на панели навигации выберите в разделе **Управление доступом** подраздел **Роли пользователей**.

2 На панели просмотра (см. Рисунок 13 на стр. 49) нажмите кнопку **Создать**.

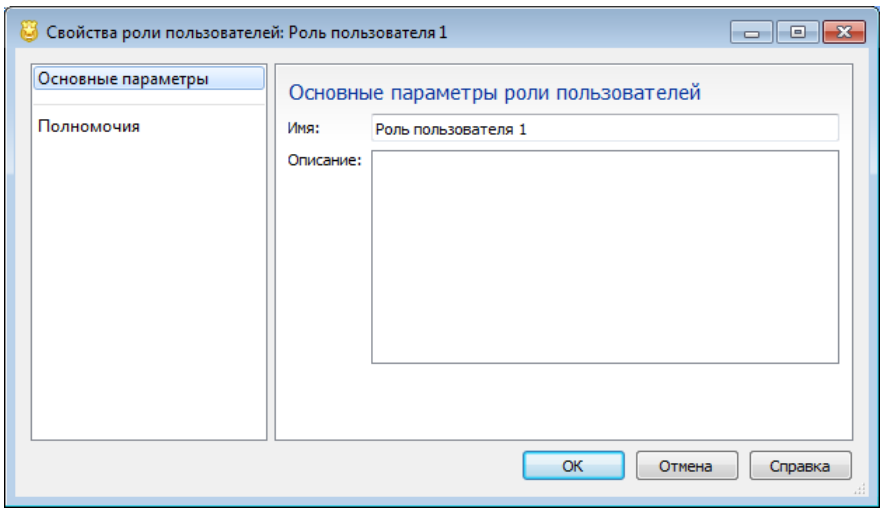

Рисунок 14. Окно создания новой роли пользователей

3 В окне **Свойства роли пользователей** в разделе **Основные параметры** задайте в соответствующих полях имя роли и ее описание.

4 В окне **Свойства роли пользователей** в разделе **Полномочия** отметьте флажками полномочия, которые должны быть разрешены для этой роли пользователей.

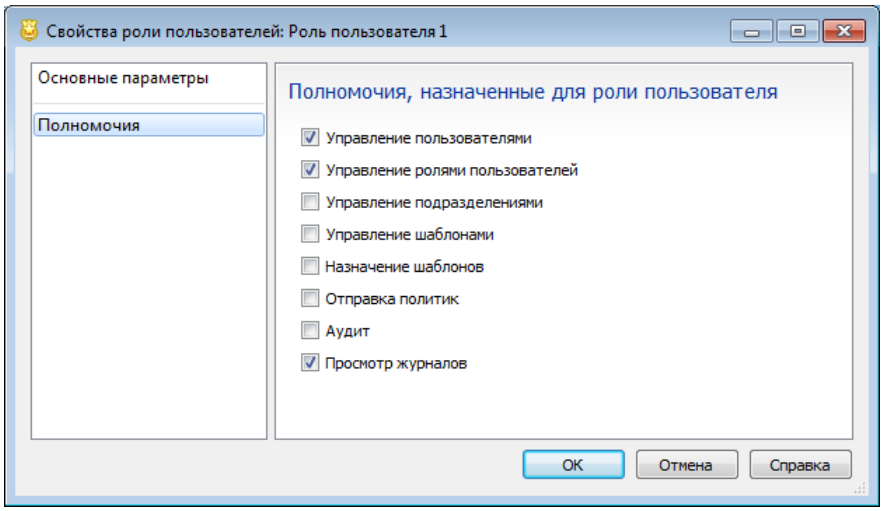

Рисунок 15. Полномочия, заданные в свойствах роли пользователей

5 Нажмите кнопку **OK**. В списке ролей пользователей появится новая роль.

Примечание. Если для роли не заданы полномочия, появится сообщение об этом. Такую роль нельзя сохранить.

Чтобы изменить существующую роль пользователей:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Роли пользователей**.

2 На панели просмотра (см. Рисунок 13 на стр. 49) выберите роль и нажмите кнопку **Свойства** или дважды щелкните запись.

3 В окне **Свойства роли пользователей** измените параметры роли или список разрешенных полномочий таким же образом, как при создании роли.

Удаление роли пользователей

Неиспользуемую роль пользователей можно удалить. Для этого:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Роли пользователей**.

2 На панели просмотра (см. Рисунок 13 на стр. 49) выберите одну или несколько ролей и нажмите кнопку **Удалить**.

3 В окне подтверждения нажмите кнопку **Удалить**. Выбранные роли пользователей будут удалены.

Смена пароля пользователя

При работе с программой ViPNet Policy Manager пользователь может сменить свой текущий пароль. Смена пароля требуется в следующих случаях:

- При первом входе в программу, который можно выполнить только под встроенной учетной записью **Supervisor**. Сообщение о смене пароля для этой учетной записи будет появляться до тех пор, пока пароль, установленный по умолчанию, не будет изменен.
- По истечении срока действия текущего пароля (в случае, если срок действия пароля ограничен).
- Для повышения надежности пароля, поскольку он не будет известен пользователю, создавшему учетную запись.

Чтобы сменить пароль:

1 В окне программы ViPNet Policy Manager в меню **Файл** выберите пункт **Сменить пароль пользователя**.

2 В окне **Смена пароля пользователя** в поле **Текущий пароль** введите действующий пароль, затем в соответствующих полях введите и подтвердите новый пароль.

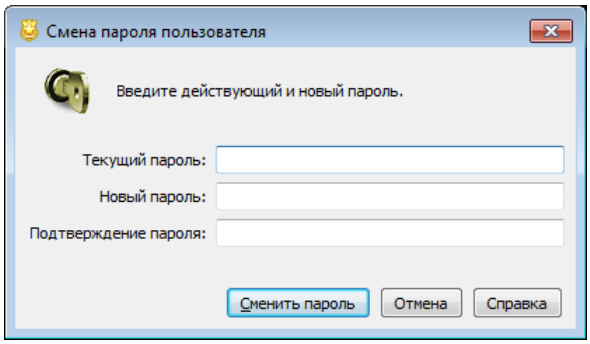

Рисунок 16. Смена пароля пользователя

3 Нажмите кнопку **Сменить пароль**. Для следующего входа в программу используйте новый пароль.

6

Работа с сетевыми узлами

Просмотр списка управляемых сетевых узлов 54

Просмотр и изменение основных параметров сетевого узла 56

Просмотр списка управляемых сетевых узлов

Сетевые узлы ViPNet (см. глоссарий, стр. 137) представляют собой компьютеры с установленным ПО ViPNet, объединенные в сети ViPNet (см. глоссарий, стр. 137). С помощью программы ViPNet Policy Manager можно управлять политикой безопасности узлов, находящихся в одной сети ViPNet. Список доступных для управления узлов отображается в разделе **Сетевые узлы**.

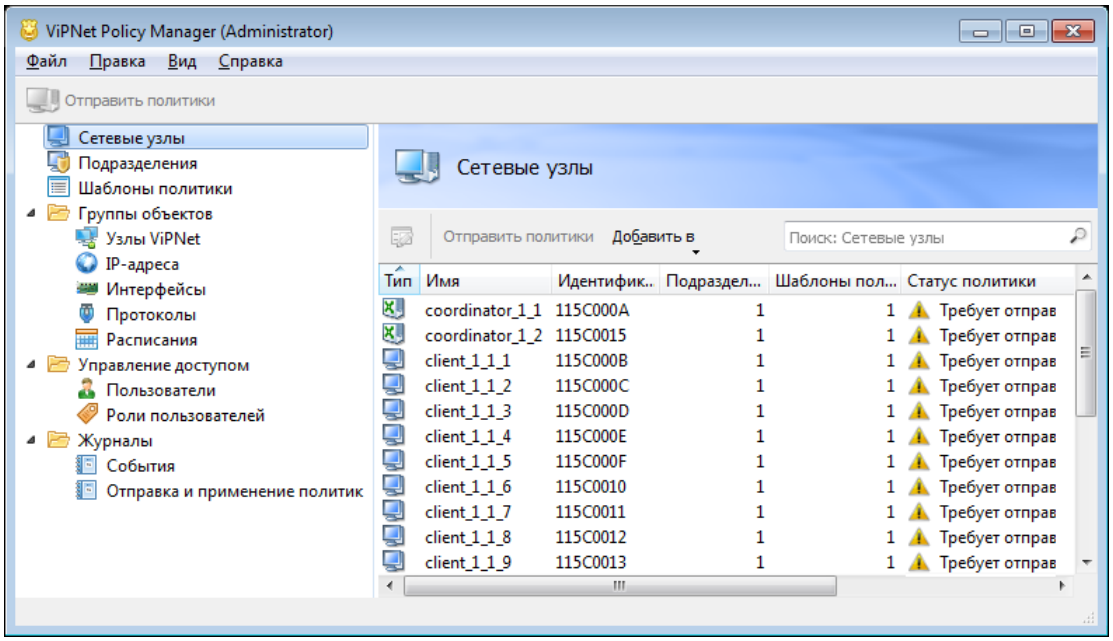

Рисунок 17. Список управляемых сетевых узлов

Для каждого сетевого узла выводится информация, указанная ниже в таблице.

Таблица 6. Отображаемая информация о сетевых узлах ViPNet

Столбец	Описание
Тип	Значок с обозначением типа узла: — координатор; — клиент.
Имя	Имя узла.
Идентификатор	Идентификатор узла в сети ViPNet.
Подразделения	Количество подразделений, в которые включен узел.
Шаблоны политики	Количество шаблонов, назначенных узлу.

Столбец	Описание
Статус политики	Статус результирующей политики безопасности, сформированной для узла в программе ViPNet Policy Manager (см. глоссарий, стр. 137): • **Не задана** — политика не сформирована, так как узлу не назначен ни один шаблон; • **Требует отправки** — имеется неотправленная политика; • **Отправлена** — политика отправлена на узел; • результат обработки политики на узле: **Получена**, **Применена**, **Отклонена** и так далее.
Дата изменения статуса политики	Дата присвоения результирующей политике безопасности текущего статуса.
Описание	Описание узла.

Набор отображаемых столбцов можно изменить. Чтобы включить или отключить отображение какого-либо столбца, щелкните правой клавишей мыши на заголовке таблицы, затем в меню установите или снимите отметку напротив соответствующего пункта меню.

Примечание. Нельзя отключить отображение имени узла.

Информацию о сетевых узлах можно отсортировать по любому столбцу. Для этого щелкните по заголовку столбца. При первом щелчке происходит сортировка по возрастанию, при повторном щелчке — по убыванию.

Список управляемых сетевых узлов может быть изменен в ЦУСе и отправлен на узел с установленной программой ViPNet Policy Manager в составе обновления справочников. При поступлении обновления список управляемых узлов изменяется в программе ViPNet Policy Manager автоматически.

Просмотр и изменение основных параметров сетевого узла

К основным параметрам сетевого узла относятся имя и описание узла, его идентификатор и адрес в сети ViPNet.

Для просмотра и изменения основных параметров сетевого узла:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Сетевые узлы**.

2 На панели просмотра (см. Рисунок 17 на стр. 54) выберите сетевой узел и нажмите кнопку **Свойства** или дважды щелкните узел.

3 В окне **Свойства сетевого узла** на левой панели выберите раздел **Основные параметры**.

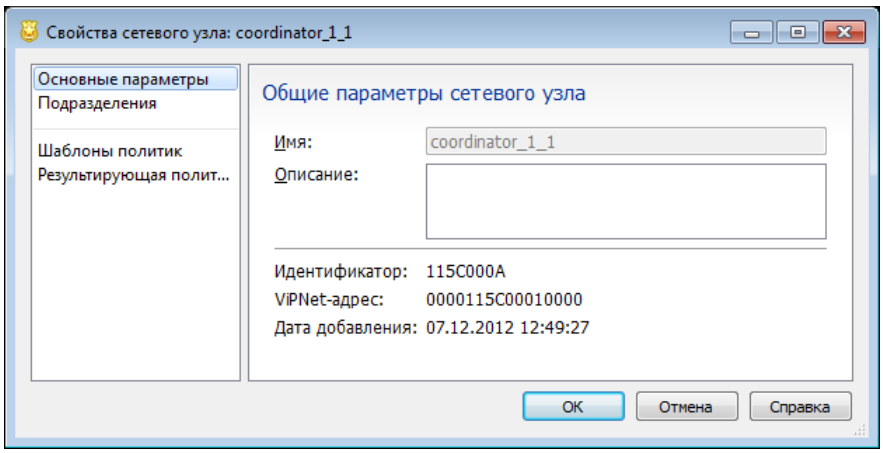

Рисунок 18. Основные параметры сетевого узла

4 Если требуется, измените в соответствующем поле описание сетевого узла.

Примечание. В программе ViPNet Policy Manager нельзя изменить параметры узла, задаваемые в ЦУСе, — имя узла, его идентификатор и адрес в сети ViPNet.

5 Чтобы сохранить изменения, нажмите кнопку **OK**. У сетевого узла появится новое описание.

7

Управление подразделениями

Назначение подразделений 58

Создание подразделения 59

Просмотр и изменение основных параметров подразделения 60

Добавление сетевых узлов в подразделение 61

Удаление подразделения 64

Назначение подразделений

Подразделения предназначены для объединения сетевых узлов, к которым должна применяться одинаковая политика безопасности. Формирование общей политики безопасности для таких узлов происходит путем назначения шаблонов не отдельным узлам, а всему подразделению. Рассылка политики безопасности на узлы подразделения может производиться как выборочно (см. «Выборочная рассылка» на стр. 111), так и сразу на все узлы подразделения (см. «Групповая рассылка» на стр. 112).

Подразделения можно выстроить иерархически, размещая одно подразделение в другом. Наверху иерархии находится корневое подразделение **Сетевые узлы**, содержащее все управляемые сетевые узлы. Имена подразделений должны быть уникальными в рамках вышестоящего подразделения. Например, подразделения, находящиеся непосредственно в корневом подразделении, должны иметь разные имена.

В программе ViPNet Policy Manager иерархическая структура подразделений отображается в разделе **Подразделения**. Для каждого подразделения указывается количество входящих в него узлов и назначенных шаблонов.

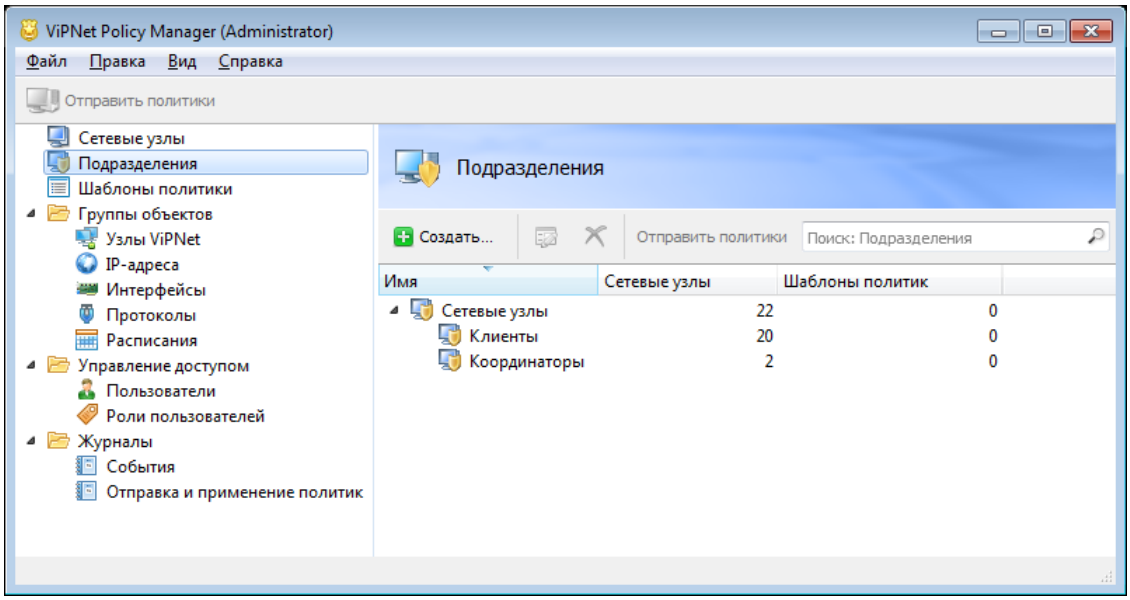

Рисунок 19. Подразделения

Примечание. Корневое подразделение **Сетевые узлы** создается автоматически и всегда присутствует в иерархии подразделений. Оно содержит все сетевые узлы, управляемые ViPNet Policy Manager, независимо от их вхождения в другие подразделения.

Создание подразделения

Чтобы создать подразделение:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.

2 На панели просмотра (см. Рисунок 19 на стр. 58) нажмите кнопку **Создать**.

3 В окне **Свойства подразделения** в разделе **Основные параметры** задайте следующие параметры:

- В поле **Имя** введите имя подразделения.
- В поле **Иерархия группы** укажите место нового подразделения в иерархии. По умолчанию новое подразделение помещается в то подразделение, которое выбрано в иерархии. Чтобы указать другое место, нажмите кнопку ... и выберите нужное подразделение.
- В поле **Описание** введите описание подразделения.

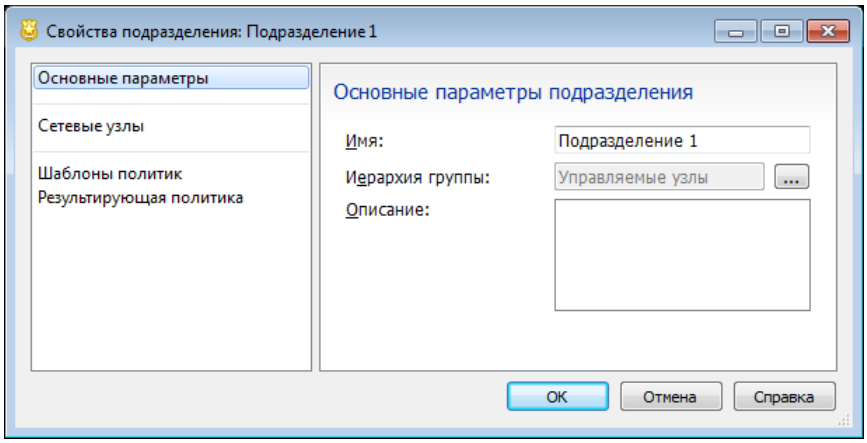

Рисунок 20. Основные параметры подразделения

4 В окне **Свойства подразделения** в разделе **Сетевые узлы** задайте список сетевых узлов, входящих в подразделение (см. «Добавление в подразделение нескольких сетевых узлов» на стр. 62).

5 В окне **Свойства подразделения** в разделе **Шаблоны политик** назначьте подразделению шаблоны политики безопасности (см. «Назначение шаблона одному подразделению» на стр. 101).

6 Нажмите кнопку **OK**. В иерархии подразделений появится новое подразделение.

Просмотр и изменение основных параметров подразделения

К основным параметрам подразделения относятся его имя и описание, а также положение в иерархии подразделений. Эти параметры задаются при создании подразделения (см. «Создание подразделения» на стр. 59), но в случае необходимости их можно изменить.

Для просмотра и изменения основных параметров подразделения:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.
2. На панели просмотра (см. Рисунок 19 на стр. 58) выберите подразделение и нажмите кнопку **Свойства** или дважды щелкните подразделение.
3. В окне **Свойства подразделения** на левой панели выберите раздел **Основные параметры** (см. Рисунок 20 на стр. 59).
4. Если требуется, измените в соответствующих полях имя подразделения и его описание.
5. Если требуется изменить положение подразделения в иерархии, нажмите кнопку справа от поля **Иерархия группы** и выберите подразделение, в которое требуется переместить данное подразделение.
6. Чтобы сохранить изменения, нажмите кнопку **OK**. У подразделения изменится имя или описание, а также оно займет новое место в иерархии (если подразделение было перемещено).

Добавление сетевых узлов в подразделение

Каждый сетевой узел может входить в одно или несколько подразделений. В этом случае политика безопасности узла будет формироваться с учетом шаблонов, назначенных этим подразделениям (см. «Правила формирования результирующей политики безопасности» на стр. 105).

Чтобы добавить сетевые узлы в подразделение, можно использовать любой из двух способов:

- Добавить в подразделение отдельный узел (см. «Добавление в подразделение одного сетевого узла» на стр. 61). Этот способ позволяет также добавить узел сразу в несколько подразделений.
- Добавить в подразделение несколько узлов за один прием (см. «Добавление в подразделение нескольких сетевых узлов» на стр. 62).

Добавление в подразделение одного сетевого узла

Чтобы добавить в подразделение один сетевой узел, выполните следующие действия:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Сетевые узлы**.
2. На панели просмотра (см. Рисунок 17 на стр. 54) выберите сетевой узел и нажмите кнопку **Свойства** или дважды щелкните узел.
3. В окне **Свойства сетевого узла** на левой панели выберите раздел **Подразделения**.

   На правой панели будет отображена иерархия подразделений. Те подразделения, в которые уже входит узел, отмечены флажками.

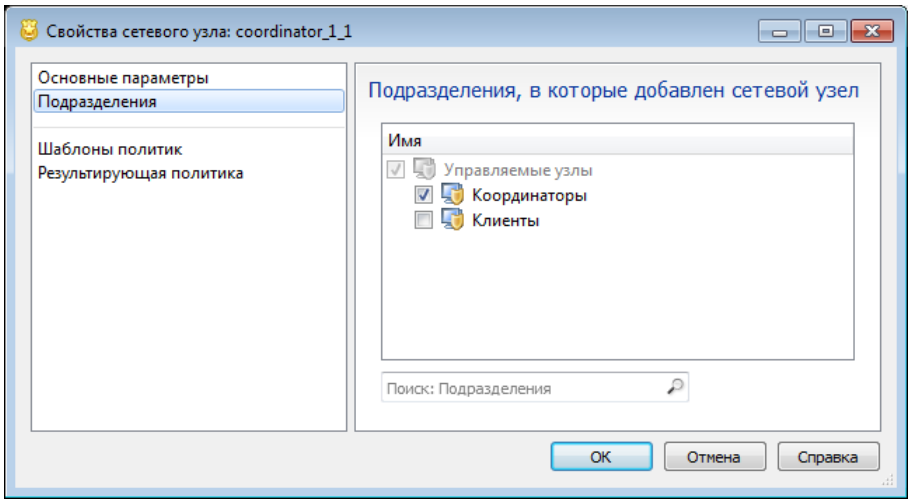

Рисунок 21. Подразделения, в которые входит узел

4 Установите флажки напротив тех подразделений, в которые требуется добавить узел, и снимите флажки напротив подразделений, из которых необходимо удалить узел.

5 Нажмите кнопку **OK**, чтобы сохранить изменения.

Добавление в подразделение нескольких сетевых узлов

В подразделение можно добавить сразу несколько сетевых узлов. Для этого:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.

2 На панели просмотра (см. Рисунок 19 на стр. 58) выберите подразделение и нажмите кнопку **Свойства** или дважды щелкните подразделение.

3 В окне **Свойства подразделения** на левой панели выберите раздел **Сетевые узлы**.

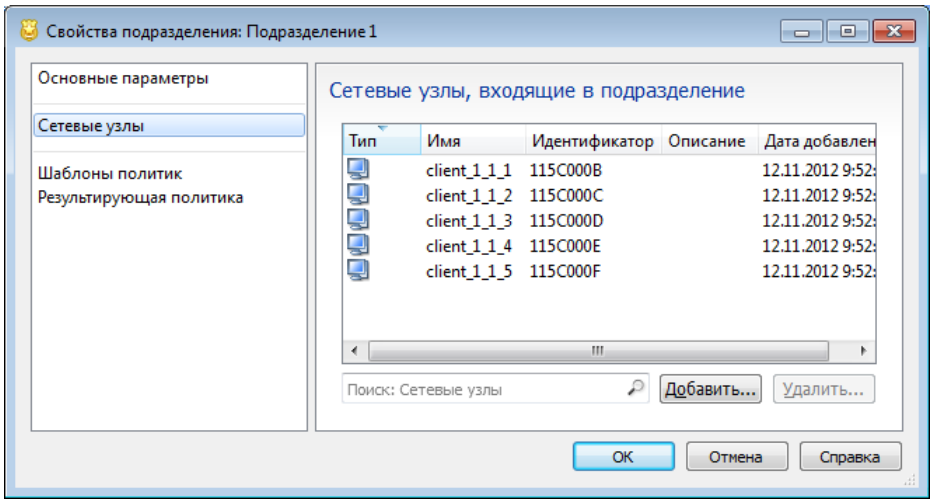

Рисунок 22. Список сетевых узлов, входящих в подразделение

4 Нажмите кнопку **Добавить**.

5 В открывшемся окне выберите в списке один или несколько узлов и нажмите кнопку **OK**. Выбранные узлы будут добавлены в список узлов, входящих в подразделение.

6 Нажмите кнопку **OK**, чтобы сохранить изменения.

Если из подразделения необходимо удалить какие-либо узлы, выполните следующее:

1 В списке узлов, входящих в подразделение, выберите один или несколько узлов и нажмите кнопку **Удалить**.

2 В окне подтверждения нажмите кнопку **Удалить**. Выбранные узлы будут исключены из списка.

3 Нажмите кнопку **OK**, чтобы сохранить изменения.

Удаление подразделения

Любое подразделение в иерархии можно удалить, кроме корневого подразделения **Сетевые узлы**, которое содержит все управляемые узлы, заданные в ЦУСе.

Чтобы удалить подразделение:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.

2 На панели просмотра (см. Рисунок 19 на стр. 58) выберите одно или несколько подразделений и нажмите кнопку **Удалить**.

3 В окне подтверждения нажмите кнопку **Удалить подразделения**.

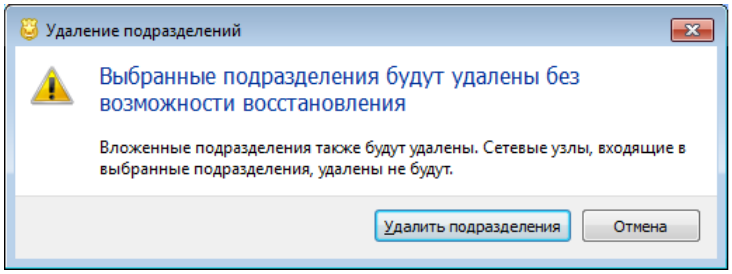

Рисунок 23. Удаление подразделений

Выбранные подразделения будут удалены. При этом также будут удалены вложенные в них подразделения.

Примечание. Сетевые узлы, входившие в удаленные подразделения, и шаблоны, назначенные удаленным подразделениям, не будут удалены.

8

Управление шаблонами политики безопасности

Общие сведения о шаблонах политики безопасности 66

Работа с группами объектов 68

Создание шаблона политики безопасности 80

Просмотр и изменение сетевых фильтров, заданных в шаблоне 81

Просмотр и изменение правил трансляции IP-адресов, заданных в шаблоне 93

Копирование шаблона политики безопасности 97

Удаление шаблона политики безопасности 98

Назначение шаблона сетевым узлам и подразделениям 99

Общие сведения о шаблонах политики безопасности

Шаблон политики безопасности — это набор сетевых фильтров и правил трансляции IP-адресов, предназначенный для реализации определенной политики безопасности. Формирование политики безопасности для сетевых узлов осуществляется путем назначения шаблонов узлам и подразделениям. На основании назначенных шаблонов создаются результирующие политики безопасности, которые рассылаются на узлы. Полученные на узлах результирующие политики безопасности совместно с фильтрами, заданными на самих узлах, определяют правила фильтрации трафика.

Шаблон может содержать:

- Сетевые фильтры (см. «Просмотр и изменение сетевых фильтров, заданных в шаблоне» на стр. 81):
  - локальные фильтры открытой сети;
  - транзитные фильтры открытой сети;
  - фильтры для туннелируемых узлов;
  - фильтры защищенной сети.
- Правила трансляции IP-адресов (см. «Просмотр и изменение правил трансляции IP-адресов, заданных в шаблоне» на стр. 93).

В программе ViPNet Policy Manager список шаблонов отображается в разделе **Шаблоны политики**. Для каждого шаблона указывается количество узлов и количество подразделений, которым назначен шаблон.

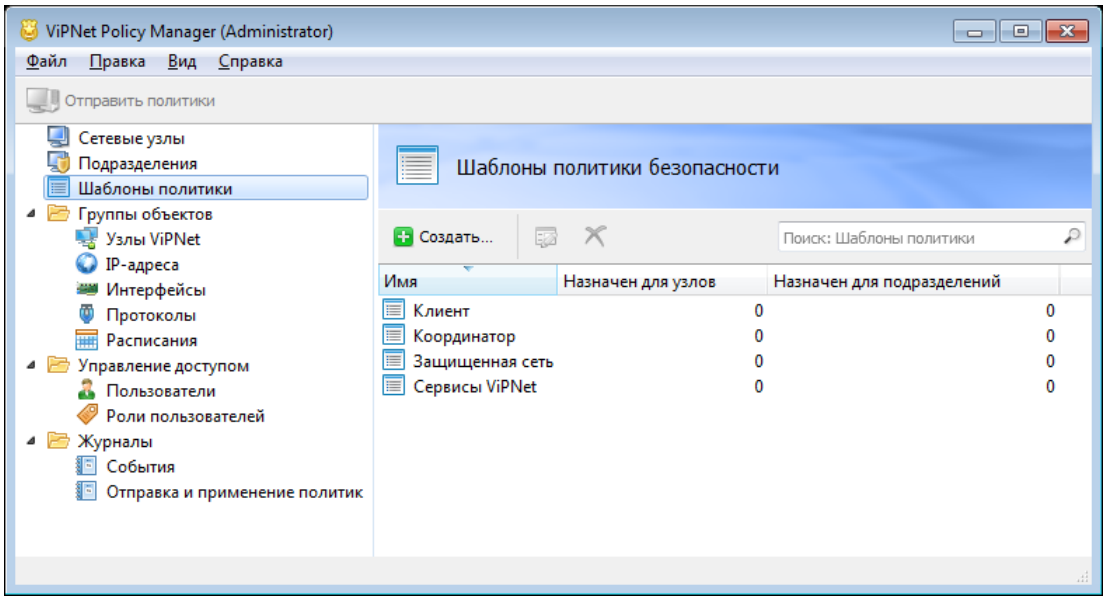

Рисунок 24. Список шаблонов политики безопасности

Примечание. В списке шаблонов всегда присутствуют типовые шаблоны политики безопасности, поставляемые в составе ПО ViPNet Policy Manager.

Работа с группами объектов

Группы объектов — это средство, позволяющее упростить создание сетевых фильтров и правил трансляции IP-адресов в шаблонах политики безопасности. Они объединяют несколько значений одного типа и могут быть заданы при настройке параметров фильтра или правила трансляции вместо отдельных объектов.

Существуют следующие виды групп объектов:

- Системные группы объектов.
- Пользовательские группы объектов.

Системные группы объектов — встроенные в ПО ViPNet Policy Manager объекты с фиксированными именами, которые могут использоваться в создаваемых сетевых фильтрах для задания отправителей и получателей IP-пакетов, а также в пользовательских группах объектов. Системные группы объектов не отображаются в списках групп и их нельзя изменить или удалить. Список системных групп объектов см. в разделе Системные группы объектов (на стр. 69).

Пользовательские группы объектов — группы объектов, создаваемые пользователем непосредственно в программе ViPNet Policy Manager. У каждой группы объектов есть свой состав, при этом из состава могут быть заданы некоторые исключения. В состав и исключения группы могут быть включены другие группы объектов того же типа или некоторые системные группы объектов. Работа с такими группами объектов осуществляется в разделе **Группы объектов**.

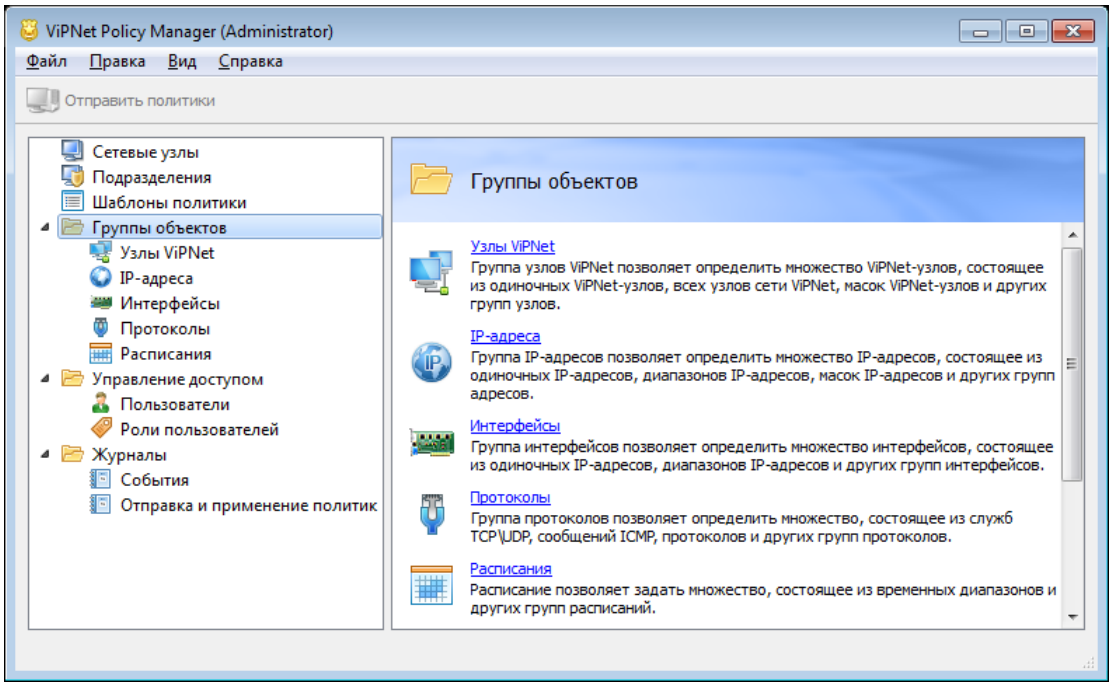

Рисунок 25. Группы объектов

Пользовательские группы объектов делятся на следующие типы:

- **Узлы ViPNet** — группа узлов защищенной сети. Используется в фильтрах защищенной сети и туннелируемых узлов.
- **IP-адреса** — любая комбинация отдельных IP-адресов и диапазонов IP-адресов или DNS-имен. Используется в правилах трансляции IP-адресов и сетевых фильтрах (за исключением фильтров защищенной сети).
- **Интерфейсы** — любая комбинация сетевых интерфейсов или IP-адресов интерфейсов. Используется в сетевых фильтрах только на координаторе (за исключением фильтров защищенной сети). Для координаторов с ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW в сетевых фильтрах также могут использоваться идентификаторы их сетевых интерфейсов.
- **Протоколы** — любая комбинация протоколов и портов. Используется во всех фильтрах и правилах трансляции IP-адресов.
- **Расписания** — любая комбинация условий применения сетевых фильтров по времени и дням недели. Используется во всех фильтрах.

Вы можете создать группу объектов любого типа. Имеет смысл создавать группы из часто используемых наборов объектов. Подробнее о создании групп см. в разделе Создание и изменение групп объектов (на стр. 70).

Системные группы объектов

В таблице ниже приведен список системных групп объектов и их значений.

Таблица 7. Системные группы объектов

Имя группы объектов	Значение
Все клиенты	Все клиенты из справочников узла
Все координаторы	Все координаторы из справочников узла
Все объекты	Совокупность всех объектов в группе конкретного типа. Задается только в составе группы объектов. Предназначена для создания групп, состоящих из всех объектов, кроме некоторых исключений
Широковещательные адреса	Все широковещательные адреса Используется при создании фильтров широковещательных пакетов
Мой узел	Свой узел Можно указать в качестве источника IP-пакетов для исходящих соединений узла или в качестве назначения для входящих соединений

Имя группы объектов	Значение
Другие узлы	Другие сетевые узлы (любые узлы, кроме своего) Можно указать в качестве источника IP-пакетов для входящих соединений узла или в качестве назначения для исходящих соединений
Туннелируемые IP-адреса	Все IP-адреса, туннелируемые координатором
Групповые адреса	Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255) Можно указать только в качестве назначения для локальных открытых соединений

Создание и изменение групп объектов

Чтобы создать новую группу объектов, выполните следующие действия:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Группы объектов**.
2. На панели просмотра щелкните ссылку с названием типа группы объектов, которую вы хотите создать, или на панели навигации выберите соответствующий подраздел.
3. На панели просмотра нажмите кнопку **Создать**.

   Откроется окно свойств группы объектов, в котором вы можете задать параметры новой группы.
4. В разделе **Основные параметры** задайте имя группы объектов и ее описание. Имя группы должно быть уникальным.
5. В разделе **Состав** определите состав создаваемой группы.

   При формировании состава группы типа:

   - **Узлы ViPNet —** укажите защищенные узлы, которые необходимо включить в создаваемую группу. Подробнее см. раздел Добавление сетевых узлов (на стр. 74).

     В состав группы узлов защищенной сети вы также можете включить системные группы объектов **Все координаторы**, **Все клиенты** и **Все объекты** (см. «Системные группы объектов» на стр. 69).

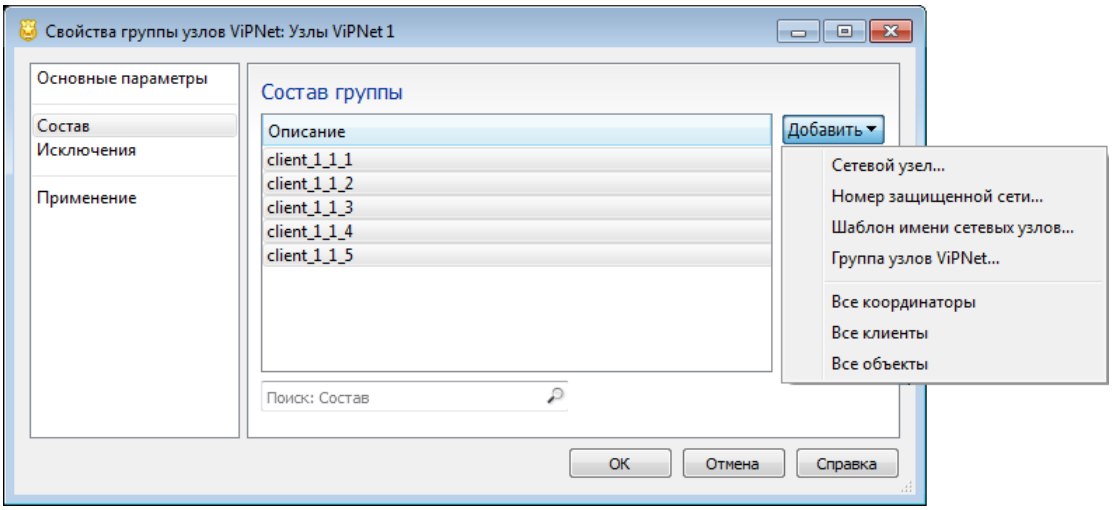

Рисунок 26. Формирование состава группы узлов

- **IP-адреса** — задайте отдельные IP-адреса, диапазон адресов или подсеть либо DNS-имена. Подробнее см. раздел Добавление IP-адресов и DNS-имен (на стр. 75).

  В состав группы IP-адресов вы также можете включить системную группу объектов **Все объекты**.

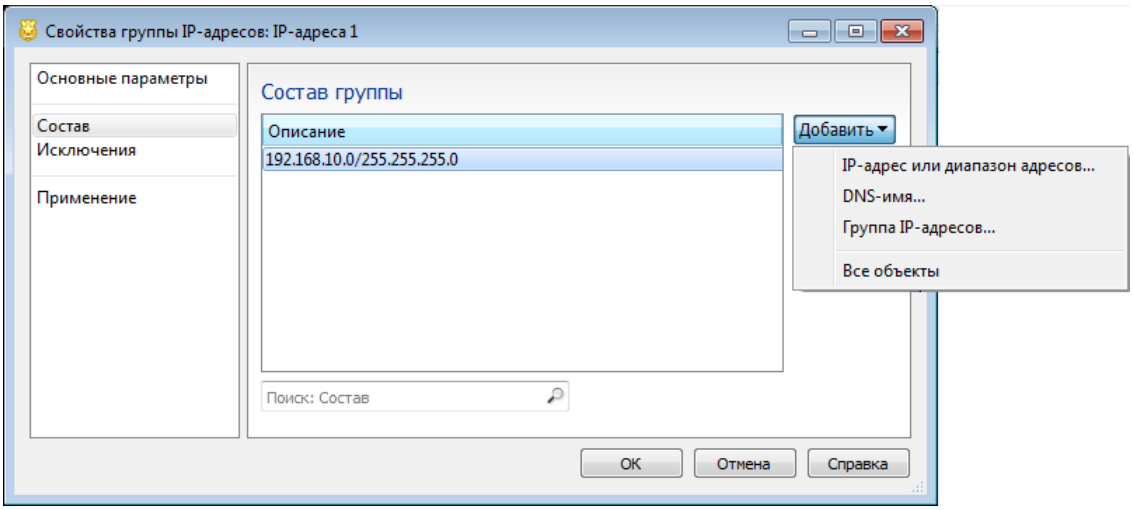

Рисунок 27. Формирование состава группы IP-адресов

- **Интерфейсы** — задайте IP-адрес интерфейса или группы интерфейсов. О добавлении IP-адресов сетевых интерфейсов см. раздел Добавление IP-адресов и DNS-имен (на стр. 75).

  Для координаторов с ПО ViPNet Coordinator for Linux и координаторов ViPNet Coordinator HW, если необходимо, задайте идентификаторы интерфейсов (см. «Добавление идентификатора сетевого интерфейса» на стр. 76).

  В состав группы интерфейсов вы также можете включить системную группу объектов **Все объекты**.

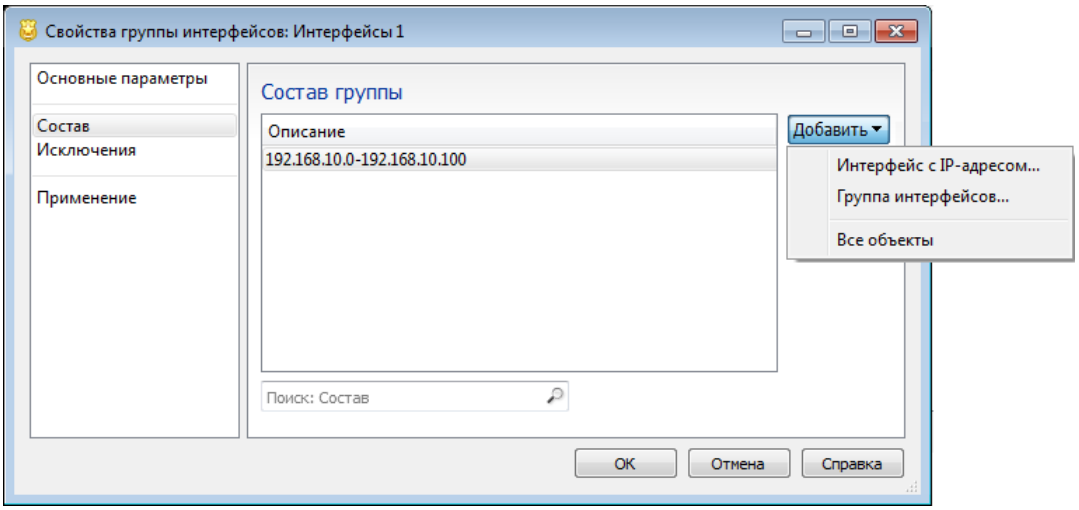

Рисунок 28. Формирование состава группы интерфейсов

- **Протоколы** — задайте протоколы и при необходимости номера портов. Подробнее см. раздел Добавление протоколов (на стр. 77).

  В состав группы протоколов вы также можете включить системную группу объектов **Все объекты**.

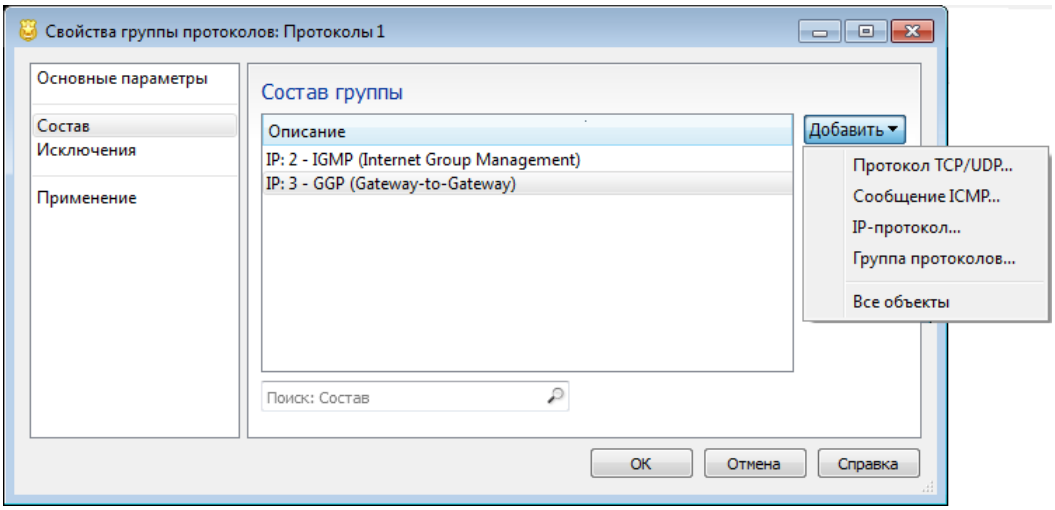

Рисунок 29. Формирование состава группы протоколов

- **Расписания** — задайте расписание, состоящее из дней недели или временных диапазонов. Впоследствии такие расписания можно использовать для ограничения времени действия сетевых фильтров. Подробнее см. раздел Добавление расписаний (на стр. 78).

  В состав группы расписаний вы также можете включить системную группу объектов **Все объекты**.

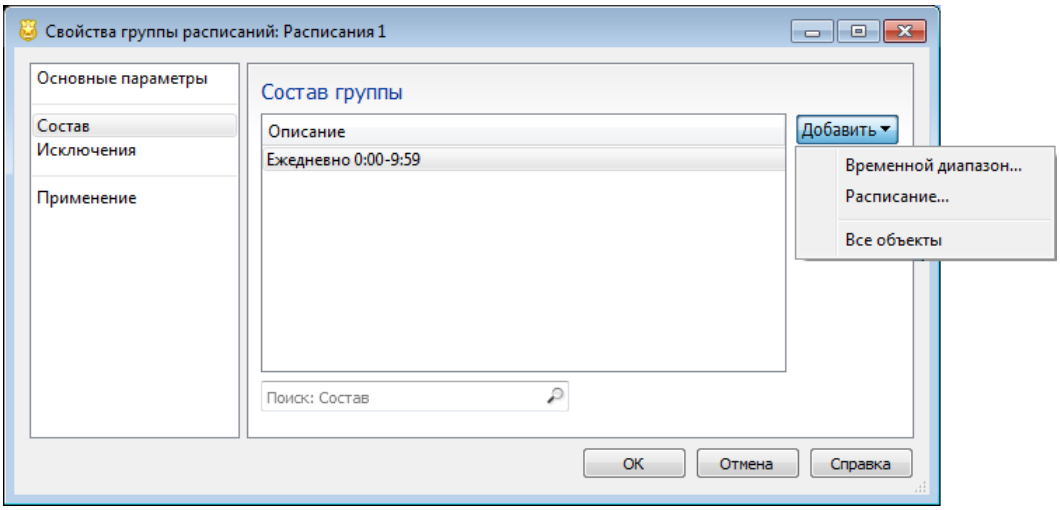

Рисунок 30. Формирование состава группы расписаний

Примечание. В каждую группу объектов могут входить группы объектов этого же типа, то есть можно организовать вложенность однотипных групп.

---

6 В разделе **Исключения** задайте исключения из состава группы объектов, то есть те элементы, которые в группу объектов не должны входить. Например, чтобы создать группу защищенных узлов, состоящую из всех координаторов, кроме одного, добавьте в состав системную группу **Все координаторы**, а в качестве исключения задайте конкретный сетевой узел — координатор.

В качестве исключения можно задать также другую группу объектов такого же типа.

Формирование исключений осуществляется аналогично формированию состава групп объектов.

Примечание. В разделе **Применение** ничего задавать не требуется. В нем отображается список фильтров, в которых используется группа объектов. При создании группы объектов данный раздел пустой.

---

7 По завершении нажмите кнопку **OK**.

В результате в списке групп объектов выбранного типа появится новая группа.

Если при создании группы объектов не был определен ее состав, то такая группа будет считаться пустой. Пустые группы не рекомендуется использовать в сетевых фильтрах, поскольку фильтры в этом случае не будут применяться.

Чтобы изменить параметры группы объектов, выберите ее в соответствующем разделе групп объектов, затем дважды щелкните или нажмите кнопку **Свойства**. После изменения основных параметров группы или ее состава в окне свойств группы нажмите кнопку **OK**.

Чтобы удалить группу объектов, выберите ее в соответствующем разделе групп объектов и нажмите кнопку **Удалить**. В появившемся окне подтвердите удаление группы. Если удаляемая группа объектов используется в каких-либо сетевых фильтрах или правилах трансляции адресов

либо входит в другие группы объектов, то появится сообщение об этом и она не будет удалена. В данном случае с помощью кнопки **Показать подробности** в окне сообщения просмотрите, в каких элементах используется данная группа, и повторите удаление, предварительно исключив группу из состава данных элементов.

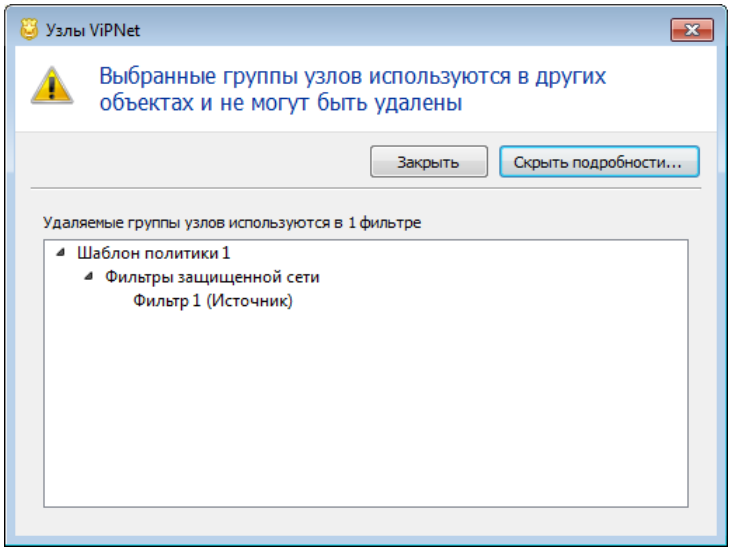

Рисунок 31. Невозможность удаления группы объектов

Добавление сетевых узлов

Сетевые узлы могут быть добавлены в состав и исключения групп узлов, а также выбраны в качестве источника или назначения при создании фильтров защищенной сети и фильтров для туннелируемых узлов следующим образом:

- При создании группы узлов или сетевых фильтров вы можете добавить выбранное множество сетевых узлов. Для этого в окне свойств группы узлов или сетевого фильтра в соответствующем разделе нажмите **Добавить** и в меню выберите **Сетевой узел**. После этого в появившемся окне выберите в списке один или несколько узлов и нажмите кнопку **OK**.

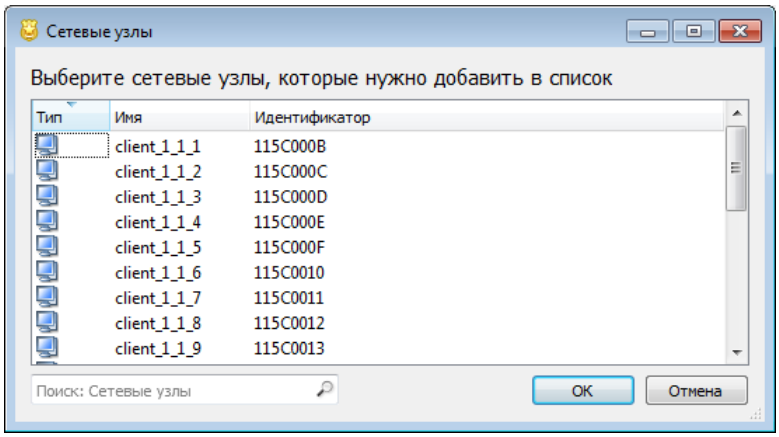

Рисунок 32. Выборочное добавление сетевых узлов

В результате будут добавлены выбранные узлы.

- При создании группы узлов вы можете добавить множество узлов определенной сети ViPNet. Для этого в нужных разделах окна свойств группы нажмите кнопку **Добавить** и в меню выберите **Номер защищенной сети**. В появившемся окне введите номер нужной сети.

  В результате будут добавлены все узлы из заданной сети.

- При создании группы узлов вы можете добавить множество узлов, имя которых соответствует заданной маске. Для этого в нужных разделах окна свойств группы нажмите кнопку **Добавить** и в меню выберите **Шаблон имени сетевых узлов**. В появившемся окне задайте маску имени узлов. Маска задается стандартным образом с использованием символов «*» и «?».

  В результате будут добавлены все узлы, имя которых соответствует заданной маске.

Добавление IP-адресов и DNS-имен

IP-адреса или DNS-имена могут быть добавлены в состав и исключения групп IP-адресов, а также заданы при определении источника и назначения в сетевых фильтрах (кроме фильтров защищенной сети) и правилах трансляции.

IP-адреса также могут быть добавлены в состав и исключения групп интерфейсов. В данном случае имеются в виду IP-адреса непосредственно сетевых интерфейсов.

Чтобы добавить IP-адреса в одном из указанных случаев:

1. В окне свойств группы IP-адресов, сетевого фильтра или правила трансляции в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **IP-адрес или диапазон адресов**, в окне свойств группы интерфейсов, фильтра или правила при задании сетевых интерфейсов — **Интерфейс с IP-адресом**.
2. В появившемся окне выполните следующие действия:
   - Если требуется добавить один конкретный IP-адрес (в том случае, если он известен), щелкните **IP-адрес** и в поле напротив введите данный IP-адрес.
   - Если требуется задать IP-адреса в рамках некоторой подсети, установите переключатель в положение **Подсеть**, после чего в соответствующих полях задайте адрес и маску данной подсети.
   - Если требуется задать диапазон IP-адресов, установите переключатель в положение **Диапазон IP-адресов**, после чего в соответствующих полях задайте начальный и конечный адрес диапазона.

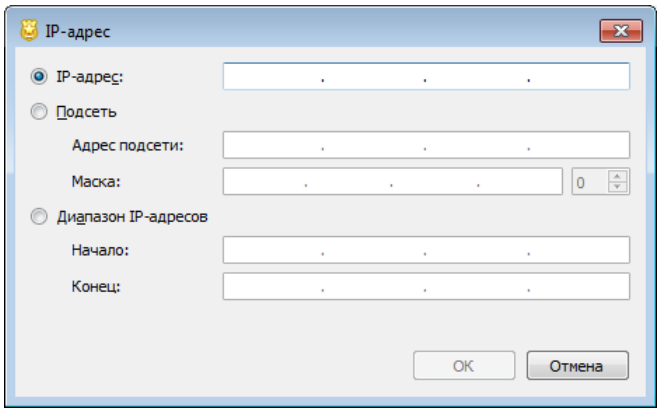

Рисунок 33. Добавление IP-адресов

После ввода необходимых данных нажмите кнопку **OK**.

В результате указанные IP-адрес или IP-адреса будут добавлены.

Чтобы добавить DNS-имя, в окне свойств группы IP-адресов или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **DNS-имя**. В появившемся окне задайте DNS-имя и нажмите кнопку **OK**.

В результате DNS-имя будет добавлено.

Добавление идентификатора сетевого интерфейса

При создании сетевых фильтров для координаторов с программным обеспечением ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW вы можете в качестве объектов использовать идентификаторы сетевых интерфейсов этих координаторов. Таким образом вы можете настроить параметры фильтра для однотипных сетевых интерфейсов разных координаторов с ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW.

Идентификаторы интерфейса могут быть добавлены в состав и исключения групп интерфейсов, а также заданы при определении источника и назначения в сетевых фильтрах (кроме фильтров защищенной сети).

Чтобы добавить идентификаторы интерфейса в одном из указанных случаев, выполните следующие действия:

Внимание! Прежде чем использовать идентификатор интерфейса в качестве объекта для сетевого фильтра, убедитесь, что на координаторах, для которых вы создаете этот сетевой фильтр, существуют интерфейсы с соответствующими идентификаторами. В противном случае сетевой фильтр не будет применен.

1. В окне свойств группы интерфейсов или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **Идентификатор интерфейса**.
2. В появившемся окне укажите идентификатор интерфейса и нажмите кнопку **OK**.

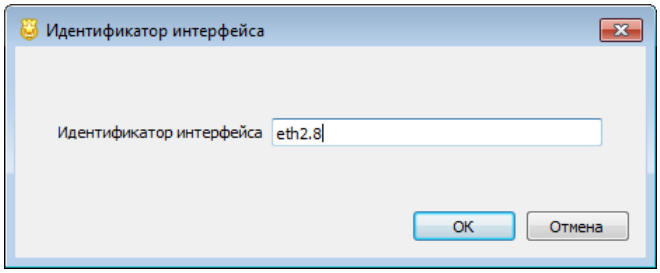

Рисунок 34. Добавление идентификатора интерфейса

В результате указанный идентификатор интерфейса будет добавлен.

Добавление протоколов

Протоколы могут быть добавлены в состав и исключения групп протоколов, а также заданы при создании любых сетевых фильтров и правил трансляции адресов.

Чтобы добавить протоколы в одном из указанных случаев, в окне свойств группы протоколов, сетевого фильтра или правила трансляции в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите:

- **Протокол TCP/UDP** — для добавления TCP- или UDP-протокола с номером порта источника и назначения. В появившемся окне выполните следующие действия:
  - В зависимости от того, какой протокол вам требуется добавить, установите переключатель **Протокол** в нужное положение.
  - Если требуется, задайте номера порта источника. Для этого выберите:
    - **Все порты** — для задания всех портов, например, если вы не знаете конкретного номера.
    - **Номер порта** — для задания номера конкретного порта. В списке напротив выберите нужный номер.
    - **Диапазон** — для задания диапазона номеров портов. В полях напротив укажите начальный и конечный адрес диапазона.
  - При необходимости аналогичным образом задайте порт назначения.

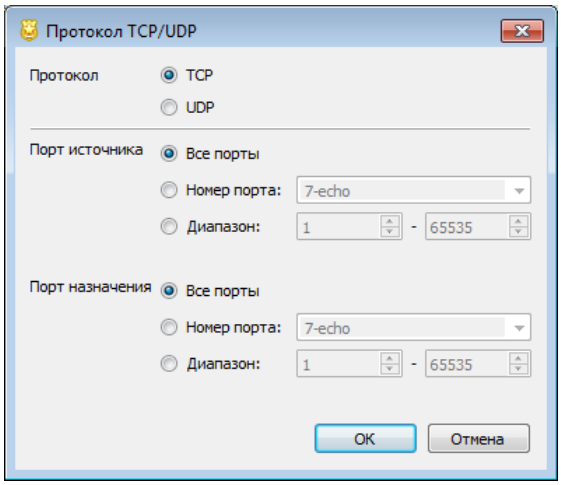

Рисунок 35. Добавление TCP- или UDP-протокола

По завершении ввода данных нажмите кнопку **OK**.

- **Сообщение ICMP** — для добавления ICMP-протокола. В появившемся окне в соответствующих списках выберите тип и код ICMP-сообщения (если требуется) и нажмите кнопку **OK**.
- **IP-протокол** — для добавления других протоколов. В появившемся окне в списке выберите нужный протокол либо введите код протокола (если он известен) и нажмите кнопку **OK**.

Добавление расписаний

Расписания действия сетевых фильтров могут быть добавлены в состав и исключения групп расписаний, а также заданы при создании любых сетевых фильтров (если требуется, чтобы фильтр действовал в конкретное время или в определенные промежутки времени).

Чтобы добавить расписание в одном из указанных случаев, выполните следующие действия:

1. В окне свойств группы расписаний или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **Временной диапазон**.
2. В появившемся окне задайте параметры расписания:
   - В группе **Время выполнения фильтра** укажите временной интервал, в течение которого будет действовать сетевой фильтр.
   - Установите переключатель в положение:
     - **Ежедневно**, если сетевой фильтр должен действовать каждый день в указанное время. Если требуется, чтобы фильтр действовал в некоторый период времени (например, в течение двух недель), установите соответствующий флажок и задайте нужный период.
     - **Еженедельно**, если сетевой фильтр должен действовать в определенные дни недели. Установите флажки напротив нужных дней недели.

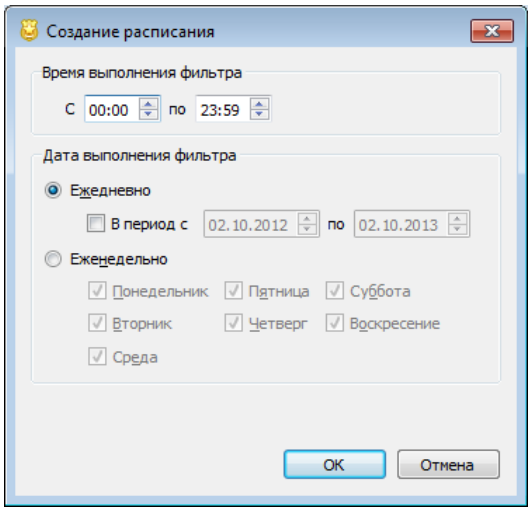

Рисунок 36. Добавление расписания

3 По завершении ввода данных нажмите кнопку **OK**.

В результате будет добавлено расписание с заданными параметрами.

Вложенность групп объектов

В каждую группу объектов могут входить группы объектов этого же типа, то есть можно организовать вложенность однотипных групп. Рассмотрим на примере, в каких случаях это может потребоваться и будет удобным.

Допустим, есть организация, которая состоит из нескольких подразделений: департамента финансов, департамента продаж и IT-отдела. В каждом подразделении имеется определенное количество сотрудников и соответственно столько же сетевых узлов. Требуется выполнить следующие операции:

1 Разрешить любые соединения IT-отдела.

2 Организовать доступ в Интернет всех сотрудников организации.

3 Организовать доступ департамента финансов к серверу 1С.

Во всех трех случаях необходимо настроить сетевые фильтры. Чтобы не создавать ряд одинаковых сетевых фильтров в каждом из указанных случаев, рекомендуется объединить сетевые узлы в соответствующие группы узлов, после чего создать по одному сетевому фильтру, используя сформированные сетевые группы. При этом целесообразно создать группы узлов таким образом: создать группы узлов каждого подразделения, а также создать общую группу, в которую будут входить группы узлов подразделений. Группы узлов IT-отдела и департамента финансов будут использоваться при создании фильтров в первом и третьем случае; общая группа узлов — при создании транзитного фильтра в процессе организации DMZ во втором случае.

Удобство в таком способе формирования групп узлов и сетевых фильтров заключается в следующем. Если, например, в каком-то подразделении появится новый сотрудник, то его узел достаточно будет добавить только в группу узлов этого подразделения, чтобы он мог осуществлять соединения в соответствии с имеющимися сетевыми фильтрами.

Создание шаблона политики безопасности

На узлах сети ViPNet по умолчанию заданы сетевые фильтры, содержащиеся в типовых шаблонах политики безопасности. Если политика безопасности сети требует настройки на узлах других фильтров, а также настройки правил трансляции IP-адресов, необходимо создать свои шаблоны политики безопасности.

Чтобы создать новый шаблон:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.

2 На панели просмотра (см. Рисунок 24 на стр. 66) нажмите кнопку **Создать**.

3 В окне **Свойства шаблона политики** в разделе **Основные параметры** задайте в соответствующих полях имя и описание шаблона.

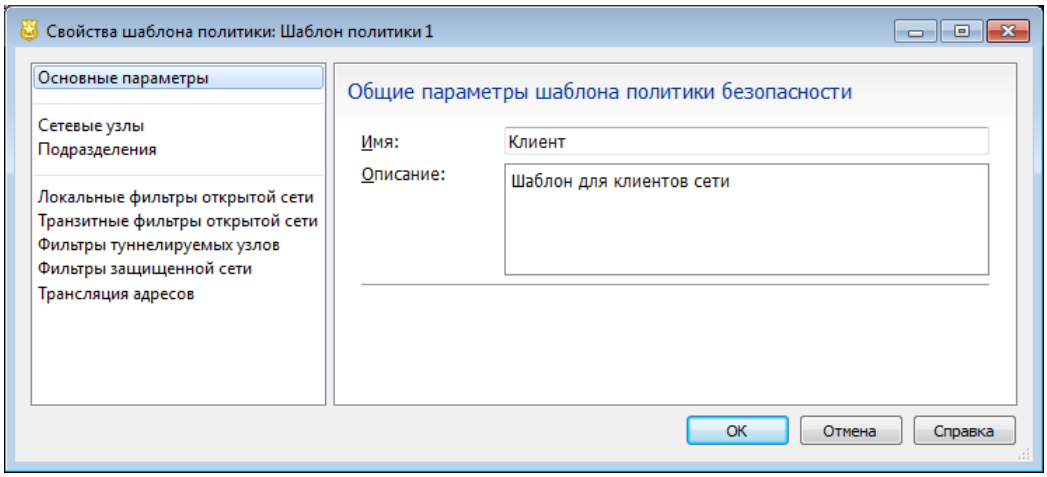

Рисунок 37. Основные параметры шаблона политики безопасности

4 Если в шаблоне требуется задать сетевые фильтры, в окне **Свойства шаблона политики** в соответствующих разделах с фильтрами задайте нужные фильтры (см. «Просмотр и изменение сетевых фильтров, заданных в шаблоне» на стр. 81).

5 Если в шаблоне требуется задать правила трансляции IP-адресов, в окне **Свойства шаблона политики** выберите раздел **Трансляция адресов** и задайте нужные правила (см. «Просмотр и изменение правил трансляции IP-адресов, заданных в шаблоне» на стр. 93).

6 Нажмите кнопку **OK**. В списке шаблонов появится новый шаблон.

Просмотр и изменение сетевых фильтров, заданных в шаблоне

Сетевые фильтры используются для блокирования или пропуска IP-пакетов в зависимости от их параметров: IP-адреса отправителя, IP-адреса получателя, используемого протокола или порта. В фильтрах задаются условия, которым должны удовлетворять IP-пакеты для применения к ним заданного действия, а также может быть задано расписание применения фильтра.

В ПО ViPNet поддерживаются следующие типы сетевых фильтров:

- Локальные фильтры открытой сети — фильтры IP-пакетов, которыми сетевые узлы ViPNet обмениваются с открытыми сетевыми узлами, то есть с узлами, на которых не установлено ПО ViPNet с функцией шифрования трафика.
- Транзитные фильтры открытой сети — фильтры открытых IP-пакетов, проходящих через координатор. Эти фильтры применяются только на сетевых узлах, являющихся координаторами.
- Фильтры для туннелируемых узлов — фильтры IP-пакетов, передаваемых координатором между туннелируемыми узлами и сетевыми узлами ViPNet. Эти фильтры применяются только на сетевых узлах, являющихся координаторами.
- Фильтры защищенной сети — фильтры IP-пакетов, которыми сетевые узлы ViPNet обмениваются между собой.

В шаблоне политики безопасности каждый тип сетевых фильтров содержится в одноименном разделе.

Чтобы просмотреть или изменить сетевые фильтры, заданные в шаблоне:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.
2. На панели просмотра (см. Рисунок 24 на стр. 66) выберите шаблон и нажмите кнопку **Свойства** или дважды щелкните шаблон.
3. В окне **Свойства шаблона политики** на левой панели выберите нужный раздел с фильтрами, например **Локальные фильтры открытой сети**.

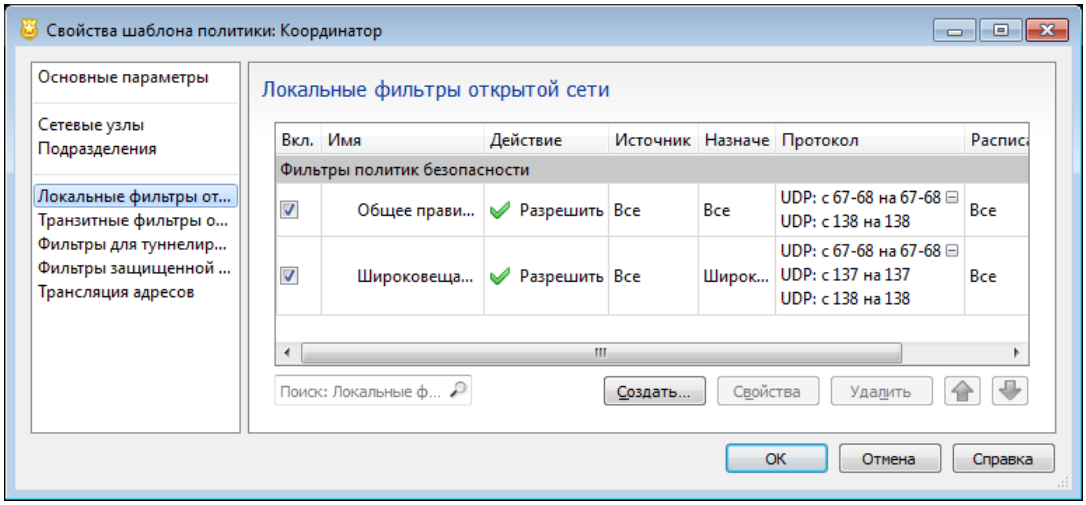

Рисунок 38. Свойства шаблона политики безопасности

4 Чтобы добавить в шаблон новый фильтр:

4.1 На правой панели нажмите кнопку **Создать**.

4.2 В окне свойств фильтра задайте параметры фильтра и нажмите кнопку **OK** (см. «Создание сетевых фильтров» на стр. 82). В списке фильтров появится новый фильтр.

5 Чтобы изменить фильтр:

5.1 На правой панели выберите фильтр и нажмите кнопку **Свойства** или дважды щелкните фильтр.

5.2 Измените параметры фильтра.

6 Чтобы удалить из шаблона фильтр:

6.1 На правой панели выберите один или несколько фильтров и нажмите кнопку **Удалить**.

6.2 В окне подтверждения еще раз нажмите кнопку **Удалить**. Выбранные фильтры будут удалены из списка локальных фильтров открытой сети.

7 Чтобы изменить порядок следования фильтров в шаблоне:

7.1 На правой панели выберите один или несколько фильтров.

7.2 С помощью кнопок и задайте нужный порядок.

8 Чтобы сохранить изменения, нажмите кнопку **OK**. Шаблон будет содержать в заданном порядке фильтры, присутствующие в списке.

Создание сетевых фильтров

Чтобы создать новый сетевой фильтр, выполните следующие действия:

1 В окне **Свойства шаблона политики** (см. Рисунок 38 на стр. 82) на левой панели выберите раздел того типа фильтров, который вы хотите создать.

2 На правой панели нажмите кнопку **Создать**. Откроется окно свойств сетевого фильтра, в котором вы можете задать параметры нового фильтра.

3 В разделе **Основные параметры** выполните следующие действия:

- Введите имя фильтра в соответствующем поле.
- Укажите действие нового фильтра (блокировать или пропускать трафик), установив переключатель **Действие** в нужное положение. По умолчанию выбрано действие **Блокировать трафик**.

4 В разделе **Источники** задайте отправителя IP-пакетов, на которые будет распространяться действие фильтра.

5 В разделе **Назначения** задайте получателя IP-пакетов, на которые будет распространяться действие фильтра.

Примечание. В разделах **Источники** и **Назначения** должны быть заданы разные адреса или диапазоны адресов, иначе фильтр нельзя будет сохранить.

---

6 В разделе **Протоколы** укажите протокол для фильтрации. Фильтром в данном случае будут обрабатываться только IP-пакеты, переданные с помощью указанного протокола.

7 В разделе **Расписание** укажите дни и время действия фильтра.

8 Для сохранения параметров нового фильтра нажмите кнопку **OK**. В результате в списке фильтров выбранного типа появится новый фильтр.

Созданный фильтр будет включен, если при задании его основных параметров не был снят соответствующий флажок. Если потребуется отключить фильтр, снимите флажок слева от его имени.

Подробнее о создании фильтров разных типов см. соответствующие разделы ниже.

Создание локальных фильтров открытой сети

Чтобы создать фильтр для локального открытого трафика, выполните следующие действия:

1 В окне **Свойства шаблона политики** (см. Рисунок 38 на стр. 82) на левой панели выберите раздел **Локальные фильтры открытой сети**.

2 На правой панели нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового фильтра.

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик.

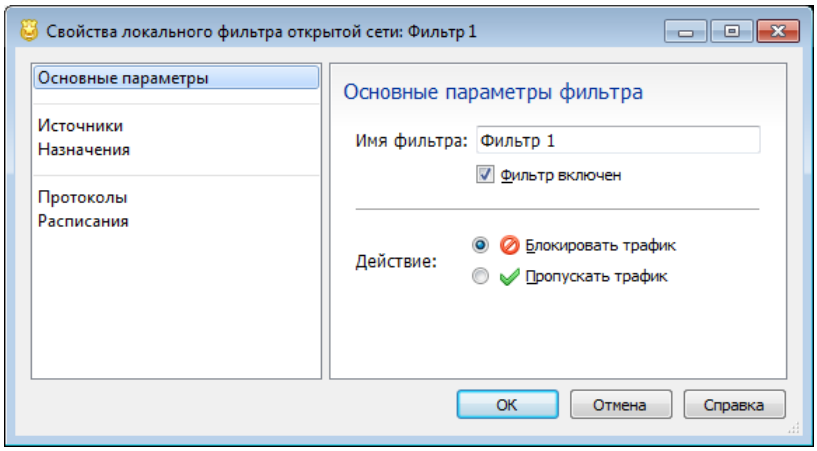

Рисунок 39. Задание основных параметров локального фильтра открытой сети

4 В разделе **Источники** задайте отправителя IP-пакетов. Для этого добавьте:

- IP-адрес или DNS-имя отправителя либо диапазон адресов, если их несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 75).
- Группы IP-адресов отправителей, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).
- Системную группу объектов **Мой узел**, если фильтр должен действовать для исходящих открытых соединений сетевого узла.
- Системную группу объектов **Другие узлы**, если фильтр должен действовать для входящих открытых соединений сетевого узла.

Если вы не укажете отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любыми открытыми узлами.

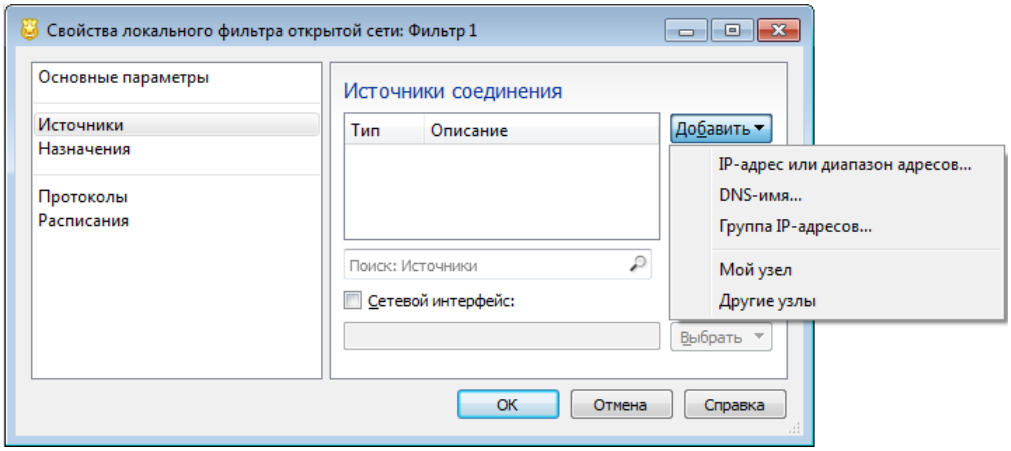

Рисунок 40. Задание отправителей открытых IP-пакетов

5 Если фильтр предназначен для координаторов, дополнительно можно указать сетевой интерфейс, на котором должны быть приняты открытые IP-пакеты от указанных источников либо с которого они должны быть отправлены (в случае, если в качестве отправителя был выбран **Мой узел**). Для этого установите флажок **Сетевой интерфейс** и добавьте:

- Отдельный IP-адрес или диапазон IP-адресов интерфейсов.

- Идентификатор интерфейса — для координаторов с ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW.
- Группу интерфейсов, если такая создана.

6 В разделе **Назначения** задайте получателя IP-пакетов. Для этого добавьте:

- IP-адрес или DNS-имя получателя либо диапазон адресов, если их несколько.
- Группы IP-адресов получателей, если такие созданы.
- Системную группу объектов **Мой узел**, если фильтр должен действовать для входящих открытых соединений сетевого узла.
- Системную группу объектов **Другие узлы**, если фильтр должен действовать для исходящих открытых соединений сетевого узла.
- Системную группу объектов **Широковещательные адреса**, если действие фильтра должно распространяться на широковещательные пакеты.
- Системную группу объектов **Групповые адреса**, если действие фильтра должно распространяться на групповую рассылку.

Если вы не укажете получателя, то действие фильтра будет распространяться на IP-пакеты, отправленные на любой открытый узел.

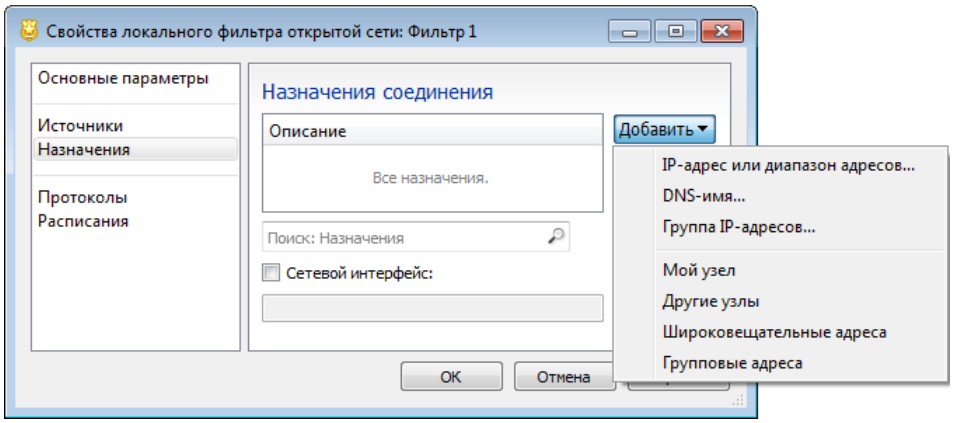

Рисунок 41. Задание получателей открытых IP-пакетов

7 Если фильтр предназначен для координаторов, дополнительно можно указать сетевой интерфейс, с которого должны быть отправлены IP-пакеты заданным получателям. Сетевой интерфейс задается так же, как описано в пункте 5.

8 В разделе **Протоколы** укажите протокол для фильтрации. Вы можете добавить нужные протоколы (см. «Добавление протоколов» на стр. 77) или группы протоколов, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).

9 В разделе **Расписания** укажите дни и время действия фильтра. Вы можете добавить новое расписание (см. «Добавление расписаний» на стр. 78) или группу расписаний, если такая создана (см. «Создание и изменение групп объектов» на стр. 70).

10 Нажмите кнопку **OK**. В результате в списке локальных фильтров открытой сети, заданных в шаблоне, появится новый фильтр.

Создание транзитных фильтров открытой сети

Чтобы создать фильтр для транзитного открытого трафика, проходящего через координатор, выполните следующие действия:

1 В окне **Свойства шаблона политики** (см. Рисунок 38 на стр. 82) на левой панели выберите раздел **Транзитные фильтры открытой сети**.

2 На правой панели нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового фильтра.

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик.

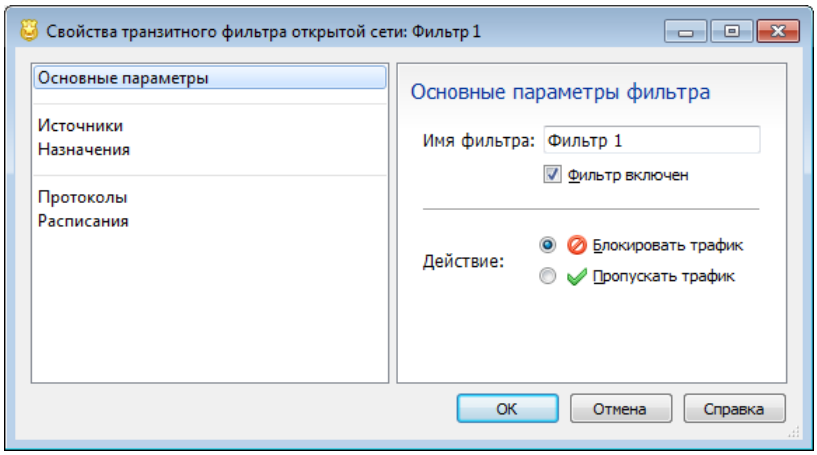

Рисунок 42. Задание основных параметров транзитного фильтра открытой сети

4 В разделе **Источники** задайте отправителя IP-пакетов. Для этого добавьте:

- IP-адрес или DNS-имя отправителя либо диапазон адресов, если их несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 75).
- Группы IP-адресов отправителей, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).

Если вы не укажете отправителя, то действие фильтра будет распространяться на транзитные IP-пакеты, отправленные любыми открытыми узлами через координатор.

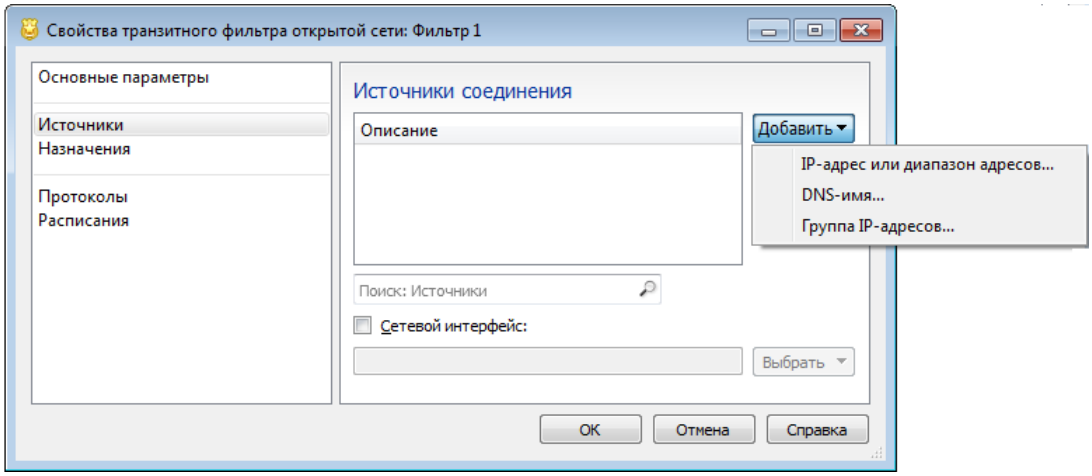

Рисунок 43. Задание отправителей транзитных IP-пакетов

5 Дополнительно можно указать сетевой интерфейс, на котором должны быть приняты транзитные IP-пакеты от указанных источников. Для этого установите флажок **Сетевой интерфейс** и добавьте:

- Отдельный IP-адрес или диапазон IP-адресов интерфейсов.
- Идентификатор интерфейса — для координаторов с ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW.
- Группу интерфейсов, если такая создана.

6 В разделе **Назначения** задайте получателя IP-пакетов. Для этого добавьте:

- IP-адрес или DNS-имя получателя либо диапазон адресов, если их несколько.
- Группы IP-адресов получателей, если такие созданы.

Если вы не укажете получателя, то действие фильтра будет распространяться на транзитные IP-пакеты, отправленные на любой открытый узел через координатор.

7 Дополнительно можно указать сетевой интерфейс, с которого должны быть отправлены транзитные IP-пакеты заданным получателям. Сетевой интерфейс задается так же, как описано в пункте 5.

8 В разделе **Протоколы** укажите протокол для фильтрации. Вы можете добавить нужные протоколы (см. «Добавление протоколов» на стр. 77) или группы протоколов, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).

9 В разделе **Расписания** укажите дни и время действия фильтра. Вы можете добавить новое расписание (см. «Добавление расписаний» на стр. 78) или группу расписаний, если такая создана (см. «Создание и изменение групп объектов» на стр. 70).

10 Нажмите кнопку **OK**. В результате в списке транзитных фильтров открытой сети, заданных в шаблоне, появится новый фильтр.

Создание фильтров для туннелируемых узлов

Чтобы создать фильтр трафика между туннелируемыми узлами координатора и защищенными узлами, выполните следующие действия:

1 В окне **Свойства шаблона политики** (см. Рисунок 38 на стр. 82) на левой панели выберите раздел **Фильтры для туннелируемых узлов**.

2 На правой панели нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового фильтра.

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик.

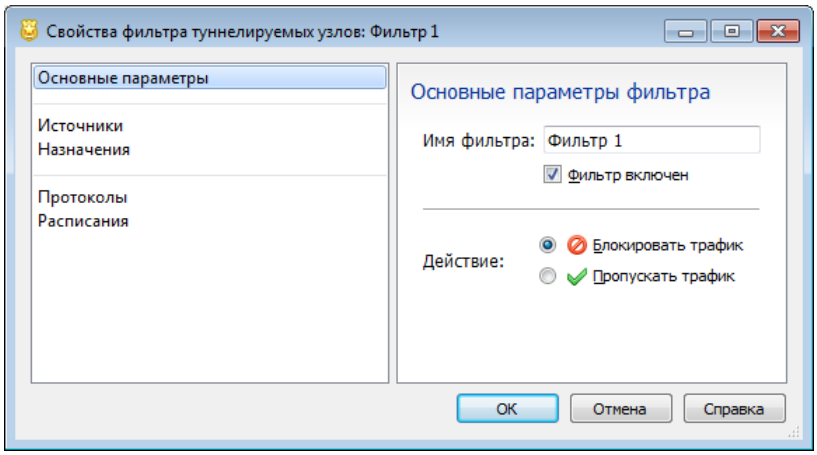

Рисунок 44. Задание основных параметров фильтра туннелируемых узлов

4 В разделе **Источники** задайте отправителя IP-пакетов при туннелированном соединении:

- Если отправителем выступает туннелируемый узел, то добавьте:
  - IP-адрес узла либо диапазон IP-адресов, если узлов несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 75).
  - Группу IP-адресов туннелируемых узлов, если такая имеется (см. «Создание и изменение групп объектов» на стр. 70).
  - Все IP-адреса узлов, туннелируемых координатором, выбрав системную группу объектов **Туннелируемые IP-адреса**.
- Если отправителем выступает защищенный узел сети ViPNet, то добавьте:
  - Один или несколько узлов защищенной сети (см. «Добавление сетевых узлов» на стр. 74).
  - Одну или несколько групп узлов сети ViPNet, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).
  - Все координаторы, связанные с узлом, выбрав системную группу объектов **Все координаторы**.
  - Все клиенты, связанные с узлом, выбрав системную группу объектов **Все клиенты**.

Примечание. Если в качестве отправителя выступает туннелируемый узел, то получателем может быть выбран только узел или узлы защищенной сети, и наоборот.

Если вы не укажете узел отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любыми туннелируемыми узлами либо любыми защищенными узлами, в зависимости от того, какие заданы узлы назначения.

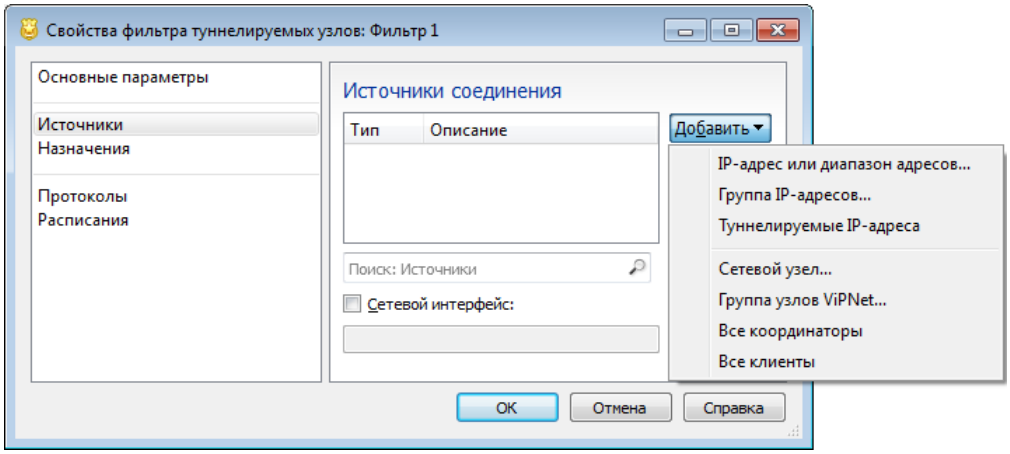

Рисунок 45. Задание отправителей туннелируемых IP-пакетов

5 Дополнительно можно указать сетевой интерфейс, на котором должны быть приняты IP-пакеты от заданных источников при туннелированном соединении. Для этого установите флажок **Сетевой интерфейс** и добавьте:

- Отдельный IP-адрес или диапазон IP-адресов интерфейсов.
- Идентификатор интерфейса — для координаторов с ПО ViPNet Coordinator for Linux и ПАК ViPNet Coordinator HW.
- Группу интерфейсов, если такая создана.

6 В разделе **Назначения** задайте получателя IP-пакетов туннелированного соединения. Если в качестве отправителя выступает туннелируемый узел, то получателем будет узел или несколько узлов сети ViPNet. Если выбран отправитель со стороны сети ViPNet, то получателем в данном случае может быть только туннелируемый узел.

Добавление получателя производится так же, как добавление отправителя (см. пункт 4). Если вы не укажете получателя, то действие фильтра будет распространяться на IP-пакеты, отправленные на любой туннелируемый узел либо на любой защищенный узел, в зависимости от того, какие узлы являются отправителями.

7 Дополнительно можно указать сетевой интерфейс, с которого должны быть отправлены IP-пакеты заданным получателям при туннелированном соединении. Сетевой интерфейс задается так же, как описано в пункте 5.

8 В разделе **Протоколы** укажите протокол для фильтрации. Вы можете добавить нужные протоколы (см. «Добавление протоколов» на стр. 77) или группы протоколов, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).

9 В разделе **Расписания** укажите дни и время действия фильтра. Вы можете добавить новое расписание (см. «Добавление расписаний» на стр. 78) или группу расписаний, если такая создана (см. «Создание и изменение групп объектов» на стр. 70).

10 Нажмите кнопку **OK**. В результате в списке фильтров для туннелируемых узлов, заданных в шаблоне, появится новый фильтр.

Создание фильтров защищенной сети

Чтобы создать фильтр для защищенного трафика, выполните следующие действия:

1 В окне **Свойства шаблона политики** (см. Рисунок 38 на стр. 82) на левой панели выберите раздел **Фильтры защищенной сети**.

2 На правой панели нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового фильтра.

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик.

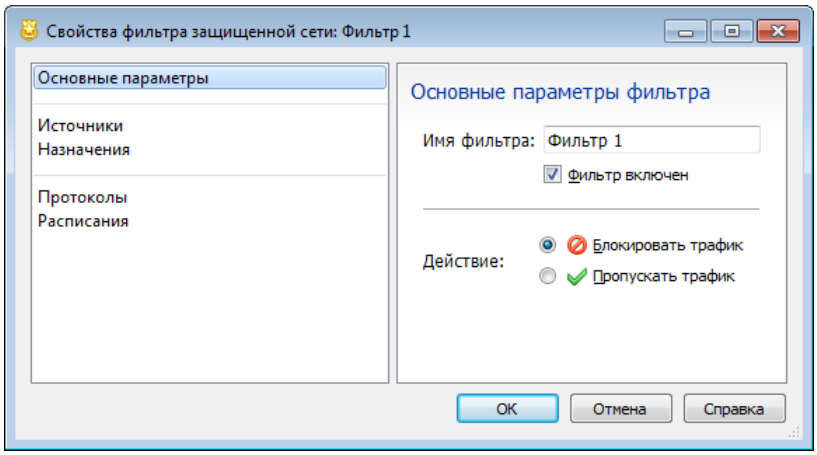

Рисунок 46. Задание основных параметров фильтра защищенной сети

4 В разделе **Источники** задайте отправителя IP-пакетов. Для этого добавьте:

- Один или несколько узлов защищенной сети (см. «Добавление сетевых узлов» на стр. 74).
- Одну или несколько групп узлов сети ViPNet, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).
- Системную группу объектов **Мой узел**, если фильтр должен действовать для исходящих соединений сетевого узла.
- Системную группу объектов **Другие узлы**, если фильтр должен действовать для входящих соединений сетевого узла.
- Все координаторы, связанные с узлом, выбрав системную группу объектов **Все координаторы**.
- Все клиенты, связанные с узлом, выбрав системную группу объектов **Все клиенты**.

Если вы не укажете отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любыми защищенными узлами.

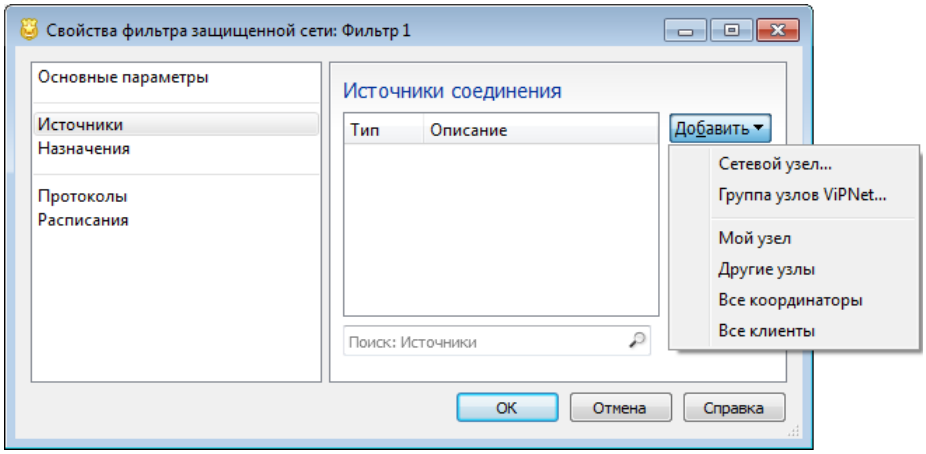

Рисунок 47. Задание отправителей защищенных IP-пакетов

5 В разделе **Назначения** задайте получателя защищенных IP-пакетов. Для этого добавьте:

- Один или несколько узлов защищенной сети.
- Одну или несколько групп узлов сети ViPNet, если такие созданы.
- Системную группу объектов **Мой узел**, если фильтр должен действовать для входящих соединений сетевого узла.
- Системную группу объектов **Другие узлы**, если фильтр должен действовать для исходящих соединений сетевого узла.
- Все координаторы, связанные с узлом, выбрав системную группу объектов **Все координаторы**.
- Все клиенты, связанные с узлом, выбрав системную группу объектов **Все клиенты**.
- Широковещательные адреса, выбрав системную группу объектов **Широковещательные адреса**. В этом случае действие фильтра будет распространяться на широковещательные пакеты.

Совет. Если в качестве получателя указать **Широковещательные адреса**, в качестве отправителя — **Мой узел** или **Другие узлы** (см. пункт 4), то будут созданы фильтры для исходящих или входящих широковещательных IP-пакетов соответственно.

Если вы не укажете получателя, то действие фильтра будет распространяться на IP-пакеты, отправленные на любой защищенный узел.

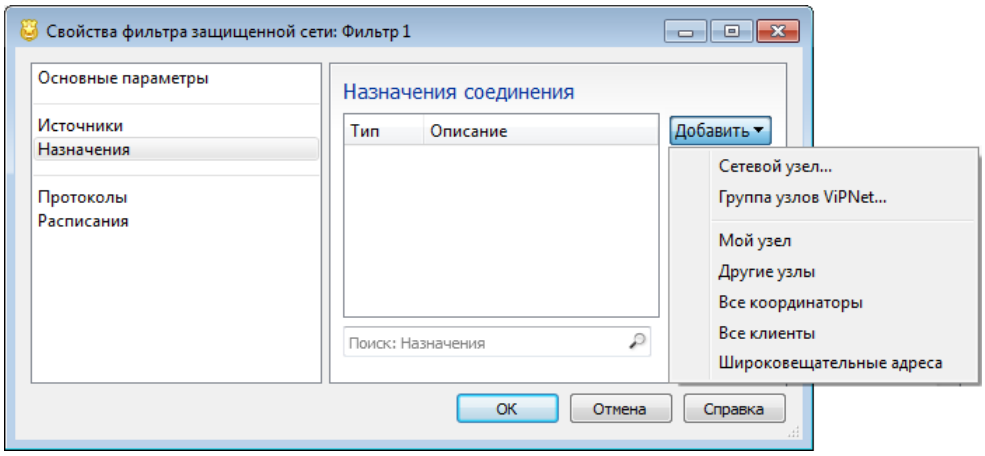

Рисунок 48. Задание получателей защищенных IP-пакетов

6 В разделе **Протоколы** укажите протокол для фильтрации. Вы можете добавить нужные протоколы (см. «Добавление протоколов» на стр. 77) или группы протоколов, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).

7 В разделе **Расписания** укажите дни и время действия фильтра. Вы можете добавить новое расписание (см. «Добавление расписаний» на стр. 78) или группу расписаний, если такая создана (см. «Создание и изменение групп объектов» на стр. 70).

8 Нажмите кнопку **OK**. В результате в списке фильтров защищенной сети, заданных в шаблоне, появится новый фильтр.

Рекомендации по созданию сетевых фильтров

Чтобы обеспечить стабильную работу ПО ViPNet, необходимо контролировать число создаваемых фильтров, потому что оно зависит от количества узлов, на которые будет распространяться действие каждого из фильтров. Мы рекомендуем придерживаться следующих ограничений:

- Если действие каждого из создаваемых фильтров распространяется на один сетевой узел или IP-адрес, общее количество фильтров не должно превышать 3000.
- Если действие каждого из создаваемых фильтров распространяется на два или большее количество сетевых узлов или IP-адресов, общее количество сетевых узлов или IP-адресов, на которые будут распространяться действия всех созданных фильтров, не должно превышать 700. При этом действие одного фильтра не должно распространяться более чем на 500 сетевых узлов или IP-адресов.

Просмотр и изменение правил трансляции IP-адресов, заданных в шаблоне

В правилах трансляции задаются правила преобразования IP-адресов на координаторе. Эти правила применяются только на сетевых узлах, являющихся координаторами.

Чтобы просмотреть или изменить правила трансляции, заданные в шаблоне:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.

2 На панели просмотра (см. Рисунок 24 на стр. 66) выберите шаблон и нажмите кнопку **Свойства** или дважды щелкните шаблон.

3 В окне **Свойства шаблона политики** на левой панели выберите раздел **Трансляция адресов**.

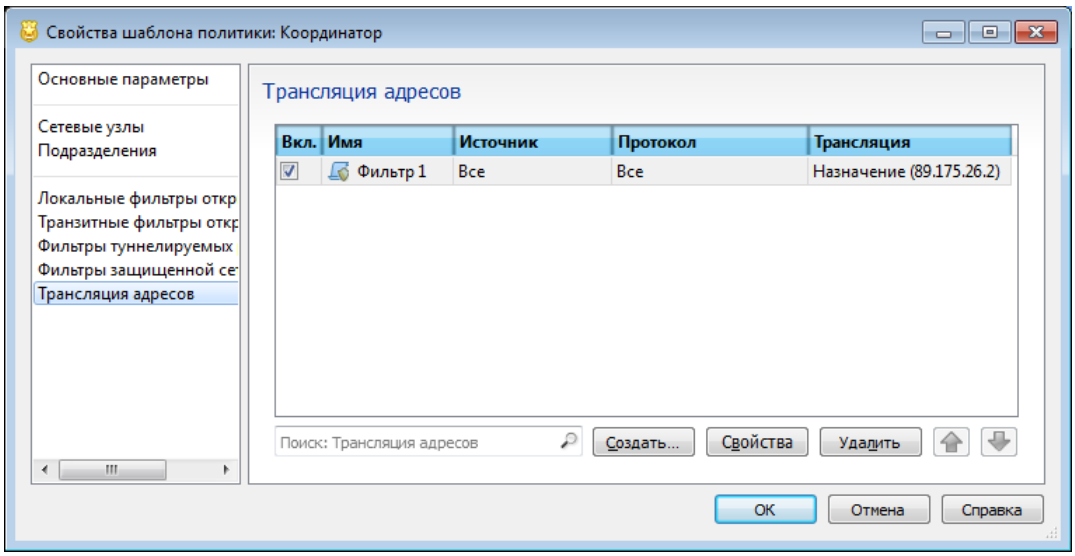

Рисунок 49. Правила трансляции IP-адресов

4 Чтобы добавить в шаблон новое правило трансляции:

4.1 На правой панели нажмите кнопку **Создать**.

4.2 В окне **Свойства правила трансляции адресов** задайте параметры правила и нажмите кнопку **OK** (см. «Создание и изменение правила трансляции IP-адресов» на стр. 94). В списке правил трансляции появится новое правило.

5 Чтобы изменить правило трансляции:

5.1 На правой панели выберите правило и нажмите кнопку **Свойства** или дважды щелкните правило.

5.2 Измените параметры правила (см. «Создание и изменение правила трансляции IP-адресов» на стр. 94).

6 Чтобы удалить из шаблона правило трансляции:

6.1 На правой панели выберите одно или несколько правил и нажмите кнопку **Удалить**.

6.2 В окне подтверждения еще раз нажмите кнопку **Удалить**. Выбранные правила будут удалены из списка правил трансляции.

7 Чтобы изменить порядок следования правил в шаблоне:

7.1 На правой панели выберите одно или несколько правил.

7.2 С помощью кнопок и задайте нужный порядок.

8 Чтобы сохранить изменения, нажмите кнопку **OK**. Шаблон будет содержать в заданном порядке правила, присутствующие в списке.

Создание и изменение правила трансляции IP-адресов

Чтобы создать новое правило трансляции IP-адресов, выполните следующие действия:

1 В окне **Свойства шаблона политики** (см. Рисунок 38 на стр. 82) на левой панели выберите раздел **Трансляция адресов**.

2 На правой панели нажмите кнопку **Создать**.

3 В окне **Свойства правила трансляции адресов** в разделе **Основные параметры** введите имя правила.

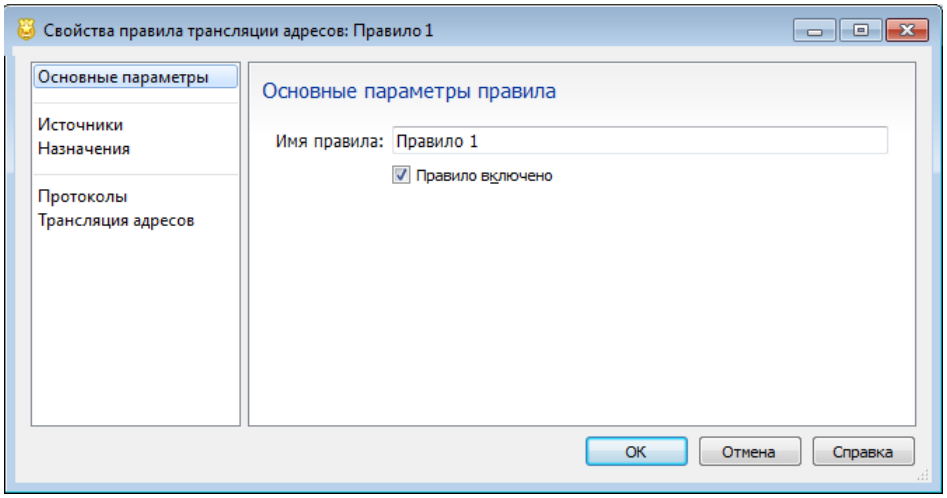

Рисунок 50. Основные параметры правила трансляции

4 Если необходимо транслировать адреса отправителей пакетов, в разделе **Источники** задайте нужные адреса. Для этого нажмите кнопку **Добавить** и в меню выберите:

- IP-адрес либо диапазон адресов, если их несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 75).
- Группы IP-адресов отправителей, если такие созданы (см. «Создание и изменение групп объектов» на стр. 70).

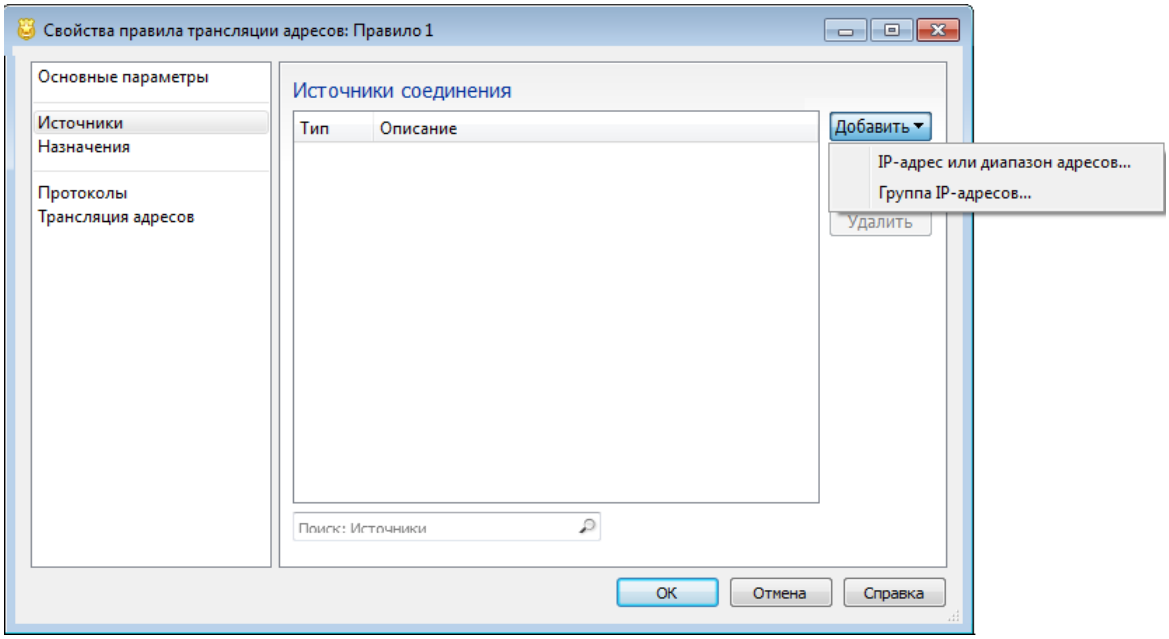

Рисунок 51. Источники правила трансляции

5 Если необходимо транслировать адрес получателя пакетов, в разделе **Назначения** задайте нужный адрес. Добавление получателя производится так же, как добавление отправителя (см. пункт 4).

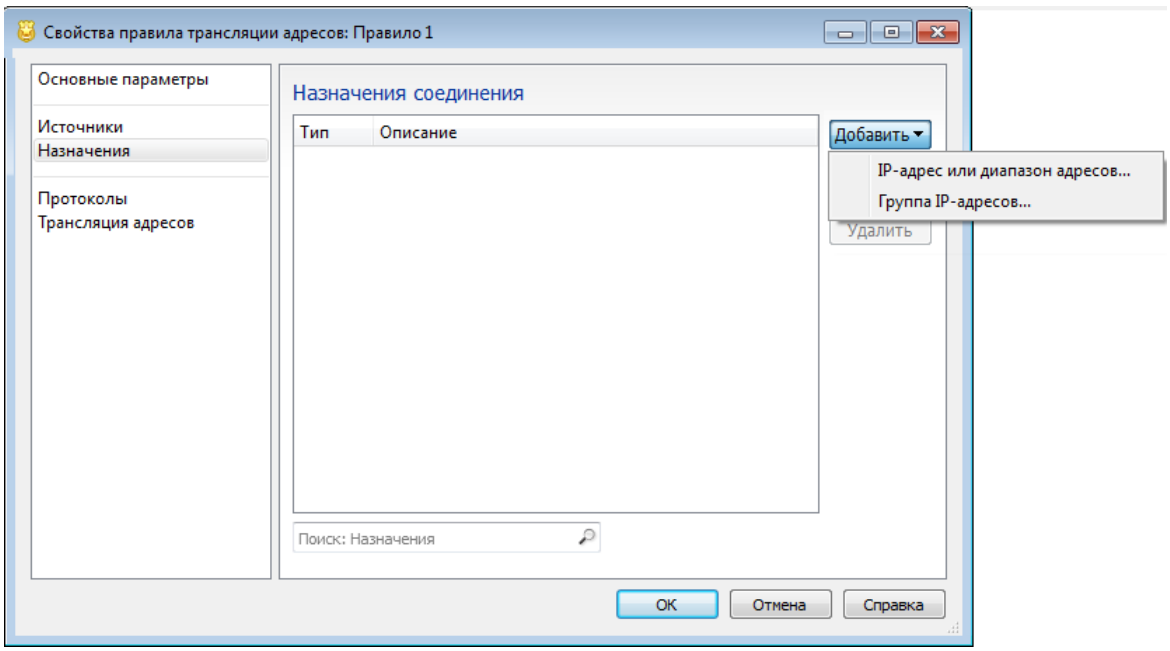

Рисунок 52. Назначения правила трансляции

6 В разделе **Трансляция адресов** задайте правило преобразования адресов.

6.1 Чтобы задать трансляцию адресов отправителей:

- В группе параметров **Трансляция источника** установите флажок **Заменять адрес источника на**.
- Установите переключатель в положение **Адрес исходящего интерфейса (определяется автоматически)**. В этом случае адрес отправителя будет заменяться на адрес внешнего интерфейса координатора, который определяется автоматически.
- Если необходимо задать другой адрес, установите переключатель в положение **Другой адрес** и в поле справа от флажка введите IP-адрес.

6.2 Чтобы задать трансляцию адреса получателя:

- В группе параметров **Трансляция назначения** установите флажок **Заменять адрес назначения на** и в поле справа от флажка введите IP-адрес.
- Если необходимо изменять порт, установите флажок **Заменять порт назначения на** и выберите в списке нужный порт.

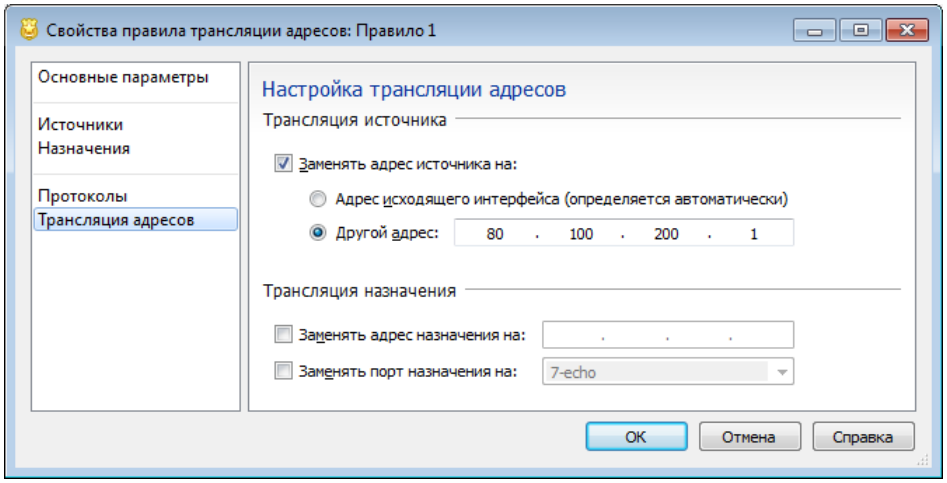

Рисунок 53. Трансляция адресов

7 Нажмите кнопку **OK**, чтобы сохранить правило.

Чтобы изменить правило трансляции IP-адресов, выполните следующие действия:

1 В окне **Свойства шаблона политики** на левой панели выберите раздел **Трансляция адресов**.

2 На правой панели выберите правило и нажмите кнопку **Свойства** или дважды щелкните правило.

3 В окне **Свойства правила трансляции адресов** измените параметры правила таким же образом, как при создании нового правила.

4 Нажмите кнопку **OK**, чтобы сохранить изменения.

Копирование шаблона политики безопасности

Если для отдельных сетевых узлов вам необходимо на основе уже существующего шаблона политики безопасности создать другой шаблон с незначительными изменениями в настройках параметров сетевых фильтров и правилах трансляции, вы можете скопировать существующий шаблон и внести необходимые изменения.

Чтобы скопировать шаблон политики безопасности, выполните следующие действия:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.

2 Выберите шаблон, который хотите скопировать, вызовите контекстное меню и выберите команду **Создать копию**.

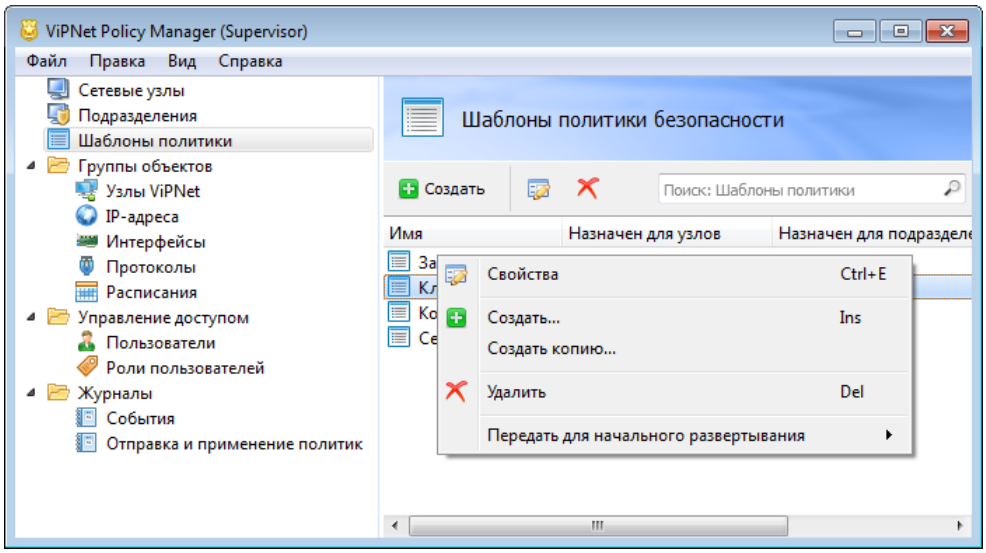

Рисунок 54. Копирование шаблона

3 В окне **Свойства шаблона политики** измените имя шаблона и его описание.

4 Если необходимо, измените параметры сетевых фильтров и правила трансляции IP-адресов, следуя рекомендациям из следующих разделов:

- Просмотр и изменение сетевых фильтров, заданных в шаблоне (на стр. 81).
- Просмотр и изменение правил трансляции IP-адресов, заданных в шаблоне (на стр. 93).

5 Нажмите кнопку **OK**, чтобы сохранить изменения.

Удаление шаблона политики безопасности

Неиспользуемый шаблон можно удалить. Для этого:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.
2. На панели просмотра (см. Рисунок 24 на стр. 66) выберите один или несколько шаблонов и нажмите кнопку **Удалить** ✕.
3. В окне подтверждения нажмите кнопку **Удалить**. Выбранные шаблоны будут удалены из списка шаблонов.

Назначение шаблона сетевым узлам и подразделениям

Шаблон политики безопасности можно назначить как отдельным сетевым узлам, так и подразделениям. Шаблоны, назначенные подразделению, распространяются на все сетевые узлы, входящие в его состав.

Назначить шаблон политики безопасности можно разными способами:

- Назначить шаблон отдельному сетевому узлу (см. «Назначение шаблона одному сетевому узлу» на стр. 99). Этот способ позволяет также назначить узлу сразу несколько шаблонов.
- Назначить шаблон нескольким сетевым узлам за один прием (см. «Назначение шаблона нескольким сетевым узлам» на стр. 100).
- Назначить шаблон отдельному подразделению (см. «Назначение шаблона одному подразделению» на стр. 101). Этот способ позволяет также назначить подразделению сразу несколько шаблонов.
- Назначить шаблон нескольким подразделениям за один прием (см. «Назначение шаблона нескольким подразделениям» на стр. 103).

Назначение шаблона одному сетевому узлу

Чтобы назначить шаблон политики безопасности одному сетевому узлу, выполните следующие действия:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Сетевые узлы**.
2. На панели просмотра (см. Рисунок 17 на стр. 54) выберите сетевой узел и нажмите кнопку **Свойства** или дважды щелкните узел.
3. В окне **Свойства сетевого узла** на левой панели выберите раздел **Шаблоны политик**.

   На правой панели будет отображен список шаблонов, уже назначенных узлу.

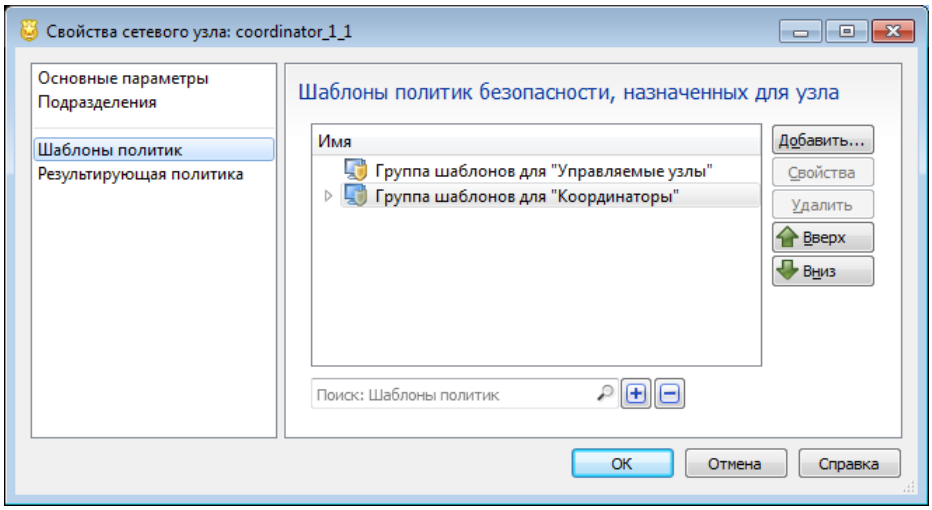

Рисунок 55. Список шаблонов политики безопасности, назначенных узлу

4 Нажмите кнопку **Добавить**.

5 В открывшемся окне выберите в списке один или несколько шаблонов и нажмите кнопку **OK**. Выбранные шаблоны будут добавлены в список шаблонов, назначенных узлу.

6 Если необходимо изменить положение шаблона в списке, используйте кнопки **Вверх** и **Вниз**.

Примечание. Порядок следования шаблонов определяет их приоритет: он уменьшается от первого в списке шаблона к последнему.

---

7 Нажмите кнопку **OK**, чтобы сохранить изменения.

Если из списка шаблонов, назначенных узлу, необходимо удалить какие-либо шаблоны, выполните следующее:

1 В списке назначенных шаблонов выберите один или несколько шаблонов и нажмите кнопку **Удалить**.

2 В окне подтверждения нажмите кнопку **Удалить**. Выбранные шаблоны будут исключены из списка.

3 Нажмите кнопку **OK**, чтобы сохранить изменения.

Назначение шаблона нескольким сетевым узлам

Шаблон политики безопасности можно назначить сразу нескольким сетевым узлам. Для этого:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.

2 На панели просмотра (см. Рисунок 24 на стр. 66) выберите шаблон и нажмите кнопку **Свойства** или дважды щелкните шаблон.

3 В окне **Свойства шаблона политики** на левой панели выберите раздел **Сетевые узлы**.

На правой панели будет отображен список узлов, которым уже назначен данный шаблон.

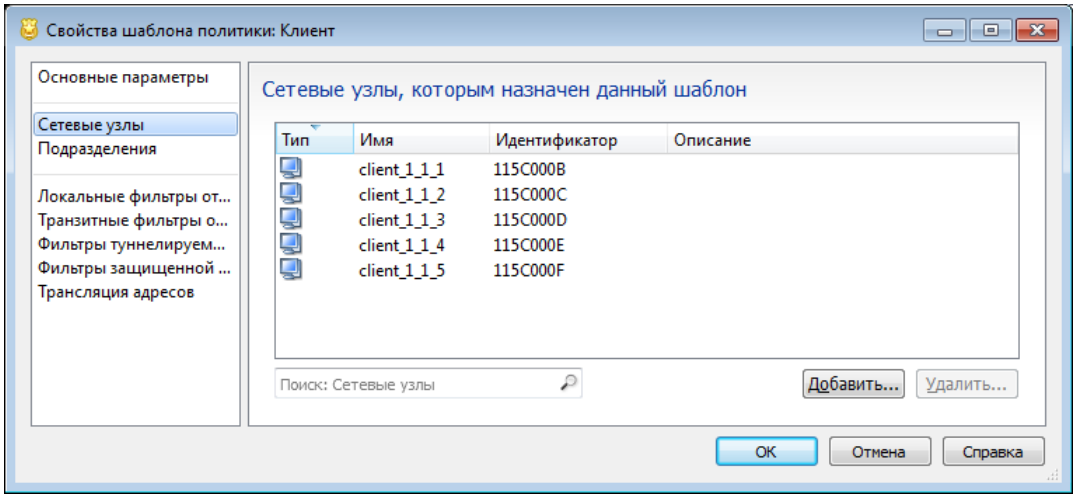

Рисунок 56. Сетевые узлы, которым назначен шаблон

4 Нажмите кнопку **Добавить**.

5 В открывшемся окне выберите в списке один или несколько узлов и нажмите кнопку **OK**. Выбранные узлы будут добавлены в список узлов, которым назначен шаблон.

6 Нажмите кнопку **OK**, чтобы сохранить изменения.

Если из списка узлов, которым назначен шаблон, необходимо удалить какие-либо узлы, выполните следующее:

1 В списке узлов, которым назначен шаблон, выберите один или несколько узлов и нажмите кнопку **Удалить**.

2 В окне подтверждения нажмите кнопку **Удалить**. Выбранные узлы будут исключены из списка.

3 Нажмите кнопку **OK**, чтобы сохранить изменения.

Назначение шаблона одному подразделению

Чтобы назначить шаблон политики безопасности одному подразделению, выполните следующие действия:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.

2 На панели просмотра (см. Рисунок 19 на стр. 58) выберите подразделение и нажмите кнопку **Свойства** или дважды щелкните подразделение.

3 В окне **Свойства подразделения** на левой панели выберите раздел **Шаблоны политик**.

На правой панели будет отображен список шаблонов, уже назначенных подразделению.

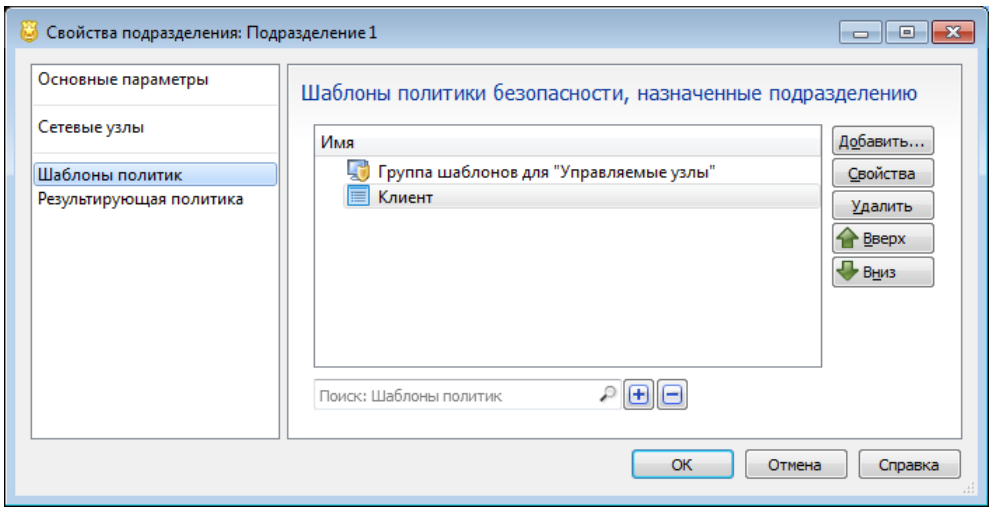

Рисунок 57. Список шаблонов политики безопасности, назначенных подразделению

4 Нажмите кнопку **Добавить**.

5 В открывшемся окне выберите в списке один или несколько шаблонов и нажмите кнопку **OK**. Выбранные шаблоны будут добавлены в список шаблонов, назначенных подразделению.

6 Если необходимо изменить положение шаблона в списке, используйте кнопки **Вверх** и **Вниз**.

Примечание. Порядок следования шаблонов определяет их приоритет: он уменьшается от первого в списке шаблона к последнему.

---

7 Нажмите кнопку **OK**, чтобы сохранить изменения.

Если из списка шаблонов, назначенных подразделению, необходимо удалить какие-либо шаблоны, выполните следующее:

1 В списке назначенных шаблонов выберите один или несколько шаблонов и нажмите кнопку **Удалить**.

2 В окне подтверждения нажмите кнопку **Удалить**. Выбранные шаблоны будут исключены из списка.

3 Нажмите кнопку **OK**, чтобы сохранить изменения.

Назначение шаблона нескольким подразделениям

Шаблон политики безопасности можно назначить сразу нескольким подразделениям. Для этого:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Шаблоны политики**.

2 На панели просмотра (см. Рисунок 24 на стр. 66) выберите шаблон и нажмите кнопку **Свойства** или дважды щелкните шаблон.

3 В окне **Свойства шаблона политики** на левой панели выберите раздел **Подразделения**.

На правой панели будет отображена иерархия подразделений. Те подразделения, которым уже назначен данный шаблон, отмечены флажком.

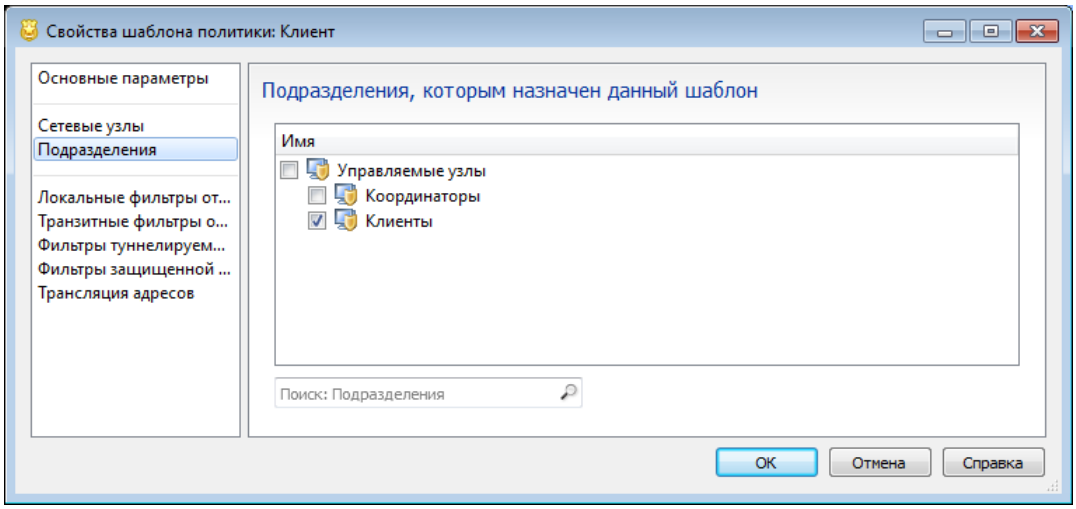

Рисунок 58. Подразделения, которым назначен шаблон

4 Установите флажки напротив тех подразделений, которым требуется назначить шаблон, и снимите флажки напротив подразделений, которым не надо назначать шаблон.

5 Нажмите кнопку **OK**, чтобы сохранить изменения.

9

Рассылка политик безопасности на сетевые узлы

Правила формирования результирующей политики безопасности 105

Отправка и получение политик безопасности 107

Применение политик безопасности на сетевых узлах 108

Просмотр результирующей политики безопасности 109

Выборочная рассылка 111

Групповая рассылка 112

Журнал отправки и применения политик безопасности 113

Правила формирования результирующей политики безопасности

Формирование результирующей политики безопасности происходит автоматически при рассылке политик безопасности на сетевые узлы. Для отправки политик безопасности на отдельный узел или небольшое число узлов используется выборочная рассылка (см. «Выборочная рассылка» на стр. 111). Рассылка политик безопасности на все узлы, входящие в подразделение, или на все управляемые сетевые узлы осуществляется с помощью групповой рассылки (см. «Групповая рассылка» на стр. 112).

Результирующая политика безопасности узла представляет собой результат объединения (с учетом приоритета) шаблонов, назначенных узлу и подразделениям, в которые входит данный узел. Если при этом имеются повторяющиеся шаблоны, в результирующую политику включается только один шаблон — тот, который имеет наибольший приоритет. При формировании результирующей политики учитываются шаблоны не только тех подразделений, в которые узел включен непосредственно, но и подразделений, вышестоящих по отношению к подразделениям узла (см. пример ниже).

Настройки из шаблонов, включенных в результирующую политику безопасности, группируются по типам согласно структуре шаблонов (см. «Общие сведения о шаблонах политики безопасности» на стр. 66).

Рассмотрим формирование результирующей политики безопасности для отдельного узла на следующем примере:

- Пусть сетевой узел входит в состав подразделений А1 и Б, причем у подразделения А1 есть вышестоящее подразделение А.
- Пусть узлу и подразделениям назначены следующие шаблоны (в порядке уменьшения приоритета):
  - подразделению А — Шаблон_1;
  - подразделению А1 — шаблоны подразделения А, Шаблон_2, Шаблон_3 и Шаблон_6;
  - подразделению Б — Шаблон_1, Шаблон_4 и Шаблон_5;
  - сетевому узлу — шаблоны подразделения А1, шаблоны подразделения Б, Шаблон_6, Шаблон_7 и Шаблон_8.

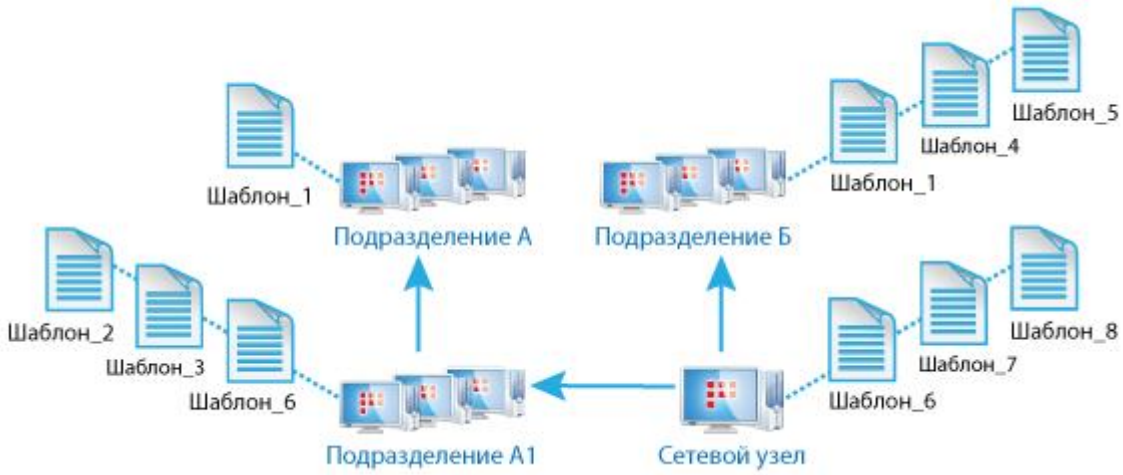

Рисунок 59. Пример формирования результирующей политики безопасности

В этом случае для сетевого узла будет сформирован результирующий список шаблонов, приведенный в таблице ниже.

Таблица 8. Последовательность формирования результирующего списка шаблонов

Подразделения / узлы	**Исходный список назначенных шаблонов**	**Результирующий список шаблонов (после удаления повторов)**
Подразделение А	Шаблон_1	Шаблон_1
Подразделение А1	Шаблон_2	Шаблон_2
	Шаблон_3	Шаблон_3
	Шаблон_6	Шаблон_6
Подразделение Б	Шаблон_1	Шаблон_4
	Шаблон_4	Шаблон_5
	Шаблон_5	Шаблон_7
Сетевой узел	Шаблон_6	Шаблон_8
	Шаблон_7	
	Шаблон_8	

Отправка и получение политик безопасности

Результирующая политика безопасности отправляется на сетевые узлы в виде xml-файла специального формата. Для обеспечения контроля целостности файла ViPNet Policy Manager вычисляет его контрольную сумму, которую сохраняет в отдельном файле с расширением `*.crg`. Файл с контрольной суммой рассылается на узлы вместе с политикой безопасности.

Внимание! Прежде чем отправить политику безопасности на узел, убедитесь, что на этом узле после добавления его в список управляемых узлов были обновлены справочники. Подробнее см. документ ViPNet Центр управления сетью. Руководство администратора«, раздел »Обновление справочников и ключей«.

При получении политики безопасности проверяется целостность файла: на узле вычисляется контрольная сумма полученного файла и сравнивается с присланной контрольной суммой. Если контрольные суммы не совпадают (то есть целостность файла нарушена), то на узле выводится сообщение об ошибке, и политика безопасности не принимается.

После проверки целостности файла, содержащего политику безопасности, и попытки применения политики на узле формируется квитанция о принятии или отклонении политики безопасности. Эта квитанция отправляется на узел с ViPNet Policy Manager, который изменяет статус политики безопасности узла согласно полученной квитанции. Текущий статус политики безопасности для каждого узла отображается в разделе **Сетевые узлы** (см. »Просмотр списка управляемых сетевых узлов« на стр. 54).

Внимание! Перед началом работы с программой ViPNet Policy Manager убедитесь, что сетевые узлы, на которые вы собираетесь отправить политики безопасности, включены в список узлов, управляемых с помощью ViPNet Policy Manager.

Применение политик безопасности на сетевых узлах

Политика безопасности, полученная сетевым узлом из программы ViPNet Policy Manager, определяет текущую политику безопасности узла, совместно с сетевыми фильтрами, настроенными на самом узле. Сетевые фильтры, полученные в составе политики безопасности, не могут быть изменены на сетевом узле.

Текущая политика безопасности, сформированная с учетом принятой политики, действительна для всех пользователей, зарегистрированных на узле, и для всех конфигураций ПО ViPNet. При добавлении новых пользователей или конфигураций к ним также применяется текущая политика.

На сетевом узле с установленным ПО ViPNet Client или ViPNet Coordinator принятые сетевые фильтры отображаются в программе ViPNet Монитор в соответствующих списках сетевых фильтров. Они расположены в группе **Фильтры политик безопасности** и имеют приоритет над фильтрами, настроенными на сетевом узле.

Вкл.	Действие	Имя	Источник	Назначение	Протокол	Расписание
Фильтры политик безопасности						
☑	Разрешить	<Все защищенные узлы>	Все	Все	Все	Все
☑	Разрешить	Широковещательные фильтры<Все з...	Все	Широкове...	UDP: с 67-68 н	Все
Настраиваемые фильтры						
☑	Разрешить	DHCP-трафик	Все	Все	DHCP	Все
☑	Разрешить	NetBIOS- и WINS-трафик	Все	Все	NetBIOS-DGM	Все
☑	Разрешить	Служебный трафик ViPNet	Все	Все	ViPNet базовы	Все
☑	Разрешить	Ping	Все	Все	ICMP8	Все
☑	Блокировать	Широковещательный трафик	Все	Широкове...	Все	Все
☑	Разрешить	Прочий исходящий трафик	Мой узел	Все	Все	Все
Фильтры по умолчанию						
☑	Блокировать	Прочий трафик	Все	Все	Все	Все

Рисунок 60. Фильтры, полученные из программы ViPNet Policy Manager

На сетевом узле с установленным ПО ViPNet Coordinator Linux принятые сетевые фильтры содержатся в файле `p_mon.xml` вместе с фильтрами, настроенными на сетевом узле, и имеют над ними приоритет. Просмотреть список сетевых фильтров можно с помощью специальной команды. Более подробную информацию см. в документе «ViPNet Coordinator Linux. Руководство администратора».

Просмотр результирующей политики безопасности

Перед отправкой политики безопасности на сетевые узлы ее можно просмотреть с целью проверки, а также сохранить в файле и распечатать.

Чтобы просмотреть результирующую политику безопасности отдельного узла, выполните следующие действия:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Сетевые узлы**.

2 На панели просмотра (см. Рисунок 17 на стр. 54) выберите сетевой узел и нажмите кнопку **Свойства** или дважды щелкните узел.

3 В окне **Свойства сетевого узла** на левой панели выберите раздел **Результирующая политика**.

На правой панели будет отображена результирующая политика безопасности узла.

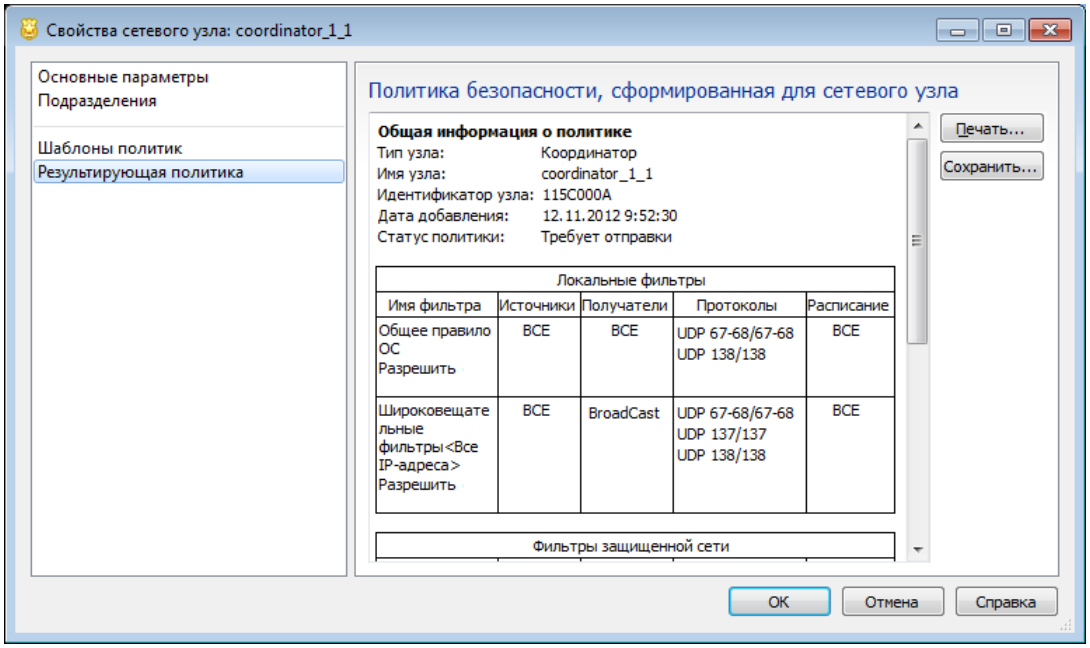

Рисунок 61. Результирующая политика безопасности узла

4 Чтобы сохранить результирующую политику безопасности в файле, нажмите кнопку **Сохранить** и укажите папку и имя файла. Политика безопасности будет сохранена в файле формата HTML.

5 Чтобы распечатать результирующую политику безопасности, нажмите кнопку **Печать**, затем в окне параметров печати выберите принтер и также нажмите кнопку **Печать**.

Чтобы просмотреть результирующую политику безопасности подразделения, выполните следующие действия:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.

2 На панели просмотра (см. Рисунок 19 на стр. 58) выберите подразделение и нажмите кнопку **Свойства** или дважды щелкните подразделение.

3 В окне **Свойства подразделения** на левой панели выберите раздел **Результирующая политика**.

На правой панели будет отображена результирующая политика безопасности подразделения.

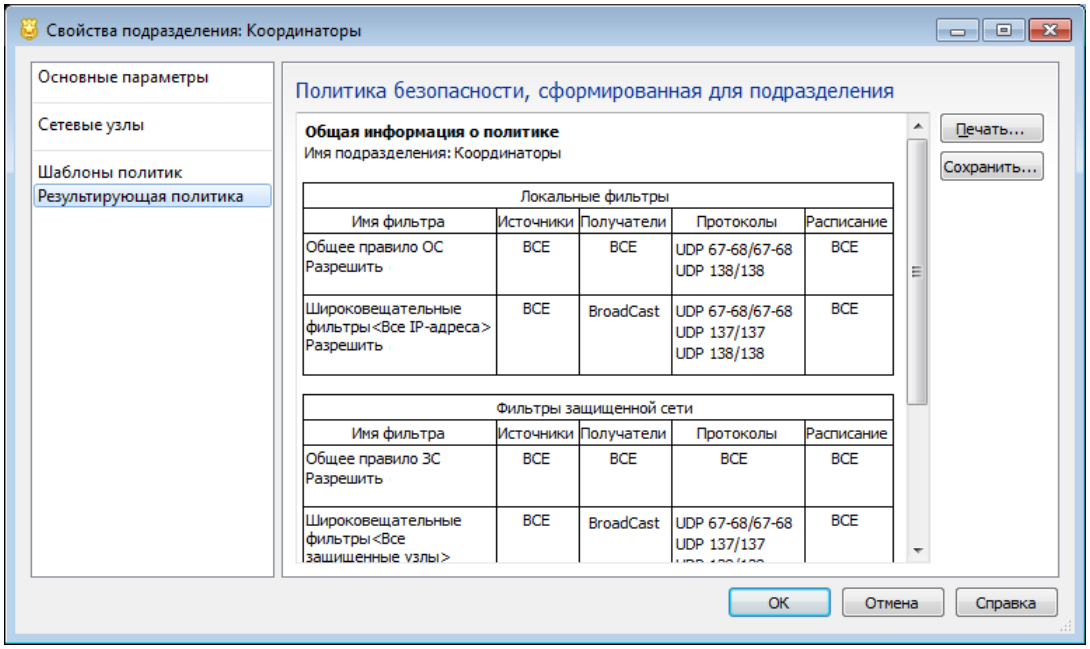

Рисунок 62. Результирующая политика безопасности подразделения

4 Чтобы сохранить результирующую политику безопасности в файле, нажмите кнопку **Сохранить** и укажите папку и имя файла. Политика безопасности будет сохранена в файле формата HTML.

5 Чтобы распечатать результирующую политику безопасности, нажмите кнопку **Печать**, затем в окне параметров печати выберите принтер и также нажмите кнопку **Печать**.

Выборочная рассылка

Выборочная рассылка используется в случае, когда политики безопасности надо отправить на ограниченное число узлов.

Чтобы выполнить выборочную рассылку:

1 В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Сетевые узлы**.

2 На панели просмотра (см. Рисунок 17 на стр. 54) выберите один или несколько узлов со статусом политики безопасности **Требует отправки**.

3 Нажмите кнопку **Отправить политики**.

4 В окне **Отправка политики** задайте условие применения политик на узлах. При выборе пункта **В указанное время** задайте дату и время применения.

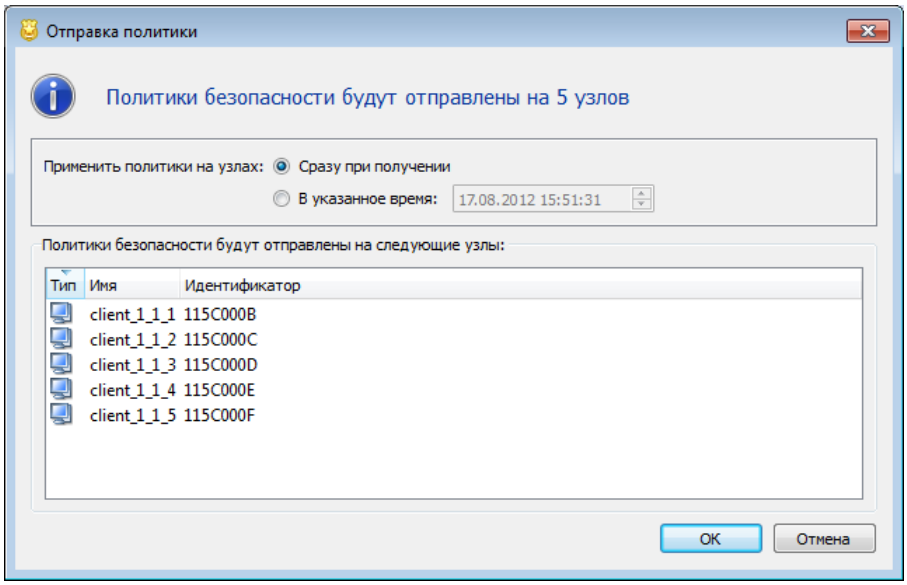

Рисунок 63. Отправка политик безопасности на сетевые узлы

5 Нажмите кнопку **OK**. Политики безопасности будут отправлены на выбранные узлы и применены на узлах сразу при получении или в указанное время.

Примечание. Если политики безопасности содержат новые или измененные фильтры, блокирующие трафик, то эти фильтры вступят в действие только после перезагрузки компьютеров, на которые были отправлены политики безопасности.

Групповая рассылка

Групповая рассылка предназначена для одновременной отправки политик безопасности на все узлы подразделений или на все управляемые сетевые узлы.

Чтобы выполнить групповую рассылку:

1. В окне программы ViPNet Policy Manager на панели навигации выберите раздел **Подразделения**.
2. На панели просмотра (см. Рисунок 19 на стр. 58) выберите одно или несколько подразделений или выберите **Сетевые узлы**.
3. Нажмите кнопку **Отправить политики**.
4. В окне **Отправка политики** (см. Рисунок 63 на стр. 111) задайте условие применения политик на узлах. При выборе пункта **В указанное время** задайте дату и время применения.
5. Нажмите кнопку **OK**. Политики безопасности будут отправлены на узлы выбранных подразделений (или на все управляемые узлы) и применены на узлах сразу при получении или в указанное время.

Примечание. Если политики безопасности содержат новые или измененные фильтры, блокирующие трафик, то эти фильтры вступят в действие только после перезагрузки компьютеров, на которые были отправлены политики безопасности.

Журнал отправки и применения политик безопасности

Все события, связанные с отправкой политик безопасности на сетевые узлы и их применением на узлах, записываются в журнал, который отображается в подразделе **Отправка и применение политик** раздела **Журналы**. Раздел **Журналы** будет присутствовать на панели навигации только в случае, если текущий пользователь программы имеет полномочие **Аудит**.

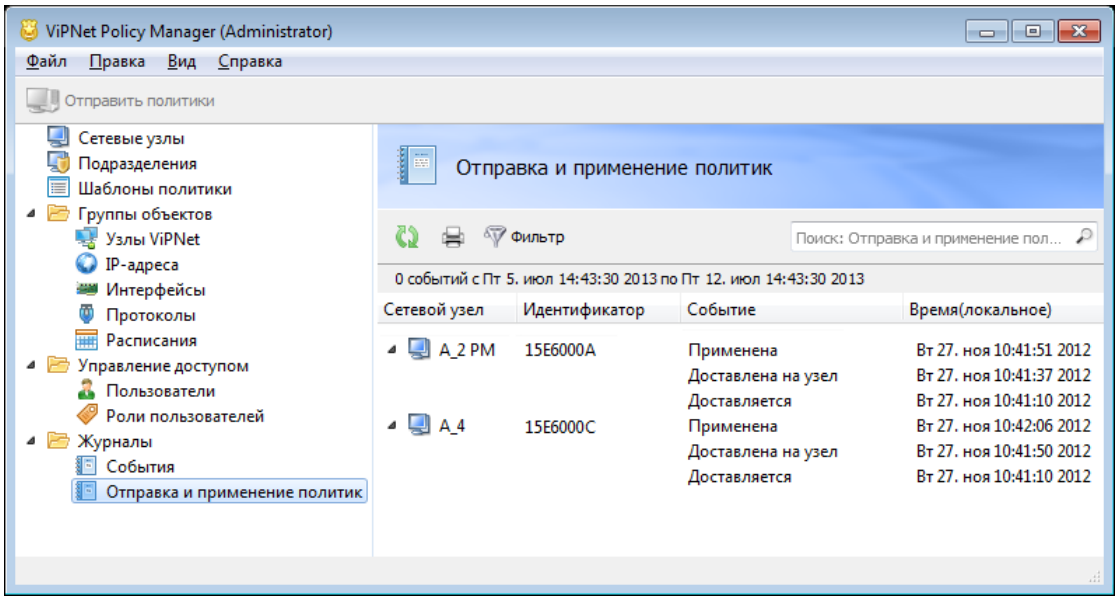

Рисунок 64. Журнал отправки и применения политик безопасности

Для каждого зарегистрированного в журнале события выводится информация, указанная ниже в таблице.

Таблица 9. Информация о событиях в журнале отправки и применения политик

Столбец	Описание
Сетевой узел	Значок с обозначением типа узла: — координатор; — клиент. За значком следует название узла.
Идентификатор	Идентификатор узла в сети ViPNet.
Событие	Описание события.
Время(локальное)	Дата и время фиксации события программой ViPNet Policy Manager.

Во время просмотра журнала события, наступившие после начала просмотра, не отображаются автоматически. Чтобы актуализировать список событий, нажмите кнопку **Обновить** .

Записи в журнале можно отфильтровать по одному или нескольким параметрам. Чтобы задать условия фильтрации:

1 Нажмите кнопку **Фильтр**.

2 В окне **Журнал событий** задайте параметры:

- **Временной диапазон** — выберите значение в списке **Диапазон** или задайте начало и конец временного интервала в соответствующих полях.
- **Событие** — установите флажки напротив нужных событий.
- **Сетевой узел** — выберите значение в списке или нажмите кнопку справа от списка и в окне с перечнем управляемых сетевых узлов выберите нужные узлы.

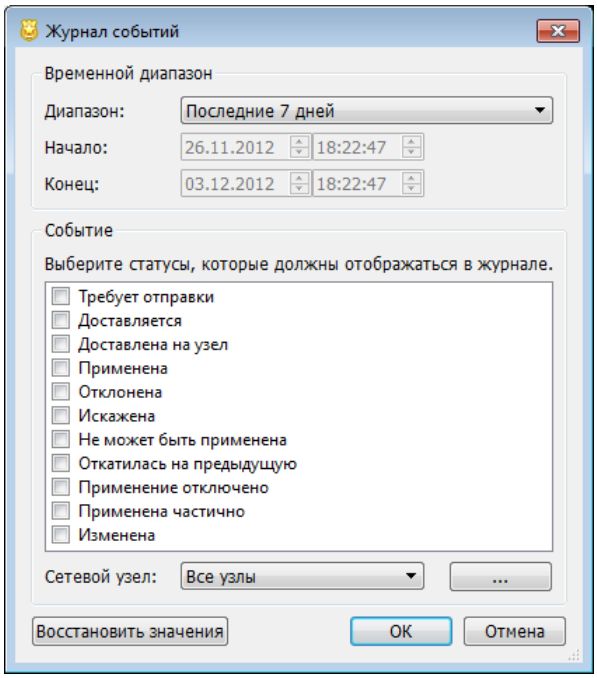

Рисунок 65. Фильтр журнала отправки и применения политик безопасности

3 Чтобы установить значения параметров, используемые по умолчанию, нажмите кнопку **Восстановить значения**.

4 Нажмите кнопку **OK**. Список событий на панели просмотра будет обновлен в соответствии с заданными параметрами.

10

Аудит действий пользователей

Работа в программе с полномочием «Аудит» 116

Просмотр журнала событий 117

Работа в программе с полномочием «Аудит»

В программе ViPNet Policy Manager ведется аудит действий пользователей, который позволяет определить, какие и когда были сделаны изменения и кто за них отвечает. Аудиту подвергаются следующие категории событий:

- Действия пользователей — вход пользователей в программу и выход из программы.
- Учетные записи — действия с учетными записями.
- Сетевые узлы — изменение списка управляемых сетевых узлов и списка шаблонов, назначенных отдельным узлам.
- Подразделения — действия с подразделениями.
- Шаблоны — действия с шаблонами политики безопасности.
- Политики — отправка политики безопасности на сетевые узлы.
- Группы объектов — действия с группами объектов, а также изменение и удаление самих записей о событиях.

Все перечисленные события регистрируются в журнале. Журнал событий доступен для просмотра только тем пользователям, которые имеют полномочие **Аудит**. В частности, такое полномочие есть у предустановленной роли пользователей **Аудитор**. Кроме просмотра журнала событий, пользователи с полномочием **Аудит** могут также просматривать подразделения, шаблоны, группы объектов, результирующие политики безопасности, а также журнал отправки и применения политик.

Просмотр журнала событий

В журнале событий регистрируются действия пользователей в программе ViPNet Policy Manager:

- вход пользователей в программу и выход из программы;
- создание, изменение и удаление учетных записей, подразделений, шаблонов политики безопасности и групп объектов;
- изменение списка шаблонов, назначенных узлам и подразделениям;
- отправка политики безопасности на сетевые узлы;
- нарушение целостности самого журнала.

Журнал отображается в подразделе **События** раздела **Журналы**. Раздел **Журналы** будет присутствовать на панели навигации только в случае, если текущий пользователь программы имеет полномочие **Аудит**.

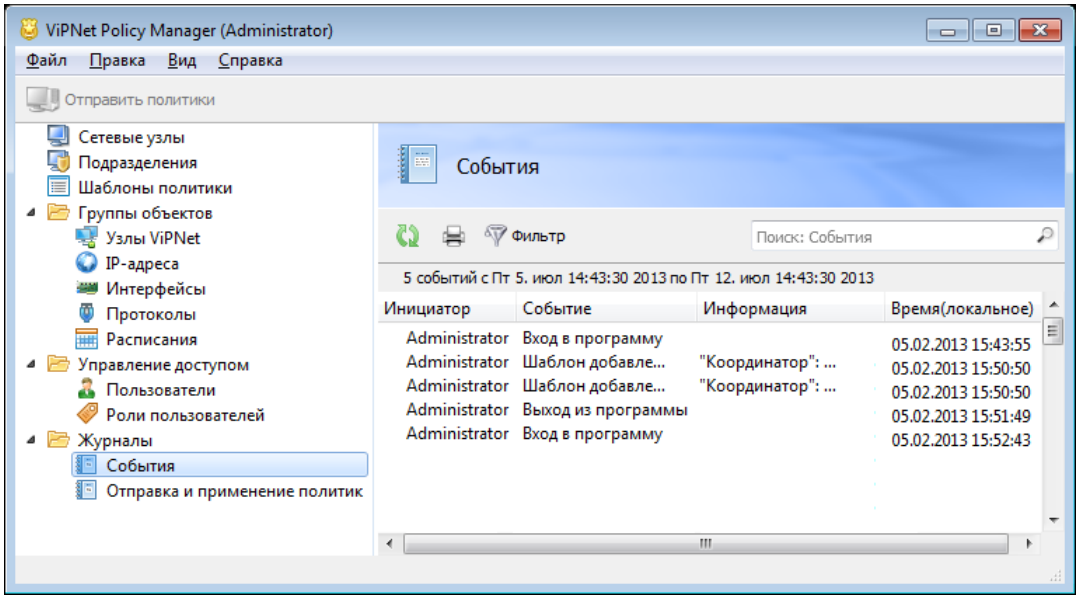

Рисунок 66. Журнал событий

Для каждого зарегистрированного в журнале события выводится информация, указанная ниже в таблице.

Таблица 10. Информация о событиях, зарегистрированных в журнале

Столбец	Описание
Инициатор	Инициатор события (пользователь программы).
Событие	Описание события.
Информация	Детализированная информация о событии.
Время(локальное)	Дата и время фиксации события программой ViPNet Policy Manager.

Во время просмотра журнала события, наступившие после начала просмотра, не отображаются автоматически. Чтобы актуализировать список событий, нажмите кнопку **Обновить** .

Записи в журнале можно отфильтровать по одному или нескольким параметрам. Чтобы задать условия фильтрации:

1 Нажмите кнопку **Фильтр**.

2 В окне **Журнал событий** задайте параметры:

- **Временной диапазон** — выберите значение в списке **Диапазон** или задайте начало и конец временного интервала в соответствующих полях.
- **Событие** — установите флажки напротив нужных событий. События сгруппированы по категориям. Вы можете выбрать сразу все события некоторой категории, установив напротив нее флажок.
- **Инициаторы** — выберите в списке пользователя или оставьте значение **Все инициаторы событий**.

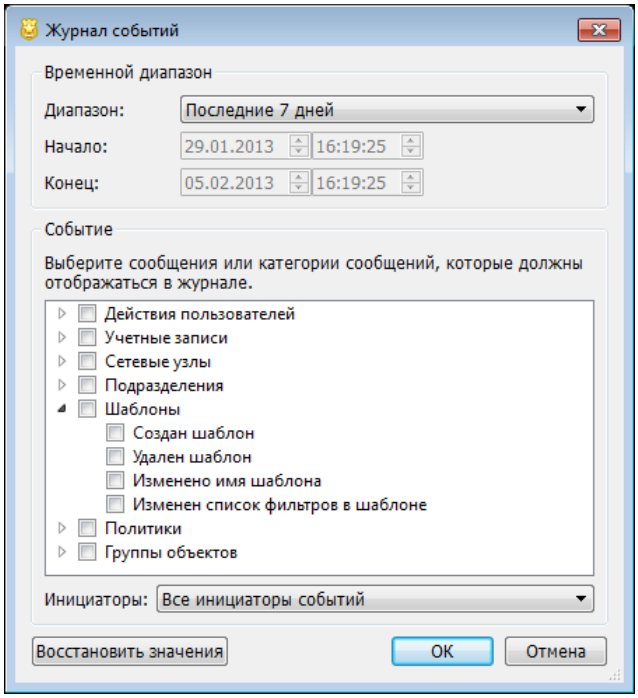

Рисунок 67. Фильтр журнала событий

3 Чтобы установить значения параметров, используемые по умолчанию, нажмите кнопку **Восстановить значения**.

4 Нажмите кнопку **OK**. Список событий на панели просмотра будет обновлен в соответствии с заданными параметрами.

A

Установка Microsoft SQL Server

В данном приложении рассматривается установка программного обеспечения Microsoft SQL Server 2005 Express Edition. Установку других версий Microsoft SQL Server следует выполнять аналогичным образом.

Подробную информацию об установке вы можете найти на веб-сайте, содержащем сведения обо всех разработках компании Microsoft http://msdn.microsoft.com/ru-ru/library/ms143441(v=sql.90).aspx.

Для установки программного обеспечения Microsoft SQL Server 2005 Express Edition выполните следующие действия:

1. Загрузите программу установки Microsoft SQL Server 2005 Express Edition с веб-сайта компании Microsoft http://www.microsoft.com/ru-ru/download/details.aspx?id=30438.
2. Запустите загруженную программу установки.
3. На странице **Лицензионное соглашение** ознакомьтесь с условиями соглашения, затем установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Далее**.
4. На странице **Установка обязательных компонентов** нажмите кнопку **Установить**. Будет выполнена установка компонентов, необходимых для работы Microsoft SQL Server. После окончания установки нажмите кнопку **Далее**.
5. После проверки конфигурации компьютера будет запущен мастер **Установка Microsoft SQL Server 2005**. На первой странице мастера нажмите кнопку **Далее**.
6. На странице **Проверка конфигурации системы** после выполнения проверки нажмите кнопку **Далее**.

7 На странице **Регистрационные сведения** в поле **Имя** введите имя пользователя, по желанию можно ввести название компании. Затем снимите флажок **Скрыть дополнительные параметры конфигурации** и нажмите кнопку **Далее**.

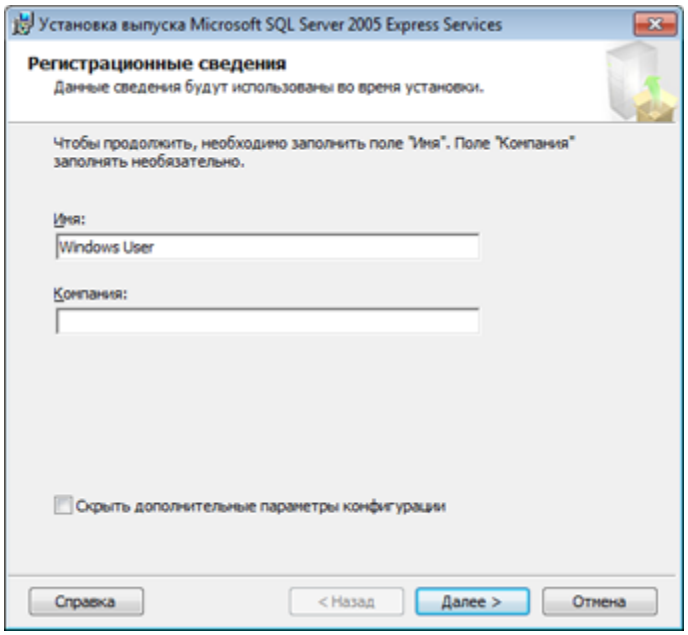

Рисунок 68. Ввод регистрационных данных при установке SQL-сервера

8 На страницах **Выбор компонентов**, **Имя экземпляра** и **Учетная запись службы** сохраните параметры по умолчанию и нажмите кнопку **Далее**.

9 На странице **Режим проверки подлинности** выберите **Смешанный режим (режим проверки подлинности Windows и режим проверки подлинности SQL Server)**. Затем в соответствующих полях задайте пароль для учетной записи администратора сервера `sa`. Пароль должен удовлетворять политике безопасности операционной системы или домена.

Выполнив необходимые действия, нажмите кнопку **Далее**.

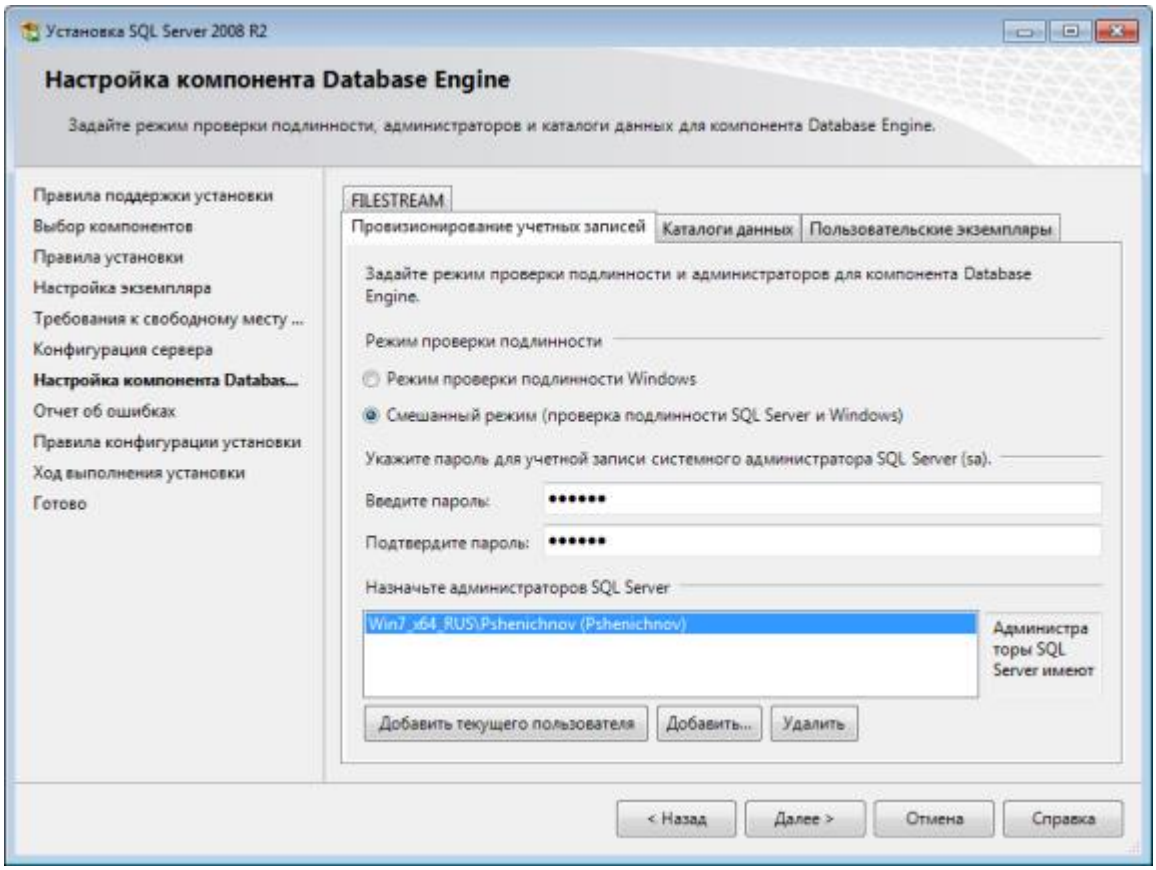

Рисунок 69. Выбор режима проверки подлинности

10 На страницах **Параметры сортировки**, **Пользовательские экземпляры** и **Параметры отчетов об ошибках и использовании** сохраните параметры по умолчанию. Для перехода на следующую страницу нажмите кнопку **Далее**.

11 На странице **Все готово для установки** нажмите кнопку **Установить**.

12 После окончания установки на странице **Выполнение установки** нажмите кнопку **Далее**.

13 На странице **Завершение установки Microsoft SQL Server 2005** нажмите кнопку **Готово**. Установка Microsoft SQL Server 2005 Express Edition завершена.

B

Региональные настройки

Для корректного отображения русской локализации интерфейса программ ViPNet в русифицированных ОС Microsoft Windows английской локализации необходимо установить поддержку кириллицы для программ, не поддерживающих Юникод. Эти настройки рекомендуется производить до установки самой программы.

Данные настройки также понадобится сделать, если установлен русскоязычный MUI (Multilanguage User Interface). Это значит, что ядро операционной системы английское, а русский язык для интерфейса и файлов справки был установлен позже. В этом случае региональные настройки по умолчанию английские и требуют изменения.

Внимание! Для изменения региональных настроек вы должны обладать правами администратора операционной системы.

Региональные настройки в ОС Windows 7, Server 2008 R2

Для установки поддержки кириллицы на ОС Windows 7, Server 2008 R2:

1 Откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

2 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

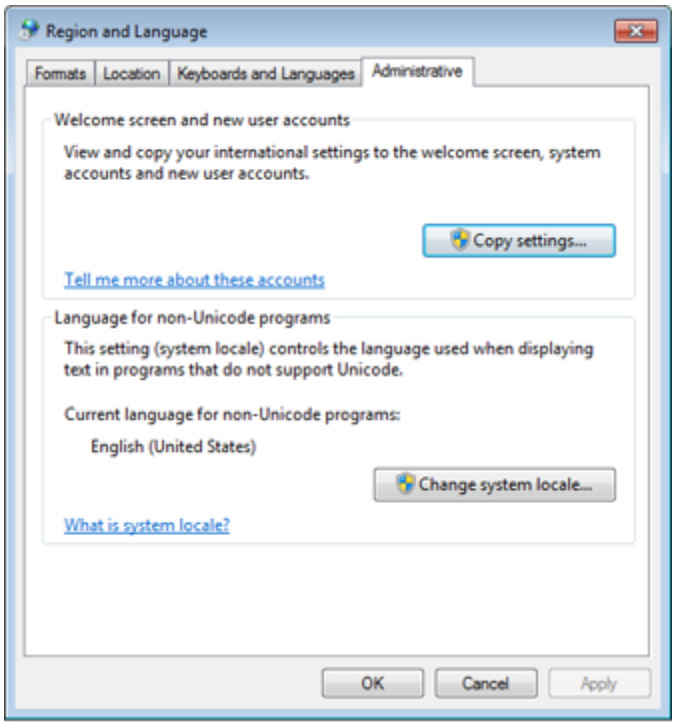

Рисунок 70. Дополнительные языковые параметры

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

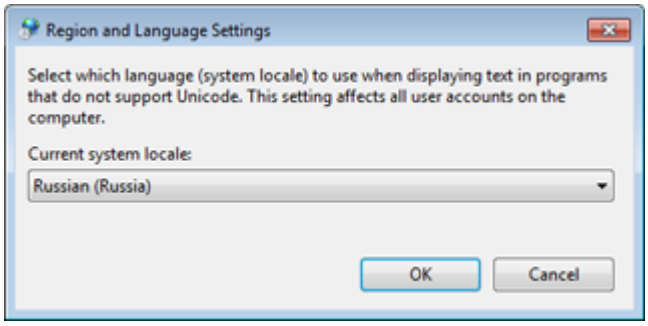

Рисунок 71. Выбор языка системы

5 Нажмите кнопку **OK**. Потребуется перезагрузка.

6 После перезагрузки откройте **Панель управления** (**Control Panel**) > **Часы, язык и регион** (**Clock, Language, and Region**) > **Язык и региональные стандарты** (**Region and Language**).

7 В окне **Язык и региональные стандарты** (**Region and Language**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

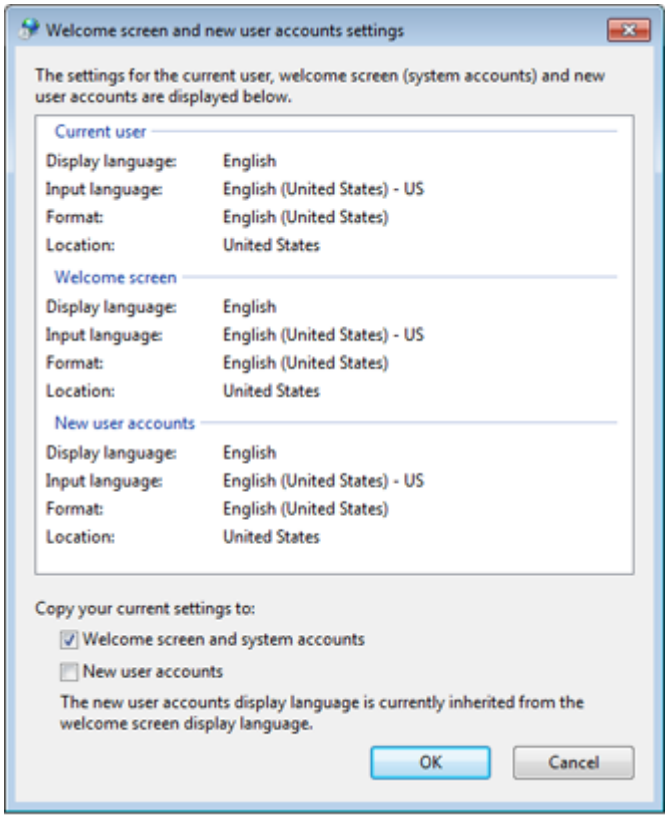

Рисунок 72. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

1 В окне **Язык и региональные стандарты** (**Region and Language**) на вкладке **Форматы** (**Formats**) в списке **Формат** (**Format**) выберите **Русский (Россия)** (**Russian (Russia)**).

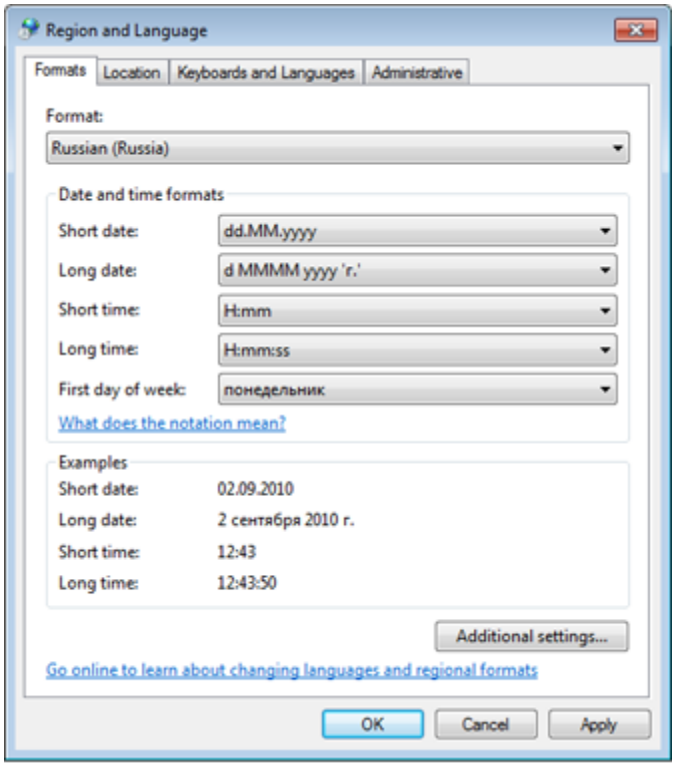

Рисунок 73. Настройка форматов

2 В окне **Язык и региональные стандарты** (**Region and Language**) на вкладке **Расположение** (**Location**) в списке **Текущее расположение** (**Current location**) выберите **Россия**.

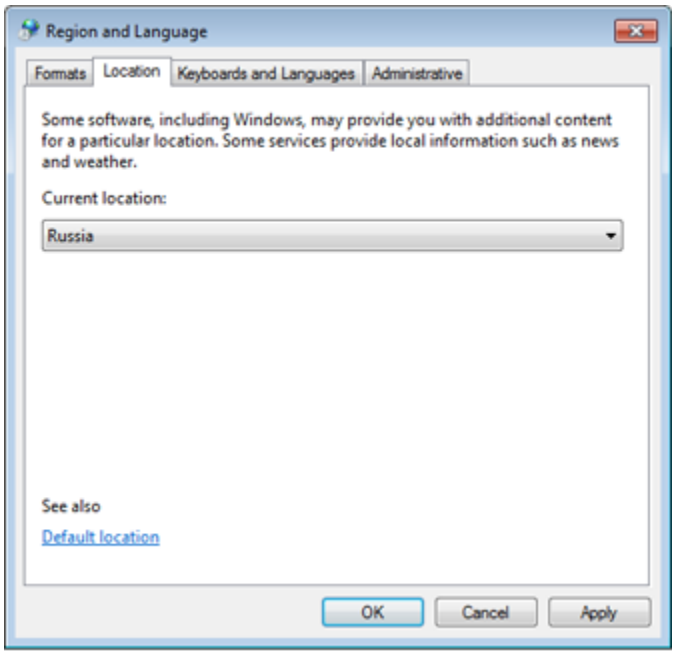

Рисунок 74. Выбор текущего расположения

Региональные настройки в ОС Windows 8, Server 2012, Windows 8.1, Server 2012 R2, Windows 10

Для установки поддержки кириллицы на ОС Windows 8, Server 2012, Windows 8.1, Server 2012 R2, Windows 10 выполните следующие действия:

1 Откройте **Панель управления** (**Control Panel**) > **Региональные стандарты** (**Region**).

2 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

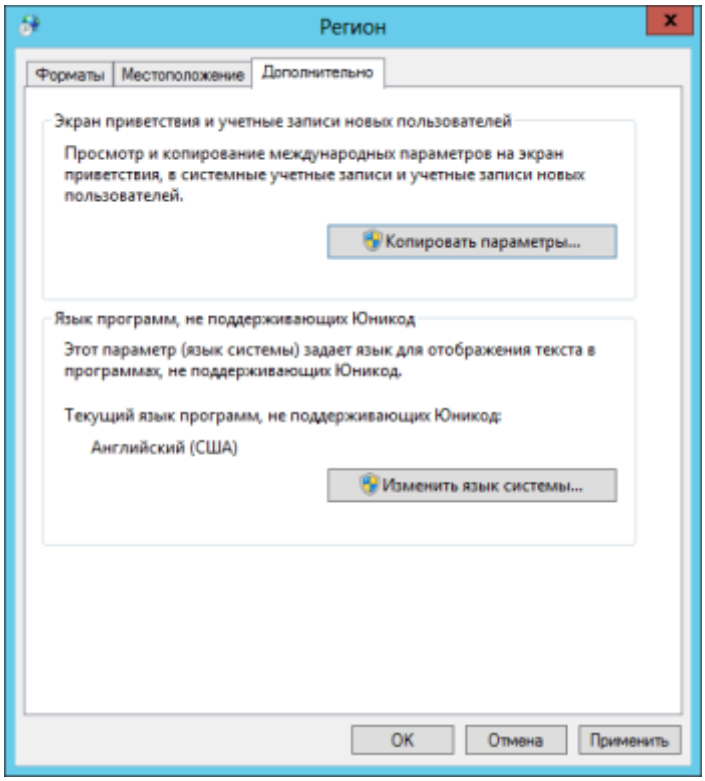

Рисунок 75. Дополнительные языковые параметры

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

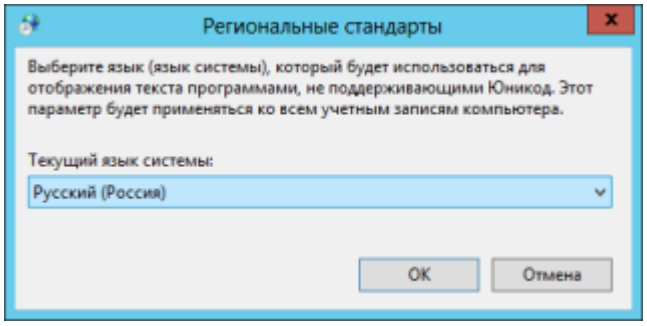

Рисунок 76. Выбор языка системы

5 Нажмите кнопку **OK**. Потребуется перезагрузка.

6 После перезагрузки откройте **Панель управления** (**Control Panel**) > **Региональные стандарты** (**Region**).

7 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

8 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

9 В открывшемся окне установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

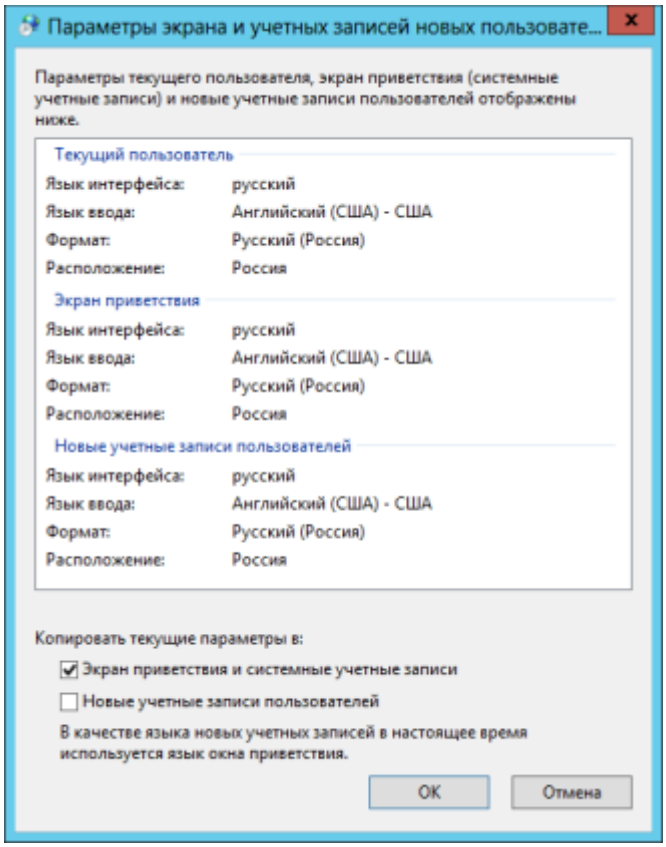

Рисунок 77. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах мы рекомендуем выполнить следующие действия:

1 В окне **Регион** (**Region**) на вкладке **Форматы** (**Formats**) в списке **Формат** (**Format**) выберите **Русский (Россия)** (**Russian (Russia)**).

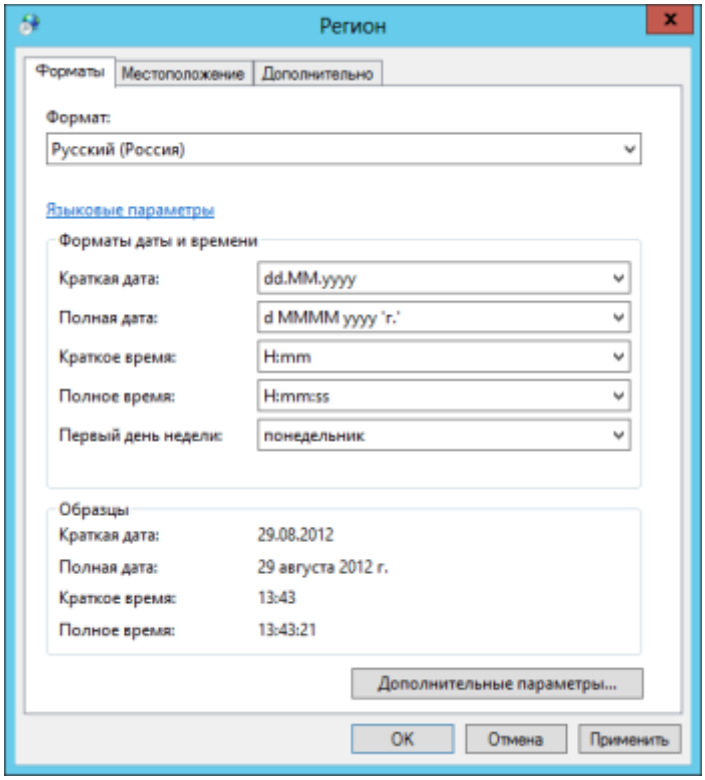

Рисунок 78. Настройка форматов

2 В окне **Регион** (**Region**) на вкладке **Местоположение** (**Location**) в списке **Основное расположение** (**Current location**) выберите **Россия**.

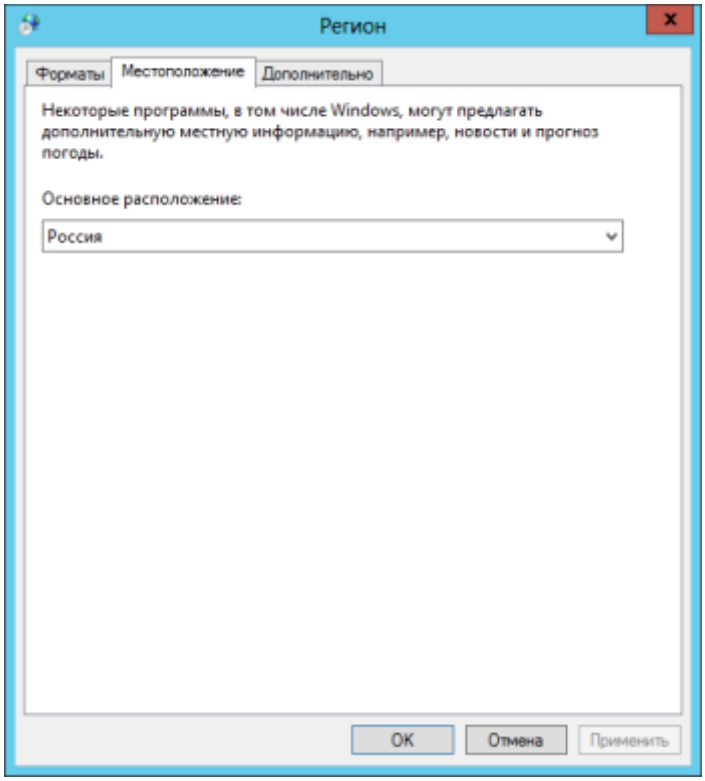

Рисунок 79. Выбор текущего расположения

C

История версий

В данном приложении описаны основные изменения в предыдущих версиях программы ViPNet Policy Manager.

Новые возможности версии 4.3.2

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Policy Manager версии 4.3.2.

- **Поддержка Windows 10**

  Начиная с версии 4.3.2, ПО ViPNet Policy Manager поддерживает операционную систему Windows 10.

- **Изменения в списке поддерживаемых версий SQL-сервера**

  Прекращена поддержка SQL-сервера версий Microsoft SQL Server 2005, Microsoft SQL Server 2008 Microsoft SQL Server 2008 R2.

  Теперь ПО ViPNet Policy Manager поддерживает SQL-сервер версий Microsoft SQL Server 2008 R2 SP1, Microsoft SQL Server 2012 SP1. Microsoft SQL Server 2014 SP1.

- **Совместимость с программным обеспечением ViPNet Administrator 4.4 и ViPNet Network Manager 4.5**

  Начиная с версии 4.3.2, ПО ViPNet Policy Manager поддерживает ПО ViPNet Administrator версии 4.4 или выше и ПО ViPNet Network Manager версии 4.5 или выше.

- **Исправление ошибок**

  Были исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Новые возможности версии 4.3.1

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Policy Manager версии 4.3.1.

- **Упрощена совместная установка с ViPNet Центр управления сетью**

  Теперь при установке программы ViPNet Policy Manager на одном компьютере с серверным приложением ViPNet Центр управления сетью вам не нужно во время установки останавливать службы NccService и NccFilewatcherService.

- **Исправление ошибок**

  Были исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Новые возможности версии 4.2

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Policy Manager версии 4.2.

- **Изменение в главном меню программы**

  Изменено название первого пункта главного меню программы. Теперь этот пункт называется **Файл**.

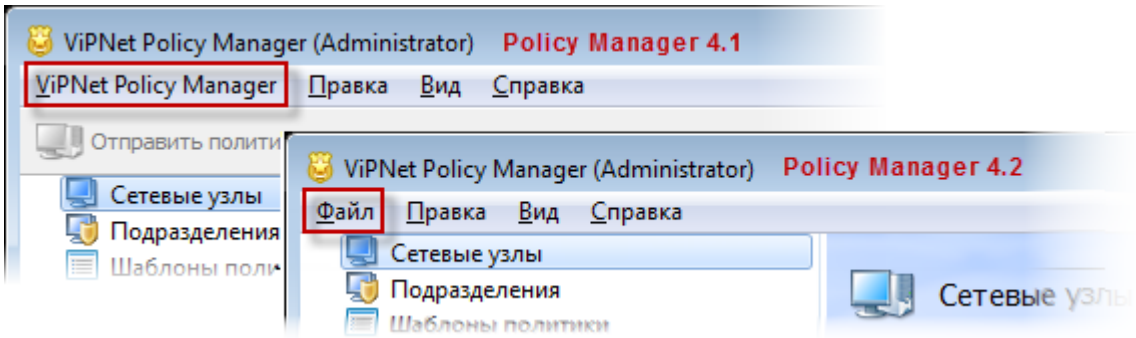

Рисунок 80. Сравнение главного меню Policy Manager 4.1 и Policy Manager 4.2

- **Ограничение на использование программы**

  В версии 4.2 введено ограничение на использование программы ViPNet Policy Manager на сетевых узлах. Теперь программу можно использовать только на сетевом узле, который является Центром управления сетью.

Новые возможности версии 4.1

Автоматическое обновление списка управляемых сетевых узлов

Реализовано автоматическое обновление списка управляемых сетевых узлов. Теперь при поступлении обновления справочников не требуется обновлять список вручную, это происходит автоматически.

Новые возможности версии 4.0

В этом разделе представлен краткий обзор изменений и новых возможностей ViPNet Policy Manager версии 4.0.

- **Изменение графического интерфейса программы**

  Графический интерфейс программы переработан и теперь оформлен так же, как интерфейс других программ ViPNet.

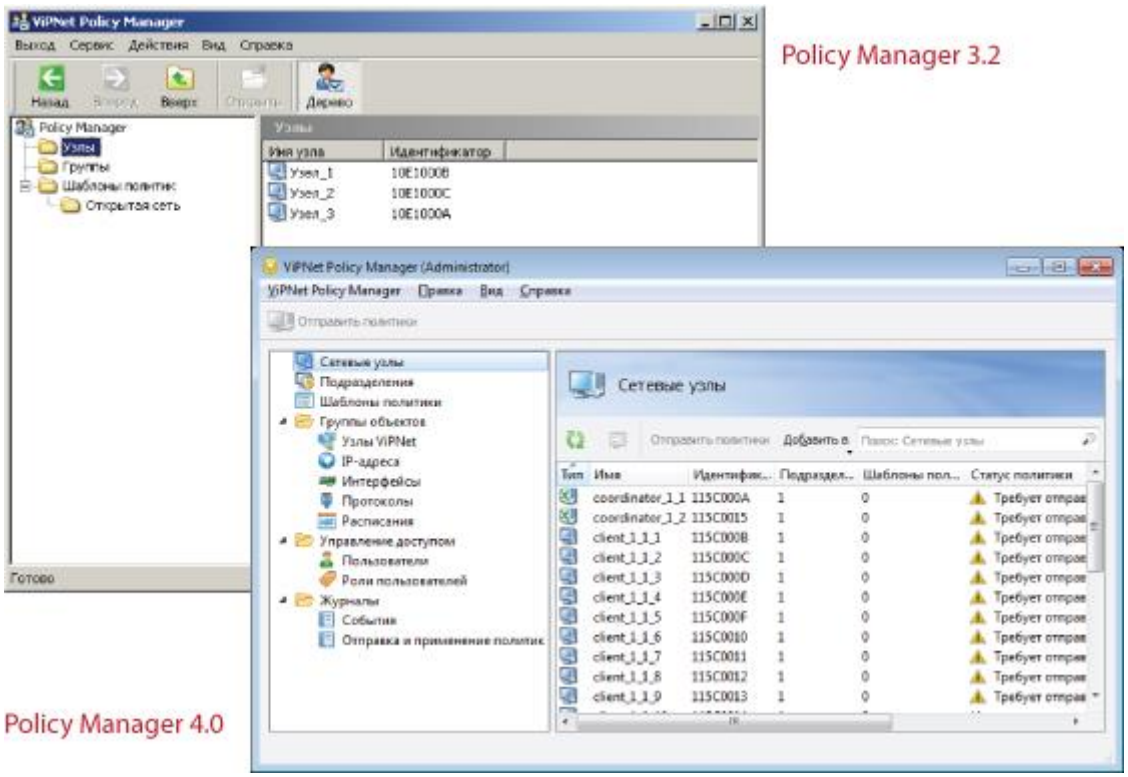

Рисунок 81. Сравнение интерфейса Policy Manager 3.2 и Policy Manager 4.0

  Основные функции программы, в том числе новые функции, находятся на панели навигации и всегда доступны пользователю без необходимости их поиска в меню (см. »Интерфейс программы« на стр. 30).

- **Изменение терминологии**

  Произведена замена некоторых терминов, используемых в ViPNet Policy Manager. Изменения приведены в таблице ниже.

Таблица 11. Изменения в терминологии

Старый термин	Новый термин
Домен управления	Сетевые узлы
Группа (узлов)	Подразделение

- **Изменение набора настроек, задаваемых в шаблонах политики безопасности**

  Режимы безопасности на интерфейсах, которые можно было задать в шаблонах политики безопасности, более не используются. Теперь шаблоны могут содержать только сетевые фильтры и правила трансляции IP-адресов (см. »Общие сведения о шаблонах политики безопасности« на стр. 66).

- **Поддержка работы с группами объектов**

  Реализована работа с группами объектов, использование которых позволяет упростить создание сетевых фильтров и правил трансляции IP-адресов в шаблонах политики безопасности. Группы объектов объединяют несколько значений одного типа и могут быть заданы вместо отдельных значений (см. »Работа с группами объектов« на стр. 68).

- **Полноценная поддержка учетных записей пользователей**

  В версии 3.2 пользователем программы ViPNet Policy Manager мог быть любой пользователь сетевого узла или его администратор. В версии 4.0 реализовано управление учетными записями, и теперь работать с программой могут только пользователи, для которых созданы соответствующие учетные записи (см. »Управление учетными записями« на стр. 45). Аутентификация пользователей ViPNet Policy Manager происходит по имени и паролю.

- **Возможность управлять ролями и полномочиями пользователей**

  Реализовано управление ролями и полномочиями пользователей ViPNet Policy Manager. Теперь вместо двух предустановленных ролей администратора и аудитора с неизменяемыми полномочиями можно использовать ряд встроенных ролей, а также создавать другие роли пользователей с необходимыми полномочиями (см. »Управление ролями пользователей« на стр. 49). Это позволяет гибко распределять обязанности между пользователями программы.

- **Возможность аудита действий пользователей**

  Реализовано ведение журнала событий, в котором регистрируются действия пользователей в программе ViPNet Policy Manager. С помощью журнала событий можно определить, какие и когда были сделаны изменения и кто за них отвечает. Для удобства аудита предусмотрена фильтрация записей в журнале по времени, событиям или инициаторам событий (см. »Просмотр журнала событий« на стр. 117).

- **Возможность фильтрации записей в журнале отправки и применения политик безопасности**

  Реализована фильтрация записей в журнале отправки и применения политик безопасности. Теперь при просмотре журнала можно отфильтровать записи по времени, событиям или сетевым узлам (см. »Журнал отправки и применения политик безопасности« на стр. 113).

- **Обновление документации и поддержка справки**

Существенно переработана документация, поставляемая вместе с программой ViPNet Policy Manager, а также создана встроенная справка, которая позволяет получить быструю помощь во время работы с программой.

D

Глоссарий

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.

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.

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.

Подразделение

Множество узлов из числа всех управляемых сетевых узлов, объединенных для коллективного назначения шаблонов политики безопасности. Одно подразделение может входить в другое, образуя иерархию.

Подсеть

Логически выделенное подмножество узлов сети.

Политика безопасности

Набор параметров, регулирующих безопасность сетевого узла. В технологии ViPNet безопасность сетевых узлов обеспечивается с помощью сетевых фильтров и правил трансляции IP-адресов.

Результирующая политика безопасности

Политика безопасности для отдельного узла, полученная в результате объединения (с учетом приоритета) шаблонов, назначенных узлу и подразделениям, в которые входит данный узел.

Роль пользователей

Набор полномочий, предназначенный для обеспечения определенных действий пользователей в программе ViPNet Policy Manager.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

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).

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.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в 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.

Туннелирующий координатор

Координатор, который осуществляет туннелирование.

Шаблон политики безопасности

Набор настроек, предназначенный для установки на сетевых узлах определенной политики безопасности. В шаблоне задаются необходимые сетевые фильтры и правила трансляции IP-адресов. Шаблон может быть назначен сетевым узлам и подразделениям.

Широковещательный пакет

Пакет, предназначенный всем компьютерам, относящимся к одной подсети, определенной соответствующей маской.

E

Указатель

В

Выборочная рассылка - 61, 109

Г

Групповая рассылка - 61, 109

Д

Добавление IP-адресов и DNS-имен - 74, 88, 90, 92, 99
Добавление в подразделение нескольких сетевых узлов - 62, 64
Добавление в подразделение одного сетевого узла - 64
Добавление идентификатора сетевого интерфейса - 8, 74
Добавление протоколов - 75, 89, 91, 93, 96
Добавление расписаний - 75, 89, 91, 94, 96
Добавление сетевых узлов - 73, 92, 94

Ж

Журнал отправки и применения политик безопасности - 16, 33, 44, 137

З

Запуск программы - 36

И

Интерфейс программы - 30, 136
История версий - 8

К

Как назначить шаблон политики безопасности сетевым узлам или подразделениям - 36, 41
Как отправить политики безопасности на сетевые узлы - 36, 39, 42
Как посмотреть журнал отправки и применения политик безопасности - 36
Как сменить пароль встроенной учетной записи - 36
Как создать подразделение - 36
Как создать учетную запись - 37
Как создать шаблон политики безопасности - 36
Копирование шаблона политики безопасности - 8

Н

Назначение шаблона нескольким подразделениям - 103
Назначение шаблона нескольким сетевым узлам - 103
Назначение шаблона одному подразделению - 62, 103
Назначение шаблона одному сетевому узлу - 103

О

Общие сведения о шаблонах политики безопасности - 41, 109, 137
Отправка и получение политик безопасности - 16

П

Подразделение - 15, 17, 39
Политика безопасности - 8, 15
Правила формирования результирующей политики безопасности - 64
Просмотр журнала событий - 33, 137
Просмотр и изменение правил трансляции IP-адресов, заданных в шаблоне - 69, 84, 101
Просмотр и изменение сетевых фильтров, заданных в шаблоне - 69, 84, 101
Просмотр списка управляемых сетевых узлов - 20, 32, 111

Р

Работа с группами объектов - 33, 137
Разграничение полномочий на основе ролей пользователей - 36, 45, 52
Рассылка политик безопасности на сетевые узлы - 43
Региональные настройки - 24
Результирующая политика безопасности - 15, 17, 58
Роль пользователей - 18, 47, 52

С

Сетевой узел ViPNet - 57
Сеть ViPNet - 57
Системные группы объектов - 71, 74
Системные требования - 16
Смена пароля пользователя - 48
Совместимость с ПО ViPNet - 15, 19
Создание и изменение групп объектов - 72, 88, 89, 90, 91, 92, 93, 94, 96, 99
Создание и изменение правила трансляции IP-адресов - 97, 98
Создание и изменение учетной записи - 47
Создание подразделения - 63
Создание сетевых фильтров - 86
Справочники - 16

Т

Транспортный модуль (MFTP) - 15
Требования к SQL-серверу для развертывания базы данных - 10, 22

У

Удаление ViPNet Policy Manager - 26
Управление подразделениями - 32, 40
Управление ролями пользователей - 33, 137
Управление учетными записями - 33, 137
Управление шаблонами политики безопасности - 32, 41
Установка Microsoft SQL Server - 22
Установка ViPNet Policy Manager - 22

Ш

Шаблон политики безопасности - 15, 17