Апплет мониторинга и управления ViPNet-координатором

Руководство пользователя

ViPNet
Virtual Private Network
infotecs

ФРКЕ.00040-06 90 02, Версия 3.2.1

ОАО "Инфотекс"

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

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

E-mail: hotline@infotecs.ru

WWW: http://www.infotecs.ru

Содержание

Введение

Для кого предназначен документ

Данный документ предназначен для пользователей, отвечающих за настройку и эксплуатацию ViPNet-координатора. В нем содержится описание работы с апплетом мониторинга и управления, предоставляющим удобный интерфейс для наблюдения за работой координатора и его настройки.

Соглашения документа

В данном документе содержатся следующие соглашения:

Указатель	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.

Общие сведения

Виртуальная сеть ViPNet. Общие принципы взаимодействия узлов в виртуальной сети

Пакет программ серии ViPNet в применении к IP-сетям является универсальным программным средством для создания виртуальных защищенных сетей (VPN) любых конфигураций, обеспечивающих прозрачное взаимодействие компьютеров, включенных в VPN, независимо от способа, места и типа выделяемого адреса при их подключении к сети.

Виртуальная сеть ViPNet строится путем установки на компьютеры (сетевые узлы) следующего ПО: ViPNet Client и ViPNet Coordinator. Сетевой узел с установленным ПО ViPNet Client называется клиентом или абонентским пунктом (АП), сетевой узел с установленным ПО ViPNet Coordinator называется координатором (или ViPNet-координатором). ПО ViPNet Client обеспечивает сетевую защиту и включение в VPN отдельных компьютеров. Компьютер с ПО ViPNet Coordinator обычно устанавливается на границах локальных сетей и их сегментов и обеспечивает:

- включение в VPN открытых и защищенных компьютеров, находящихся в этих локальных сетях или их сегментах, независимо от типа адреса, выделяемого им;
- разделение и защиту сетей от сетевых атак и оповещение компьютера с ПО ViPNet Client о состоянии других сетевых узлов, связанных с ним.

Компьютеры сети ViPNet могут располагаться внутри локальных сетей любого типа, поддерживающих IP-протокол. Это может быть сеть Ethernet или PPPoE через XDSL-подключение, PPP через обычный Dial UP или ISDN, сеть сотовой связи GPRS или Wireless-устройства, сети MPLS или VLAN. ПО ViPNet автоматически поддерживает разнообразные протоколы канального уровня.

Компьютеры сети ViPNet могут работать в сети как автономно, то есть не использовать никакие межсетевые экраны, так и через различные межсетевые экраны и другие устройства, выполняющие функции преобразования адресов (NAT).

При невозможности или нежелании установки программных средств на какие-либо компьютеры локальной сети работу по защите трафика таких компьютеров можно поручить ПО ViPNet Coordinator. В этом случае ViPNet-координатор создаст

защищенный туннель для этих компьютеров до аналогичного координатора или непосредственно до конечного компьютера (абонентского пункта).

Основой всех программ для виртуальной сети является специальный драйвер ViPNet, взаимодействующий непосредственно с драйверами сетевых интерфейсов операционной системы (реальных или их эмулирующих). Драйвер ViPNet перехватывает и контролирует весь IP-трафик, поступающий и исходящий из компьютера.

При взаимодействии в сети с другими компьютерами, также оснащенными ПО ViPNet, программа обеспечивает установление между такими компьютерами защищенных VPN-соединений. При этом осуществляется шифрование всего IP-трафика между двумя компьютерами, что делает недоступным этот трафик для любых других компьютеров, в том числе имеющих такое же ПО.

Управление виртуальной сетью и допустимыми связями, созданием и распределением ключевой информации между узлами осуществляется с помощью программ Центр управления сетью (ЦУС) и Удостоверяющий и Ключевой центр (УКЦ).

Обмен управляющей информацией (справочники, ключи, программное обеспечение и др.) с ЦУС и объектов сети между собой, а также обмен почтовой информацией производится через ViPNet-координатор (используется функциональная составляющая координатора – сервер-маршрутизатор) с помощью специального транспортного протокола над TCP/IP. В координаторе функцию сервера-маршрутизатора реализует транспортный модуль MFTP.

Оповещение абонентского пункта о состоянии других узлов сети по умолчанию осуществляет координатор (точнее, его функциональная составляющая – сервер IP-адресов), на котором этот абонентский пункт был зарегистрирован в ЦУС. Этот координатор всегда владеет полным объемом информации обо всех узлах сети, связанных с данным абонентским пунктом. Однако при необходимости пользователь (или по команде из ЦУС) может выбрать в качестве сервера IP-адресов любой другой координатор, доступный ему. В этом случае абонентский пункт также сможет получить информацию о большинстве связанных с ним узлов и рассказать им о себе.

Назначение апплета мониторинга и управления

Апплет мониторинга и управления (далее - апплет) предназначен для наблюдения за работой ViPNet-координатора (функционирующего под управлением ОС Linux) и его настройки посредством web-интерфейса. Апплет позволяет следить за работой и управлять следующими разновидностями координаторов:

- ViPNet-координатор с установленным ПО ViPNet Coordinator Linux;
- ПАК NME-RVPN ViPNet;
- ПАК ViPNet MiniGate;
- ПАК ViPNet Coordinator HW.

Апплет предоставляет следующие возможности по мониторингу ViPNet-координатора:

- мониторинг состояния узлов сети ViPNet, имеющих связь (заданную в ЦУС) с данным ViPNet-координатором:
  - просмотр настроек сетевых узлов;
  - проверка соединения с сетевыми узлами;
- просмотр статистики IP-пакетов по сетевым интерфейсам ViPNet-координатора;
- просмотр информации о блокированных IP-пакетах;
- просмотр журнала регистрации IP-пакетов;
- просмотр очереди конвертов MFTP;
- просмотр журнала конвертов MFTP;
- мониторинг состояния системы защиты от сбоев, включая просмотр журнала переключений состояний.

С помощью апплета можно управлять следующими настройками ViPNet-координатора:

- настройка правил фильтрации транзитных IP-пакетов;
- настройка правил фильтрации локальных IP-пакетов;

- настройка правил фильтрации широковещательных IP-пакетов;
- настройка правил трансляции адресов;
- настройка параметров сетевых интерфейсов ViPNet-координатора;
- настройка туннелируемых адресов;
- настройка автоматического обновления информации, предоставляемой для просмотра.

Для мониторинга и управления ViPNet-координатором требуется авторизация пользователя по паролю. При этом различают 2 режима работы - режим пользователя и режим администратора, каждый со своим паролем. Режим работы определяет полномочия по управлению ViPNet-координатором: в режиме пользователя разрешен только просмотр информации о работе ViPNet-координатора (мониторинг), в режиме администратора доступны и мониторинг, и управление настройками ViPNet-координатора. Подробнее о режимах работы апплета см. раздел Режимы работы апплетав главе Работа с апплетом мониторинга и управления.

Системные требования

Мониторинг и управление ViPNet-координатором посредством web-интерфейса можно осуществлять как локально на сервере, на котором установлено ПО ViPNet Coordinator Linux, так и удаленно с других компьютеров.

Для локального мониторинга и управления на сервере должно быть установлено следующее ПО:

- Интернет-браузер – FireFox (версии 2.0 и выше).
- Исполнительная среда Java – JRE (версии 1.5.0 и выше).

Для удаленного мониторинга и управления на компьютере, откуда будут осуществляться мониторинг и управление, должно быть установлено следующее ПО:

- ViPNet Client [Монитор].

  ViPNet-клиент должен быть зарегистрирован в прикладной задаче "Клиент SGA", иметь связь с ViPNet-координатором, мониторинг и управление которым требуется осуществлять, а также иметь доступ к удаленному мониторингу и управлению. Регистрация узлов в прикладных задачах и задание связей между узлами осуществляются в Центре управления сетью (ЦУС). Наличие доступа ViPNet-клиента к удаленному мониторингу и управлению зависит от конфигурации ViPNet-координатора. Подробнее о настройке доступа см. документ "Апплет мониторинга и управления ViPNet-координатором. Руководство администратора".
- Интернет-браузер – Microsoft Internet Explorer (версии 6.0 и выше) или FireFox (версии 2.0 и выше).
- Исполнительная среда Java – JRE (версии 1.5.0 и выше).

Запуск апплета и завершение работы с ним

Запустить апплет можно одним из следующих способов:

1. В программе ViPNet Client [Монитор] в окне **Защищенная сеть** выберите нужный координатор и нажмите команду **Web-ссылка** в главном меню **Действия** или в контекстном меню (Рисунок 1), либо нажмите кнопку  (**Web-ссылка**) на панели инструментов.

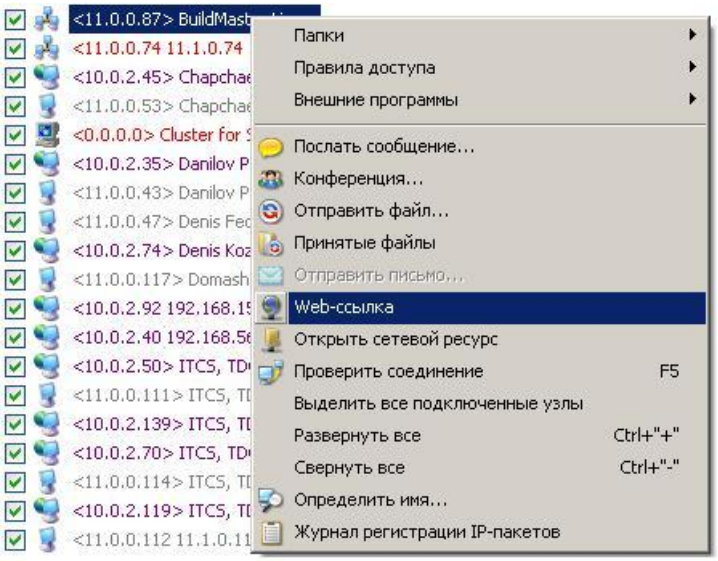

Рисунок 1. Команда для запуска апплета мониторинга и управления

2. Введите в адресной строке Интернет-браузера IP-адрес или DNS-имя ViPNet-координатора.

Откроется окно Интернет-браузера для запуска апплета (Рисунок 2).

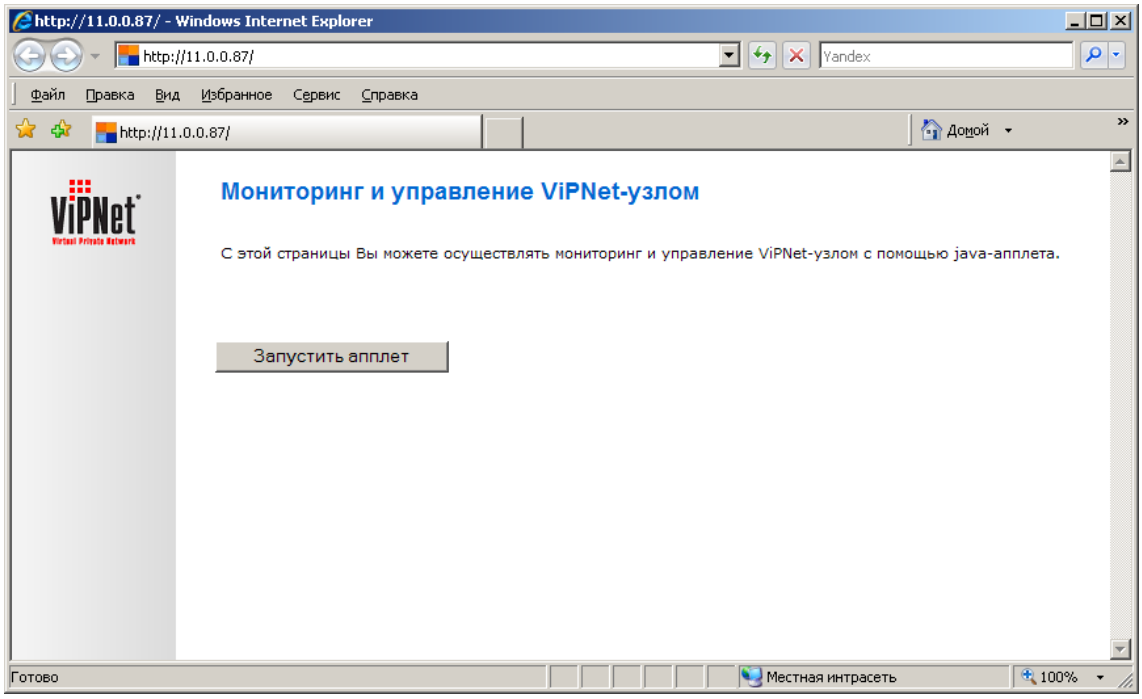

Рисунок 2. Запуск апплета мониторинга и управления

Нажмите кнопку **Запустить апплет**.

Примечание. Если ViPNet-клиент, установленный на данном компьютере, не зарегистрирован в прикладной задаче "Клиент SGA" (см. раздел Системные требования), то появится сообщение об отсутствии разрешения на мониторинг и управление ViPNet-координатором и апплет не запустится.

Появится окно для ввода пароля пользователя (Рисунок 3).

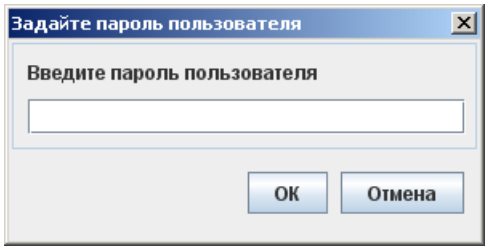

Рисунок 3 .Запрос пароля пользователя

Введите пароль и нажмите кнопку **ОК**. Если введен верный пароль, апплет последовательно устанавливает соединение со службами (демонами) iplir, mftp и

failover и выводит об этом соответствующие сообщения (Рисунок 4). Можно прервать дальнейшее соединение со службами, нажав кнопку **Отмена** в любом из сообщений.

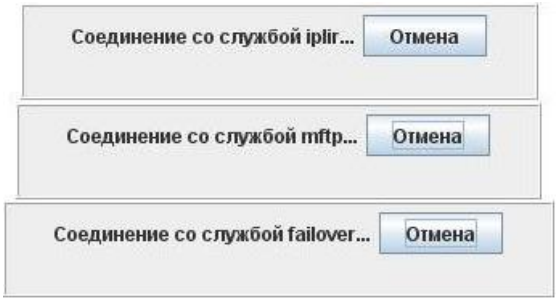

Рисунок 4. Соединение со службами

Если при старте апплета будет установлено соединение хотя бы с одной из служб, то откроется окно апплета (см. главу Работа с апплетом мониторинга и управления).

Если апплету не удастся установить соединение ни с одной из служб, то появится сообщение об отсутствии соединения (Рисунок 5). Для повторного соединения со службами нажмите в этом сообщении кнопку **Присоединиться к узлу**.

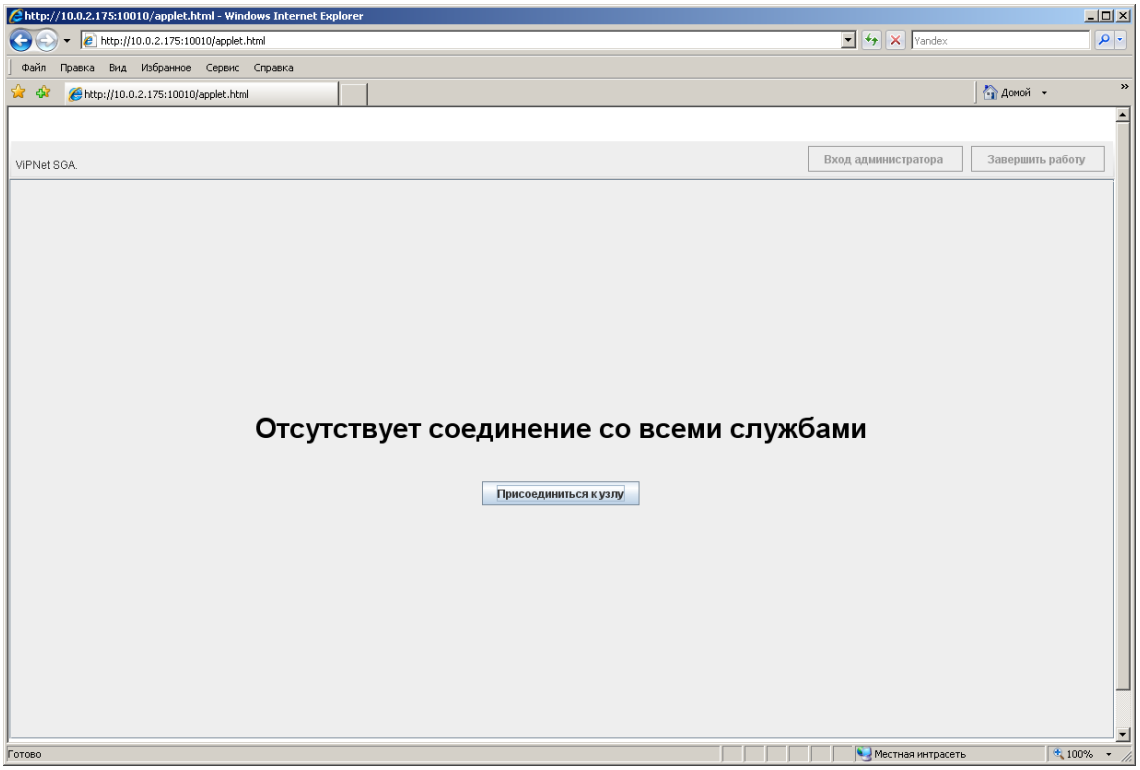

Рисунок 5. Отсутствие соединения со службами

Для завершения работы с апплетом можно закрыть Интернет-браузер или нажать кнопку **Завершить работу**, расположенную на панели инструментов. В последнем случае появится запрос на подтверждение завершения работы (Рисунок 6). Для завершения работы нажмите кнопку **Да**, для продолжения работы – кнопку **Нет**.

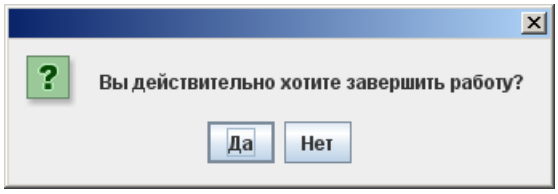

Рисунок 6. Запрос на подтверждение завершения работы

Работа с апплетом мониторинга и управления

Основные вкладки апплета

После старта апплета и установки соединения хотя бы с одной из служб откроется окно апплета (Рисунок 7). Окно апплета разделено на две панели. На левой панели в виде дерева отображается название координатора и структура вкладок. На правой панели отображается содержимое вкладки, выбранной в дереве. Если на правой панели отображается таблица, то информацию в таблице можно отсортировать по любому столбцу, щелкнув мышью по его заголовку.

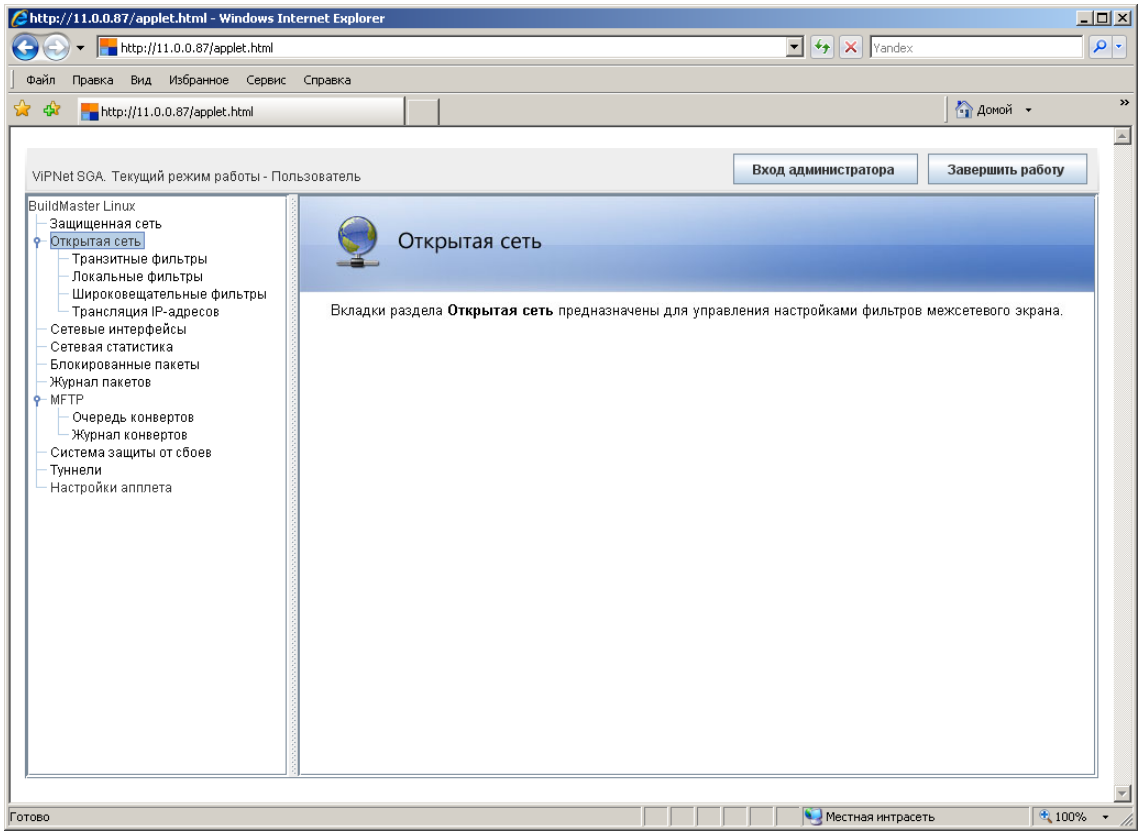

Рисунок 7. Окно апплета мониторинга и управления

Апплет имеет следующие основные вкладки:

- **Защищенная сеть** – вкладка для просмотра списка узлов (пользователей) защищенной сети ViPNet, с которыми связан координатор, и проверки соединения с этими узлами (см. раздел Просмотр списка узлов защищенной сети ViPNet).

- **Открытая сеть** – раздел, объединяющий вкладки для просмотра и настройки фильтров открытой сети и правил трансляции IP-адресов:
  - **Транзитные фильтры** – вкладка для настройки правил фильтрации транзитных IP-пакетов (см. раздел Настройка правил фильтрации транзитных IP-пакетов).
  - **Локальные фильтры** – вкладка для настройки правил фильтрации локальных IP-пакетов (см. раздел Настройка правил фильтрации локальных IP-пакетов).
  - **Широковещательные фильтры** – вкладка для настройки правил фильтрации широковещательных IP-пакетов (см. раздел Настройка правил фильтрации широковещательных IP-пакетов).
  - **Трансляция IP-адресов** – вкладка для настройки правил трансляции IP-адресов (см. раздел Настройка правил трансляции адресов).
- **Сетевые интерфейсы** – вкладка для настройки сетевых интерфейсов (см. раздел Настройка параметров сетевых интерфейсов).
- **Сетевая статистика** – вкладка для просмотра статистики IP-пакетов по сетевым интерфейсам (см. раздел Просмотр статистики IP-пакетов по сетевым интерфейсам).
- **Блокированные пакеты** – вкладка для просмотра списка IP-пакетов, заблокированных на координаторе (см. раздел Просмотр информации о блокированных IP-пакетах).
- **Журнал пакетов** – вкладка для просмотра и поиска информации в журнале регистрации IP-пакетов (см. раздел Просмотр журнала регистрации IP-пакетов).
- **MFTP** – раздел, объединяющий вкладки для запроса информации о работе транспортного модуля MFTP:
  - **Очередь конвертов** – вкладка для запроса информации о текущей очереди конвертов MFTP, ожидающих отправки (см. раздел Просмотр очереди конвертов MFTP).
  - **Журнал конвертов** – вкладка для запроса информации в журнале регистрации обработанных конвертов MFTP (см. раздел Просмотр журнала конвертов MFTP).
- **Система защиты от сбоев** – вкладка для просмотра состояния системы защиты от сбоев (см. раздел Просмотр состояния системы защиты от сбоев).
- **Туннели** – вкладка для просмотра статистики по количеству туннелируемых адресов и настройки диапазонов туннелируемых адресов (см. раздел Настройка туннелируемых адресов).
- **Настройки апплета** – вкладка для настройки системы автоматического обновления информации на вкладках **Защищенная сеть**, **Сетевые интерфейсы**, **Сетевая статистика** и **Система защиты от сбоев** (см. раздел Настройки системы автообновления).

За предоставление информации, отображаемой на каждой из вкладок апплета, отвечает определенная служба, а именно:

- Служба iplir – все вкладки раздела **Открытая сеть**, а также вкладки **Защищенная сеть**, **Сетевые интерфейсы**, **Сетевая статистика**, **Блокированные пакеты**, **Журнал пакетов**, **Туннели**.
- Служба mftp – все вкладки раздела **MFTP**.
- Служба failover – вкладка **Система защиты от сбоев**.

Если соединение с какой-либо из служб не было установлено (или было потеряно), то информация на соответствующих вкладках апплета будет недоступна (вкладки будут неактивны). При выборе в дереве неактивной вкладки появится сообщение о недоступности службы и кнопка **Установить соединение** (Рисунок 8).

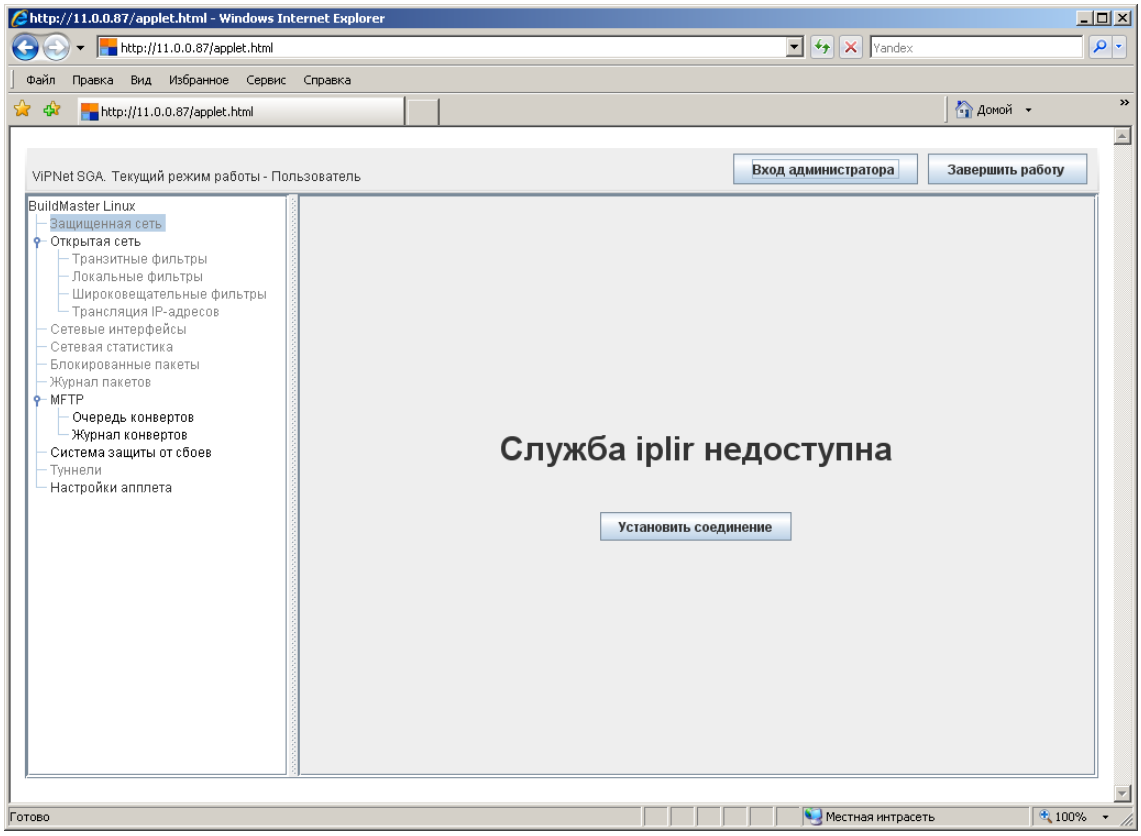

Рисунок 8. Сообщение о недоступности службы

В окне апплета можно получить сведения о версии апплета и версии ViPNet-координатора. Для этого надо выбрать на левой панели название координатора (Рисунок 9).

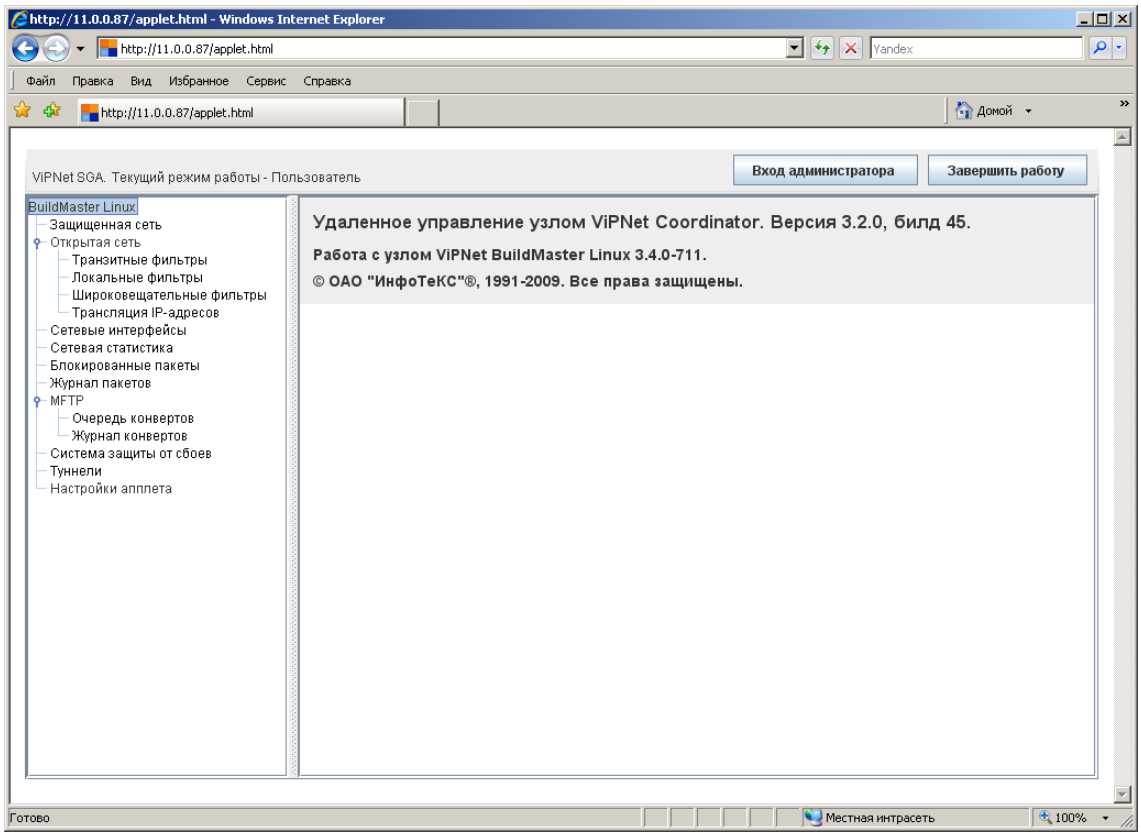

Рисунок 9. Сведения о версиях установленного ПО

Режимы работы апплета

Для работы с апплетом предусмотрены 2 режима – режим пользователя и режим администратора. От режима работы зависит уровень полномочий по управлению координатором: в режиме пользователя доступен только мониторинг координатора (просмотр информации), в режиме администратора дополнительно доступны все действия по управлению координатором.

При запуске апплета по умолчанию устанавливается режим пользователя и запрашивается пароль пользователя ViPNet-узла. Если введен неверный пароль, появится сообщение об ошибке авторизации (Рисунок 10).

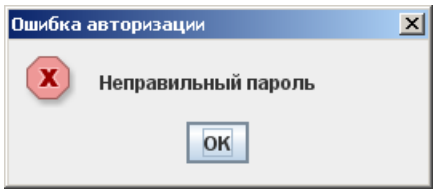

Рисунок 10. Ошибка авторизации

Если введен верный пароль, происходит старт апплета. Слева над окном апплета отображается название текущего режима работы. Справа над окном апплета расположена панель инструментов, содержащая кнопки **Вход администратора** и **Завершить работу** (Рисунок 11).

Рисунок 11. Панель инструментов

Название кнопки **Вход администратора** меняется в зависимости от текущего режима работы:

- В режиме пользователя кнопка называется **Вход администратора** и используется для перехода в режим администратора. При переходе в режим администратора появится окно для ввода пароля администратора ViPNet-сети (Рисунок 12).

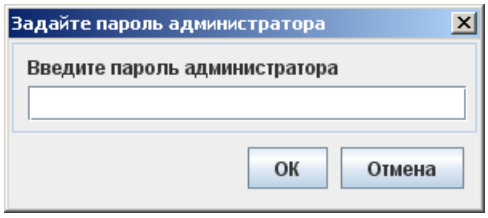

Рисунок 12. Запрос пароля администратора

Если введен неверный пароль, появится сообщение об ошибке и апплет останется в режиме пользователя.

Примечание. Пароль администратора запрашивается каждый раз при переходе из режима пользователя в режим администратора.

- В режиме администратора кнопка называется **Выход администратора** и используется для возврата в режим пользователя.

Примечание. При выходе из режима администратора в режим пользователя пароль пользователя не запрашивается.

Если при возврате в режим пользователя апплету не удастся установить соединение ни с одной из служб, то появится сообщение об отсутствии соединения (см. Рисунок 5).

Мониторинг и управление координатором с помощью апплета может осуществляться одновременно с нескольких компьютеров. При этом доступ к координатору в режиме пользователя разрешен любому количеству пользователей, в режиме администратора – только одному администратору. Если на одном из компьютеров установлен режим администратора, то при попытке перейти в этот режим на любом другом компьютере появится сообщение о том, что режим администратора уже установлен (Рисунок 13).

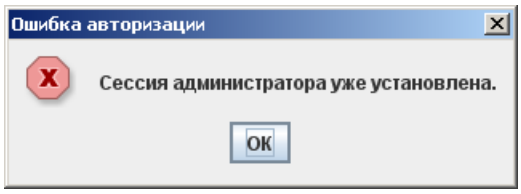

Рисунок 13. Сообщение об установленной сессии администратора

Просмотр списка узлов защищенной сети ViPNet

Просмотр списка узлов защищенной сети ViPNet, с которыми связан координатор, доступен на вкладке **Защищенная сеть** (Рисунок 14). Соединение с этими узлами осуществляется только в защищенном режиме.

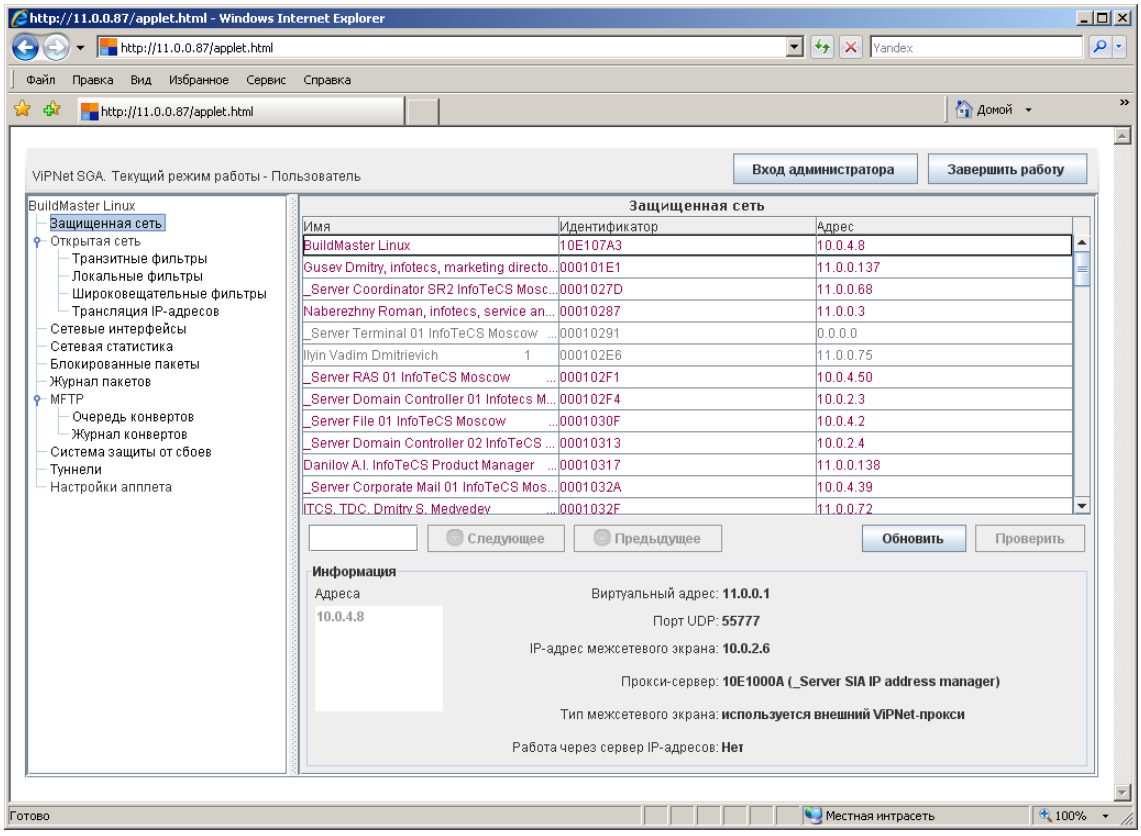

Рисунок 14. Защищенная сеть

В верхней части вкладки расположен список защищенных узлов. Для каждого узла отображаются его имя, идентификатор и текущий IP-адрес доступа. Сетевые узлы выделяются в списке разными цветами:

- **фиолетовый** – сетевой узел доступен;

- **серый** – сетевой узел недоступен.

Цвета, используемые для отображения доступных и недоступных сетевых узлов, задаются в файле ресурсов апплета и при необходимости могут быть изменены.

В нижней части вкладки отображается информация об узле, выбранном в списке (см. Просмотр настроек сетевых узлов).

На вкладке **Защищенная сеть** доступны следующие элементы управления:

- Поле ввода для поиска нужной записи по заданной подстроке. Поиск производится по всем столбцам.
- Кнопки перехода к следующей (кнопка **Следующее**) либо предыдущей (кнопка **Предыдущее**) записи, содержащей подстроку, указанную в поле поиска.
- Кнопка **Обновить** для получения актуальной информации о защищенных узлах.
- Кнопка **Проверить** для проверки соединения с выбранным узлом (см. Проверка соединения с сетевыми узлами).

Просмотр настроек сетевых узлов

Апплет предоставляет возможность просмотреть сетевые настройки защищенных узлов. Для просмотра настроек выберите узел в списке защищенных узлов, при этом в нижней части вкладки **Защищенная сеть** появится информация о сетевых настройках этого узла.

Для каждого узла выводится следующая информация:

Название столбца	Описание
Адреса	IP-адреса всех сетевых интерфейсов, доступных на узле.
Виртуальный адрес	IP-адрес, назначенный узлу на ViPNet-координаторе.
Порт UDP	Порт доступа к узлу через межсетевой экран.
IP-адрес межсетевого экрана	IP-адрес доступа к узлу через межсетевой экран.
Прокси-сервер	ViPNet-координатор, выступающий в качестве межсетевого экрана для выбранного узла.
Тип межсетевого экрана	Тип межсетевого экрана, используемого выбранным

Название столбца	Описание
	узлом.
Работа через сервер IP-адресов	Признак работы узла через сервер IP-адресов: **Да** – на узле задана настройка работы через межсетевой экран с динамической трансляцией адресов и включена одноименная опция; **Нет** – в остальных случаях.

Проверка соединения с сетевыми узлами

Апплет предоставляет возможность узнать текущий статус сетевых узлов – доступны они или нет. Чтобы узнать статус сетевого узла, надо проверить соединение с этим узлом. Для этого выберите узел в списке защищенных узлов и нажмите кнопку **Проверить**. Начнется процесс проверки соединения (Рисунок 15).

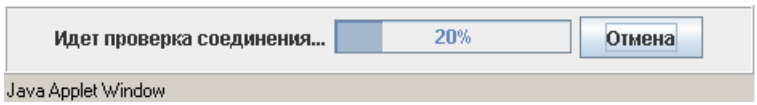

Рисунок 15. Проверка соединения с узлом

Проверка соединения происходит между координатором и выбранным узлом. Можно прервать проверку, для этого нажмите кнопку **Отмена**. По окончании проверки выводится результат – доступен узел или нет (Рисунок 16).

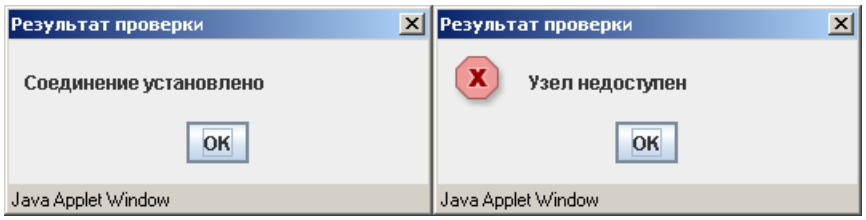

Рисунок 16. Результат проверки соединения с узлом

Настройка правил фильтрации транзитных IP-пакетов

Правила фильтрации транзитных IP-пакетов задают фильтры IP-пакетов, которые только проходят через ViPNet-координатор на пути от отправителя к получателю. Эти правила содержатся в секции **[forward]** файла конфигурации координатора **firewall.conf**. Подробное описание файла **firewall.conf** и синтаксиса правил см. в документе "ViPNet Coordinator Linux. Руководство администратора".

С помощью апплета можно посмотреть правила фильтрации транзитных IP-пакетов, а также настроить правила: определить порядок применения правил, создать новые правила, изменить и удалить существующие правила. Порядок применения правил соответствует их порядку следования в файле **firewall.conf**. Первоначально правила отображаются в интерфейсе апплета в том порядке, в котором они записаны в файле **firewall.conf**. При изменении порядка правил с помощью апплета и сохранении этих изменений правила записываются в файл **firewall.conf** в порядке, заданном в апплете.

Настройка правил фильтрации транзитных IP-пакетов выполняется на вкладке **Транзитные фильтры**. В режиме пользователя доступен только просмотр правил (Рисунок 17).

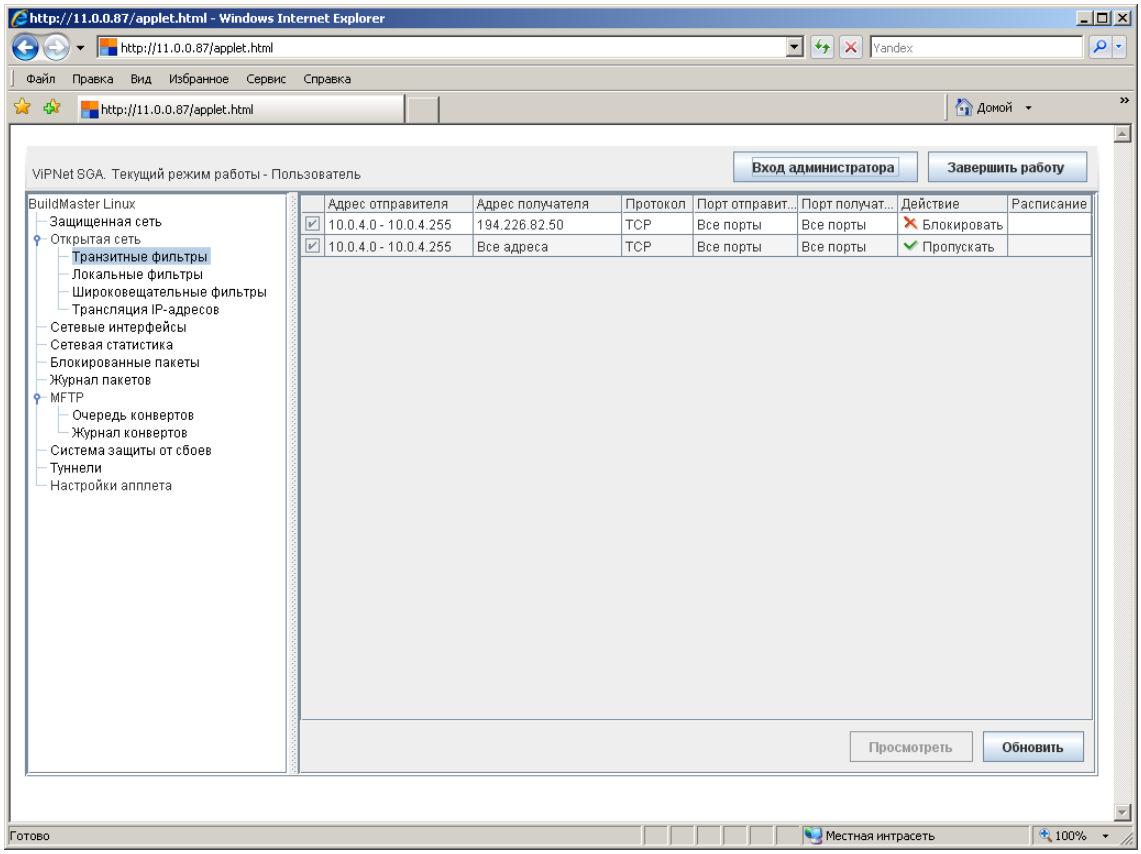

Рисунок 17. Фильтры транзитных IP-пакетов (режим пользователя)

В режиме администратора, помимо просмотра, доступны все действия по настройке правил фильтрации транзитных IP-пакетов (Рисунок 18).

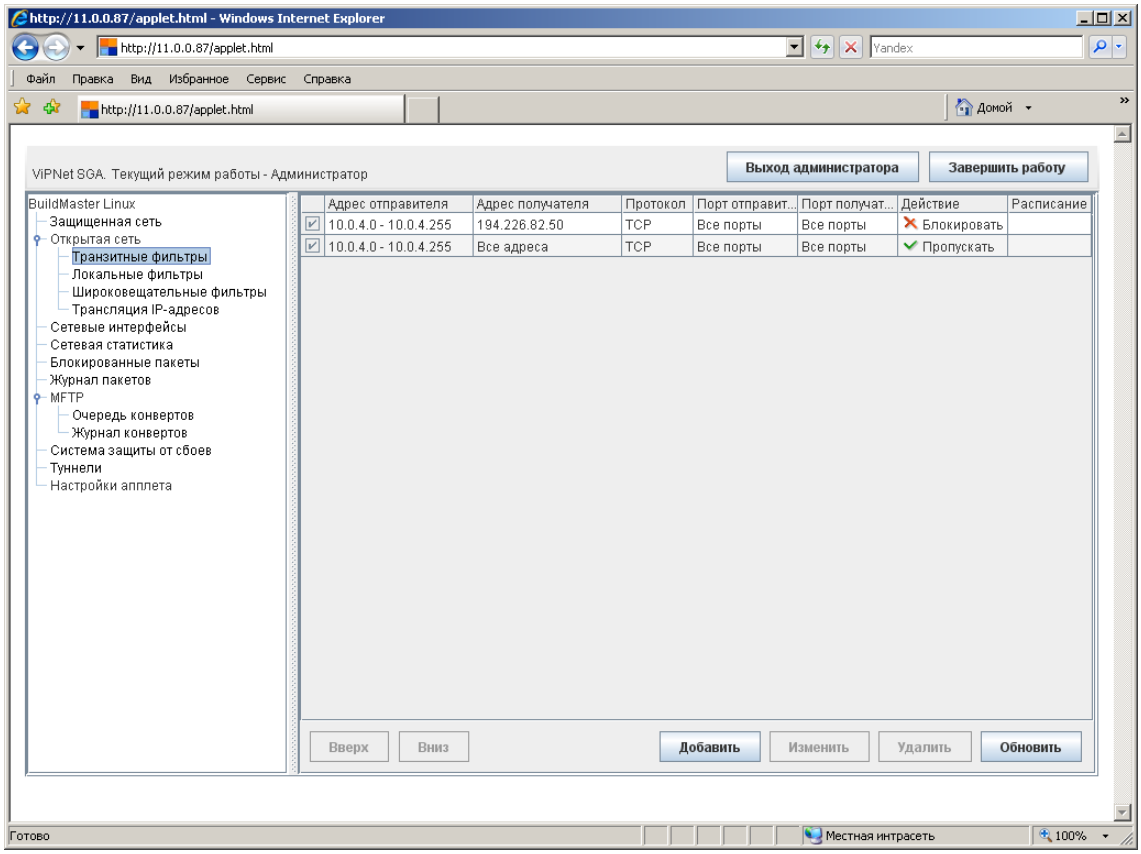

Рисунок 18. Фильтры транзитных IP-пакетов (режим администратора)

В режиме администратора доступны следующие элементы управления правилами:

- Кнопки перемещения выбранного в списке правила на одну позицию вверх (кнопка **Вверх**) или на одну позицию вниз (кнопка **Вниз**).
- Кнопка **Добавить** для создания нового правила.
- Кнопка **Изменить** для изменения выбранного в списке правила.
- Кнопка **Удалить** для удаления выбранного в списке правила.

  Перед удалением правила появится запрос на подтверждение удаления (Рисунок 19). Для удаления правила нажмите кнопку **ОК**, для отмены удаления – кнопку **Cancel**.

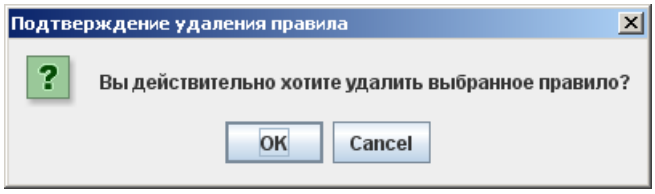

Рисунок 19. Запрос на подтверждение удаления правила

Просмотр правил фильтрации транзитных IP-пакетов

Вкладка **Транзитные фильтры** содержит список правил фильтрации транзитных IP-пакетов. Для каждого правила выводятся следующие составляющие:

Название столбца	Описание
1-й столбец не имеет названия	Флажок, указывающий на включение или отключение правила. Если правило включено (действует), то флажок установлен, иначе флажок снят.
Адрес отправителя	Условие для адреса отправителя пакета.
Адрес получателя	Условие для адреса получателя пакета.
Протокол	Условие для протокола, к которому должен принадлежать пакет.
Порт отправителя	Условие для порта отправителя пакета.
Порт получателя	Условие для порта получателя пакета.
Действие	Действие, которое нужно применить к пакету, параметры которого удовлетворяют условиям правила.
Расписание	Значок, указывающий на наличие расписания. При отсутствии расписания столбец пустой.

В режиме пользователя можно посмотреть любое правило в отдельном окне. Для этого выберите в списке правило и нажмите кнопку **Просмотреть.**

Чтобы получить актуальный список правил из файла конфигурации **firewall.conf**, нажмите кнопку **Обновить**. Эта кнопка присутствует на вкладке в любом режиме работы апплета.

В файле **firewall.conf** допустимы комплексные формы записи условий (списки протоколов, IP-адресов и т.д., группировка условий), которые невозможно отобразить в интерфейсе апплета. При просмотре правил с помощью апплета такие комплексные формы заменяются более простыми путем преобразования и/или декомпозиции правил, так что просматриваемый список правил может отличаться от списка правил, заданного в файле **firewall.conf**. Если изменить и затем сохранить правила с помощью апплета, то в файл **firewall.conf** будет записан список правил в том виде, в котором он отображается в апплете. Подробнее о декомпозиции правил фильтрации см. документ "ViPNet Coordinator Linux. Руководство администратора".

Создание и изменение правил фильтрации транзитных IP-пакетов

Для создания нового или изменения существующего правила фильтрации транзитных IP-пакетов необходимо войти в режим администратора. Чтобы создать новое правило, нажмите кнопку **Добавить**. Чтобы изменить правило, выберите в списке правило и нажмите кнопку **Изменить**. Появится окно, содержащее параметры правила. Для нового правила все параметры установлены в значения по умолчанию (Рисунок 20).

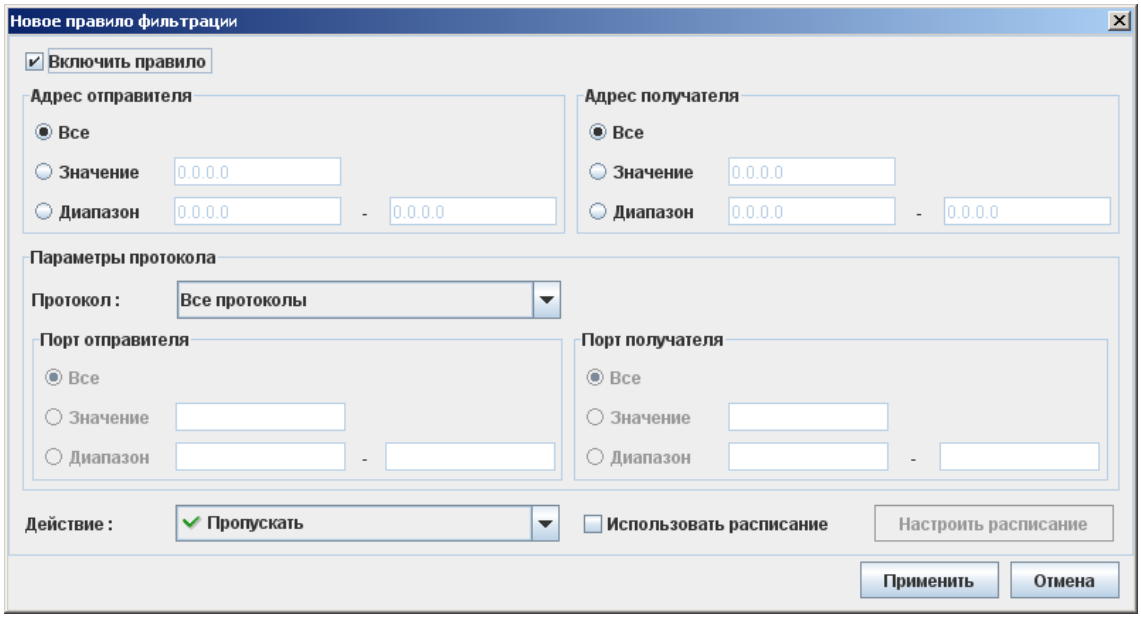

Рисунок 20. Создание правила фильтрации транзитных IP-пакетов

Значение протокола (поле **Протокол**) выбирается из списка, содержащего значения **Все протоколы**, **TCP**, **UDP**, **ICMP**. Для протоколов **TCP** и **UDP** можно задать условия для портов в полях **Порт отправителя** и **Порт получателя**. При выборе значения **Все протоколы** эти поля становятся недоступными, т.к. не во всех протоколах есть понятие порта (в протоколе ICMP его нет). При выборе значения **ICMP** вместо полей для портов появятся поля **Тип сообщения ICMP** и **Код сообщения ICMP** (Рисунок 21). В качестве типа и кода сообщения ICMP можно либо указать все значения (переключатель **Все**), либо задать одно значение (переключатель **Значение**).

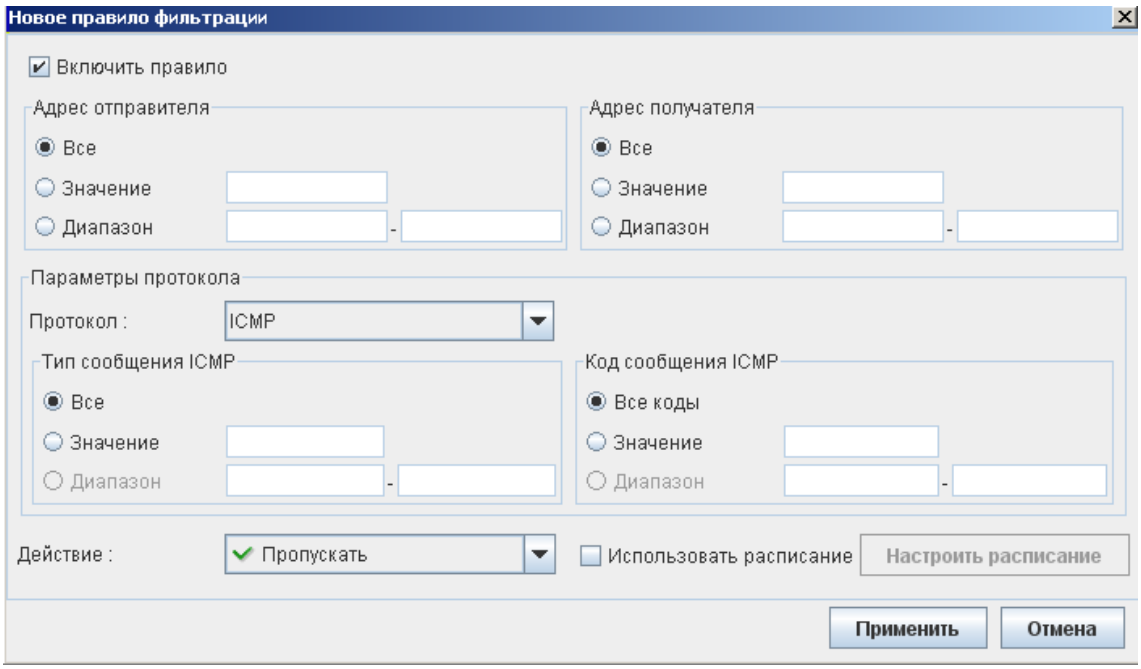

Рисунок 21. Создание транзитного фильтра для протокола ICMP

Установите требуемые значения параметров и нажмите кнопку **Применить**. Чтобы отказаться от создания нового правила или изменения параметров существующего правила, нажмите кнопку **Отмена**.

Настройка расписания

Расписание позволяет задать временные интервалы, в течение которых действует правило. Для нового правила по умолчанию расписание отсутствует, т.е. правило действует постоянно. Если правило должно действовать по расписанию, в окне с параметрами правила установите флажок **Использовать расписание** и нажмите кнопку **Настроить расписание**. Появится окно, содержащие параметры для настройки расписания (Рисунок 22).

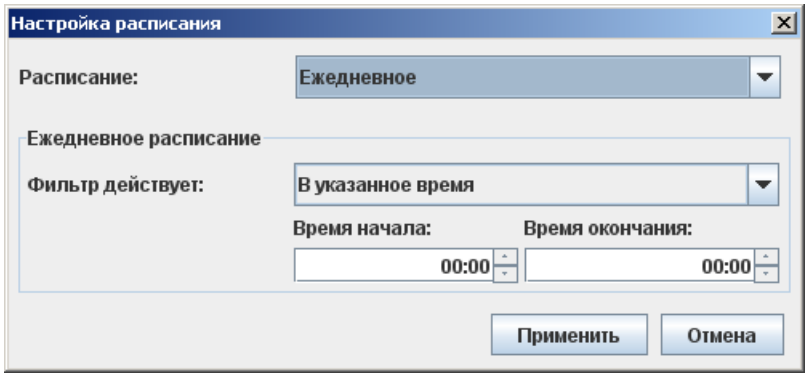

Рисунок 22. Настройка ежедневного расписания

Расписание может быть одного из двух типов - ежедневное (Рисунок 22) или еженедельное (Рисунок 23). Для указания типа расписания выберите нужное значение в списке **Расписание**.

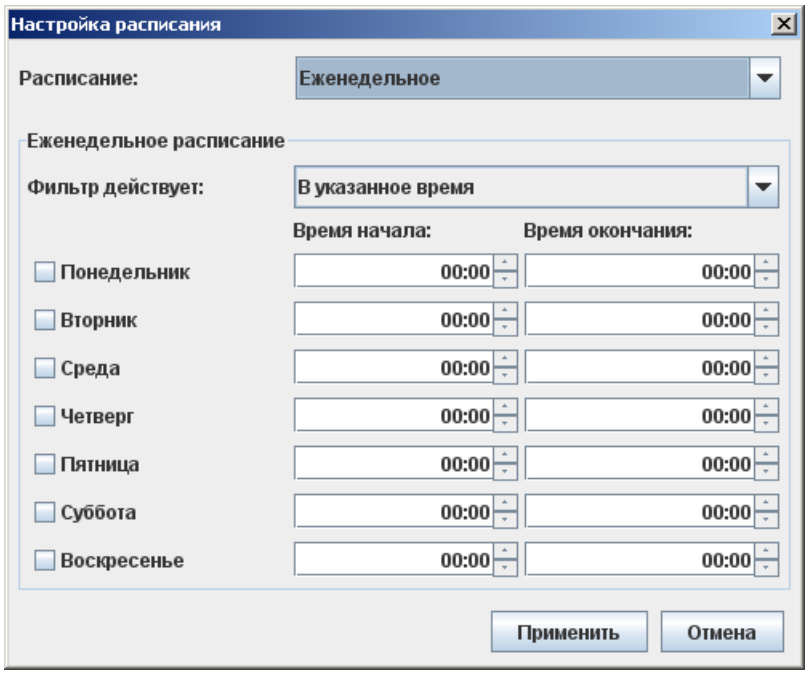

Рисунок 23. Настройка еженедельного расписания

Расписание можно настроить таким образом, чтобы правило действовало в указанное в нем время или, наоборот, не действовало в указанное время. Для этого выберите нужное значение в списке **Фильтр действует**:

- **В указанное время** – правило будет действовать в те интервалы времени, которые указаны в расписании, и не будет действовать в остальное время;

- **Все время, кроме указанного** – правило не будет действовать в указанные интервалы времени и будет действовать в остальное время.

Задайте требуемые интервалы времени. Для еженедельного расписания установите флажки около тех дней недели, для которых задаются интервалы времени. Те дни, для которых флажки не установлены, окажутся за пределами заданных интервалов времени.

Чтобы расписание вступило в силу, нажмите кнопку **Применить**. Чтобы игнорировать все внесенные в расписание изменения, нажмите кнопку **Отмена**.

Настройка правил фильтрации локальных IP-пакетов

Правила фильтрации локальных IP-пакетов задают фильтры IP-пакетов, у которых отправителем либо получателем является ViPNet-координатор. Эти правила содержатся в секции **[local]** файла конфигурации координатора **firewall.conf**. Подробное описание файла **firewall.conf** и синтаксиса правил см. в документе "ViPNet Coordinator Linux. Руководство администратора".

С помощью апплета можно посмотреть правила фильтрации локальных IP-пакетов, а также настроить правила: определить порядок применения правил, создать новые правила, изменить и удалить существующие правила. Порядок применения правил соответствует их порядку следования в файле **firewall.conf**. Первоначально правила отображаются в интерфейсе апплета в том порядке, в котором они записаны в файле **firewall.conf**. При изменении порядка правил с помощью апплета и сохранении этих изменений правила записываются в файл **firewall.conf** в порядке, заданном в апплете.

Настройка правил фильтрации локальных IP-пакетов выполняется на вкладке **Локальные фильтры**. В режиме пользователя доступен только просмотр правил (Рисунок 24).

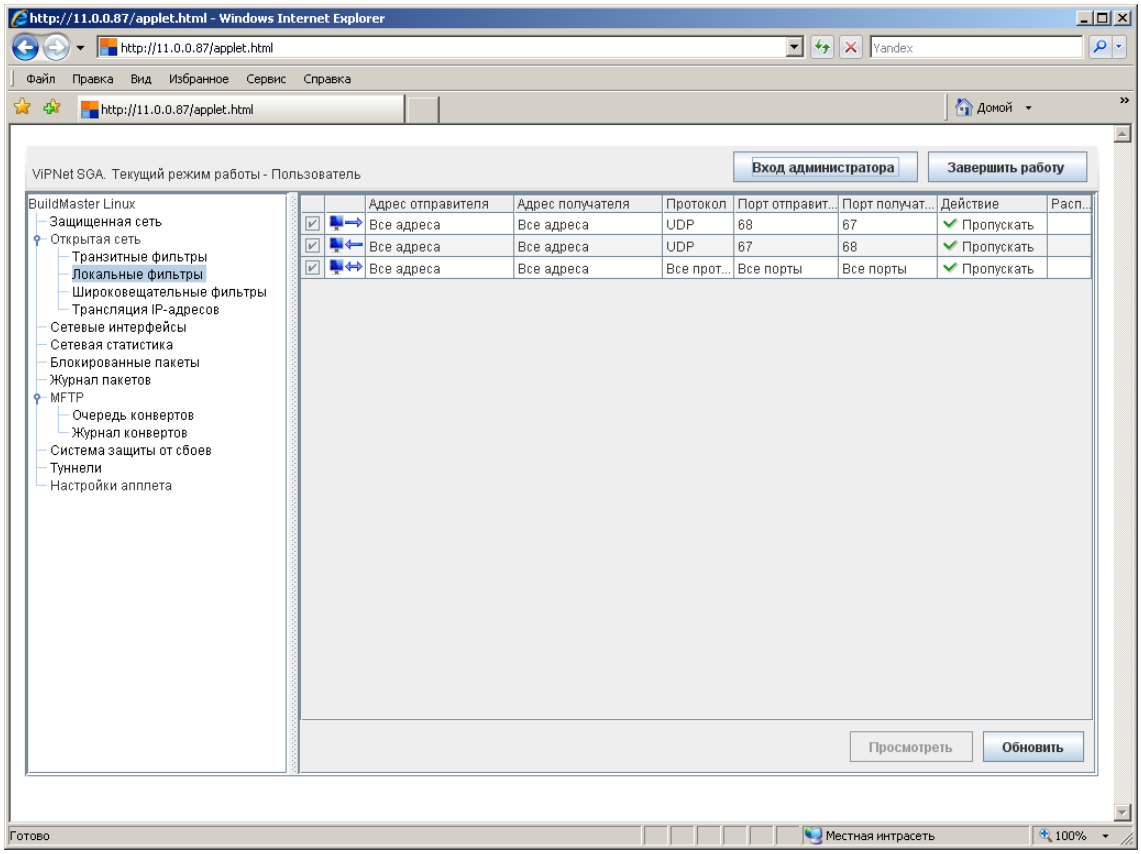

Рисунок 24. Фильтры локальных IP-пакетов (режим пользователя)

В режиме администратора, помимо просмотра, доступны все действия по настройке правил фильтрации локальных IP-пакетов (Рисунок 25).

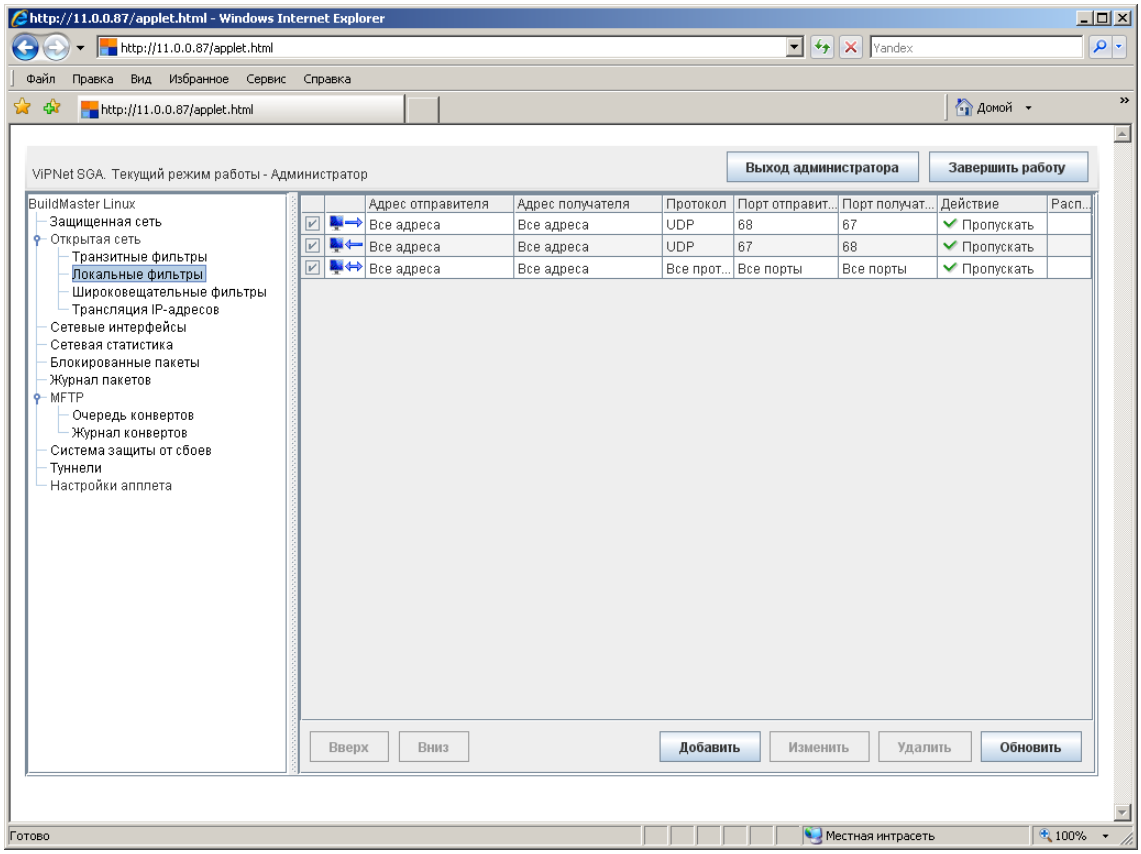

Рисунок 25. Фильтры локальных IP-пакетов (режим администратора)

В режиме администратора доступны следующие элементы управления правилами:

- Кнопки перемещения выбранного в списке правила на одну позицию вверх (кнопка **Вверх**) или на одну позицию вниз (кнопка **Вниз**).
- Кнопка **Добавить** для создания нового правила.
- Кнопка **Изменить** для изменения выбранного в списке правила.
- Кнопка **Удалить** для удаления выбранного в списке правила.

  Перед удалением правила появится запрос на подтверждение удаления (см. Рисунок 19). Для удаления правила нажмите кнопку **ОК**, для отмены удаления – кнопку **Cancel**.

Просмотр правил фильтрации локальных IP-пакетов

Вкладка **Локальные фильтры** содержит список правил фильтрации локальных IP-пакетов. Для каждого правила выводятся следующие составляющие:

Название столбца	Описание
1-й столбец не имеет названия	Флажок, указывающий на включение или отключение правила. Если правило включено (действует), то флажок установлен, иначе флажок снят.
2-й столбец не имеет названия	Условие для направления установления соединения. Условие отображается следующими значками:  – установление соединения по инициативе получателя;  – установление соединения по инициативе отправителя;  – установление соединения в любом направлении.
Адрес отправителя	Условие для адреса отправителя пакета.
Адрес получателя	Условие для адреса получателя пакета.
Протокол	Условие для протокола, к которому должен принадлежать пакет.
Порт отправителя	Условие для порта отправителя пакета.
Порт получателя	Условие для порта получателя пакета.
Действие	Действие, которое нужно применить к пакету, параметры которого удовлетворяют условиям правила.
Расписание	Значок, указывающий на наличие расписания. При отсутствии расписания столбец пустой.

В режиме пользователя можно посмотреть любое правило в отдельном окне. Для этого выберите в списке правило и нажмите кнопку **Просмотреть**.

Чтобы получить актуальный список правил из файла конфигурации **firewall.conf**, нажмите кнопку **Обновить**. Эта кнопка присутствует на вкладке в любом режиме работы апплета.

В файле **firewall.conf** допустимы комплексные формы записи условий (списки протоколов, IP-адресов и т.д., группировка условий), которые невозможно отобразить в интерфейсе апплета. При просмотре правил с помощью апплета такие комплексные формы заменяются более простыми путем преобразования и/или декомпозиции правил, так что просматриваемый список правил может отличаться от списка правил, заданного в файле **firewall.conf**. Если изменить и затем сохранить правила с помощью апплета, то в файл **firewall.conf** будет записан список правил в том виде, в котором он отображается в апплете. Подробнее о декомпозиции правил фильтрации см. документ "ViPNet Coordinator Linux. Руководство администратора".

Создание и изменение правил фильтрации локальных IP-пакетов

Для создания нового или изменения существующего правила фильтрации локальных IP-пакетов необходимо войти в режим администратора. Чтобы создать новое правило, нажмите кнопку **Добавить**. Чтобы изменить правило, выберите в списке правило и нажмите кнопку **Изменить**. Появится окно, содержащее параметры правила. Для нового правила все параметры установлены в значения по умолчанию (Рисунок 26).

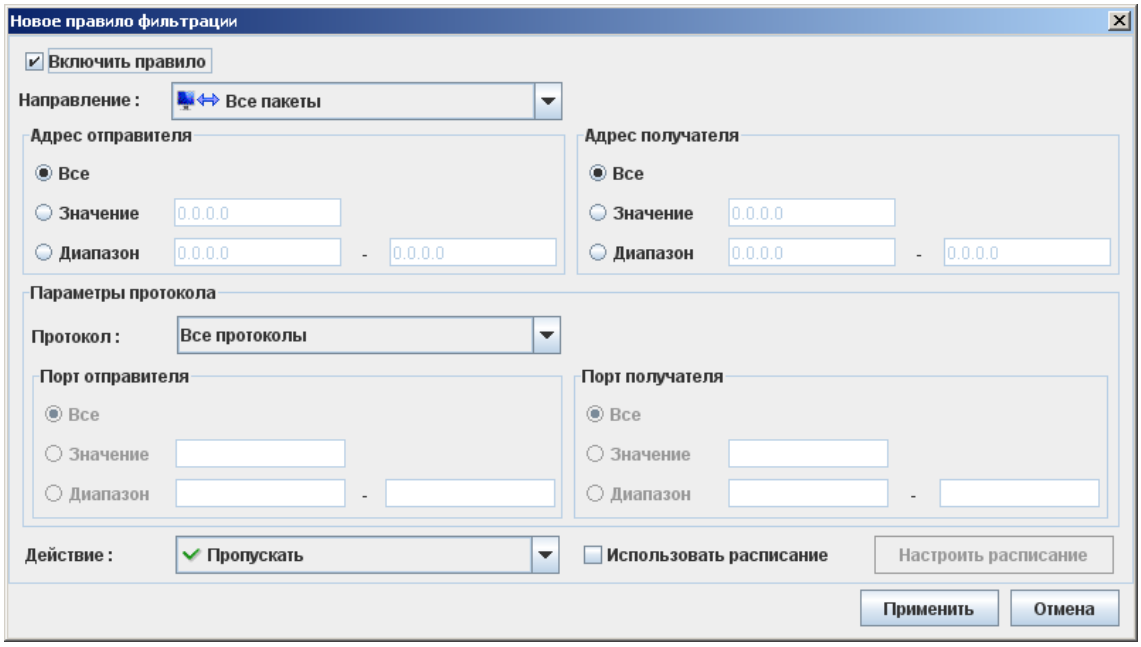

Рисунок 26. Создание правила фильтрации локальных IP-пакетов

Значение протокола (поле **Протокол**) выбирается из списка, содержащего значения **Все протоколы**, **TCP**, **UDP**, **ICMP**. Для протоколов **TCP** и **UDP** можно задать условия для портов в полях **Порт отправителя** и **Порт получателя**. При выборе значения **Все**

протоколы эти поля становятся недоступными, т.к. не во всех протоколах есть понятие порта (в протоколе ICMP его нет). При выборе значения **ICMP** вместо полей для портов появятся поля **Тип сообщения ICMP** и **Код сообщения ICMP** (Рисунок 27). В качестве типа и кода сообщения ICMP можно либо указать все значения (переключатель **Все**), либо задать одно значение (переключатель **Значение**).

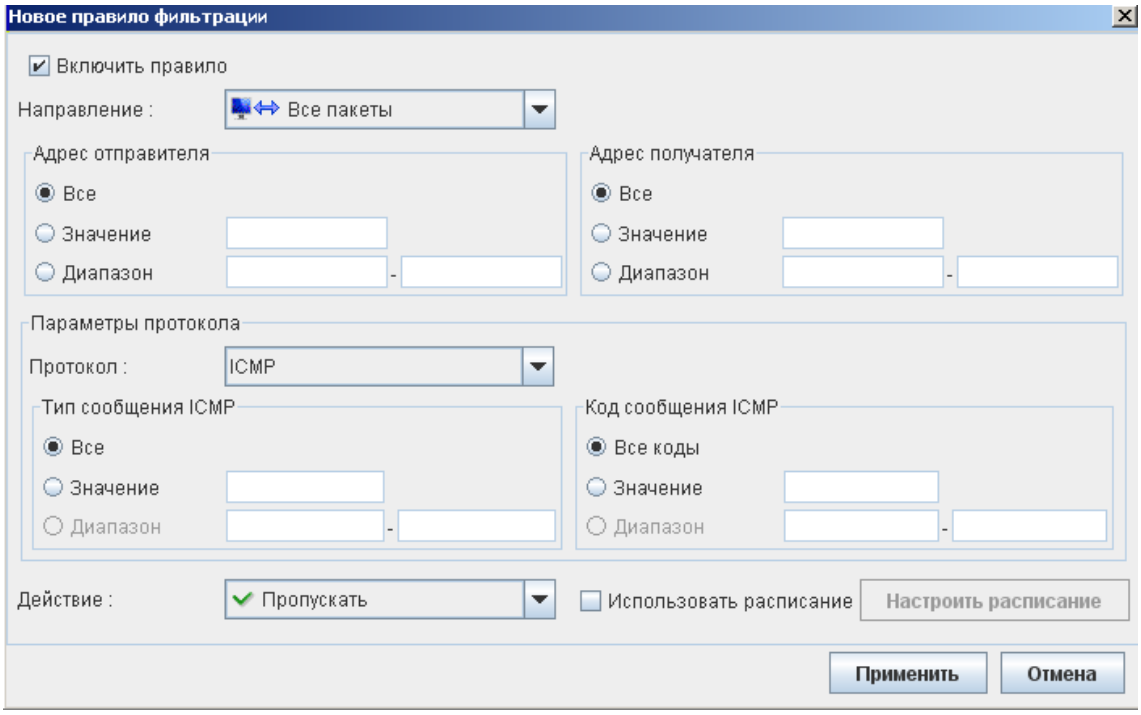

Рисунок 27. Создание локального фильтра для протокола ICMP

Установите требуемые значения параметров и нажмите кнопку **Применить**. Чтобы отказаться от создания нового правила или изменения параметров существующего правила, нажмите кнопку **Отмена**.

Настройка расписания

Расписание позволяет задать временные интервалы, в течение которых действует правило. Для нового правила по умолчанию расписание отсутствует, т.е. правило действует постоянно. Если правило должно действовать по расписанию, в окне с параметрами правила установите флажок **Использовать расписание** и нажмите кнопку **Настроить расписание**. Появится окно, содержащие параметры для настройки расписания. Настройка расписания для правил фильтрации локальных IP-пакетов выполняется так же, как для правил фильтрации транзитных IP-пакетов (см. Настройка расписания в разделе Настройка правил фильтрации транзитных IP-пакетов).

Настройка правил фильтрации широковещательных IP-пакетов

Правила фильтрации широковещательных IP-пакетов содержатся в секции **[broadcast]** файла конфигурации координатора **firewall.conf**. Подробное описание файла **firewall.conf** и синтаксиса правил см. в документе "ViPNet Coordinator Linux. Руководство администратора".

С помощью апплета можно посмотреть правила фильтрации широковещательных IP-пакетов, а также настроить правила: определить порядок применения правил, создать новые правила, изменить и удалить существующие правила. Порядок применения правил соответствует их порядку следования в файле **firewall.conf**. Первоначально правила отображаются в интерфейсе апплета в том порядке, в котором они записаны в файле **firewall.conf**. При изменении порядка правил с помощью апплета и сохранении этих изменений правила записываются в файл **firewall.conf** в порядке, заданном в апплете.

Настройка правил фильтрации широковещательных IP-пакетов выполняется на вкладке **Широковещательные фильтры**. В режиме пользователя доступен только просмотр правил (Рисунок 28).

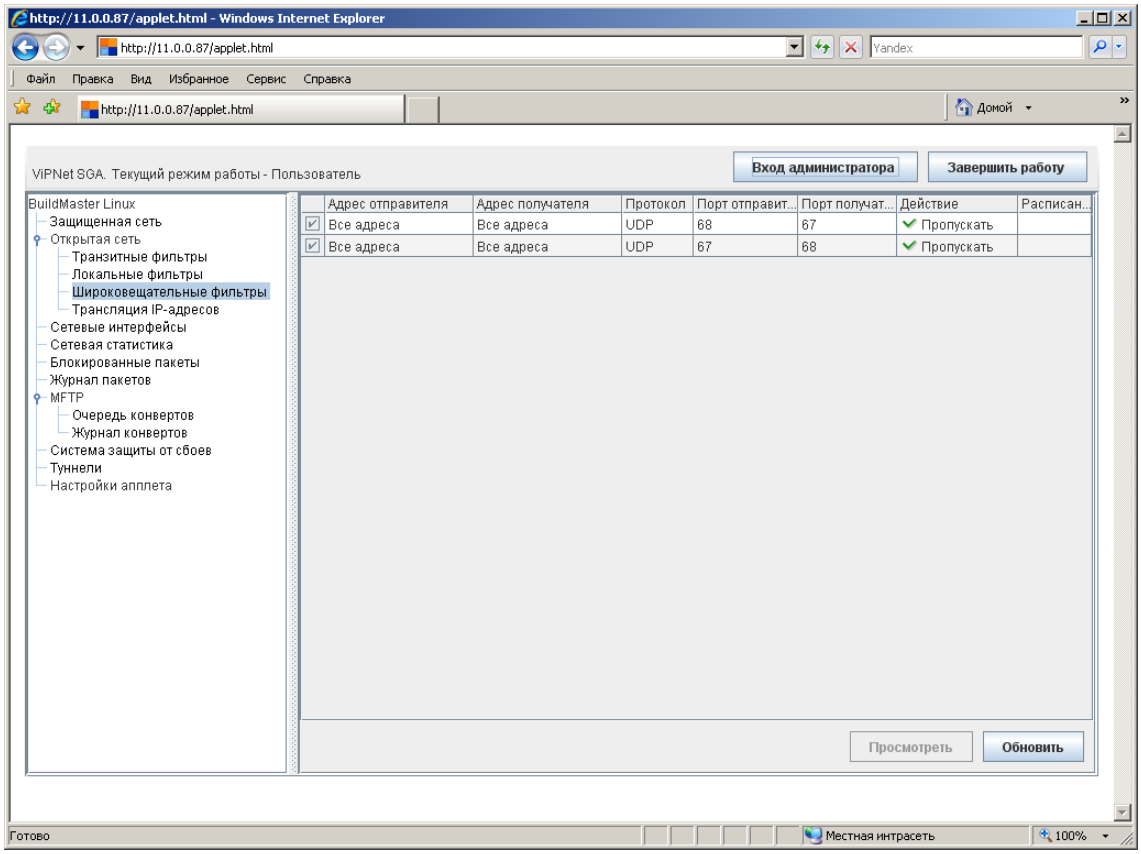

Рисунок 28. Фильтры широковещательных IP-пакетов (режим пользователя)

В режиме администратора, помимо просмотра, доступны все действия по настройке правил фильтрации широковещательных IP-пакетов (Рисунок 29).

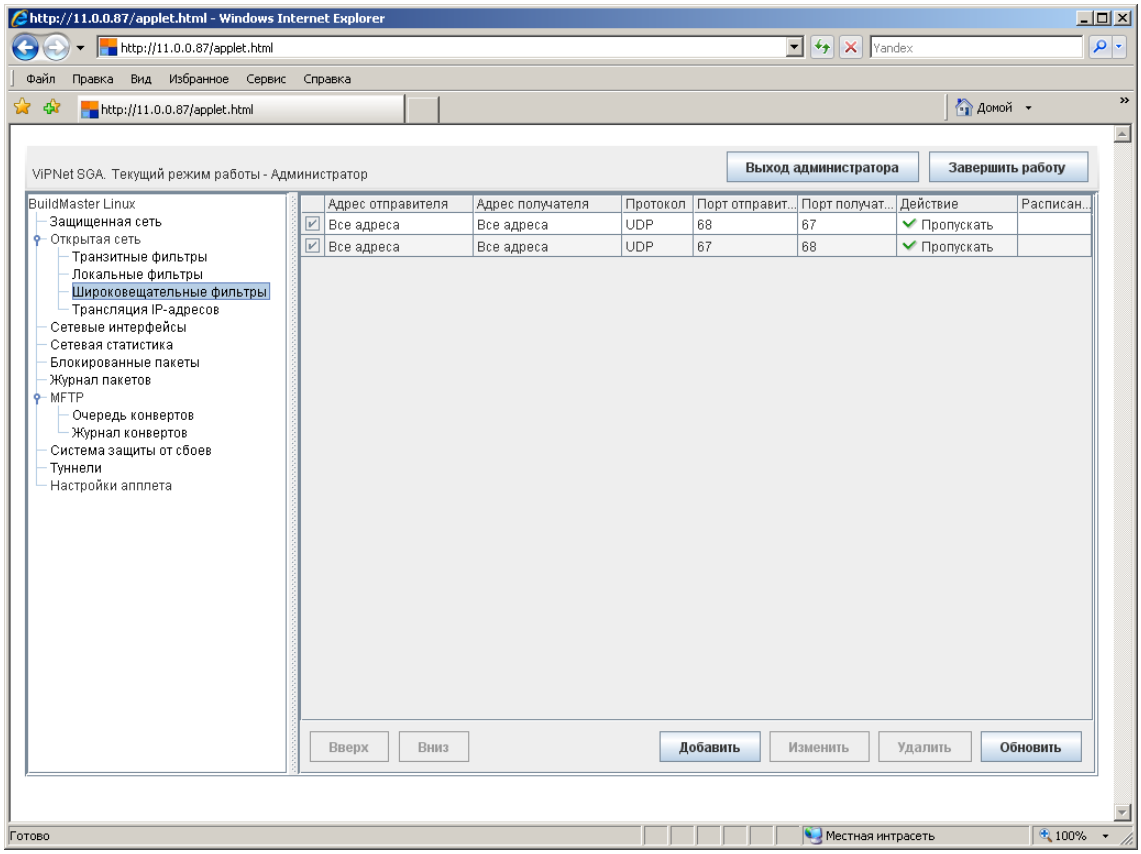

Рисунок 29. Фильтры широковещательных IP-пакетов (режим администратора)

В режиме администратора доступны следующие элементы управления правилами:

- Кнопки перемещения выбранного в списке правила на одну позицию вверх (кнопка **Вверх**) или на одну позицию вниз (кнопка **Вниз**).
- Кнопка **Добавить** для создания нового правила.
- Кнопка **Изменить** для изменения выбранного в списке правила.
- Кнопка **Удалить** для удаления выбранного в списке правила.

  Перед удалением правила появится запрос на подтверждение удаления (см. Рисунок 19). Для удаления правила нажмите кнопку **ОК**, для отмены удаления – кнопку **Cancel**.

Просмотр правил фильтрации широковещательных IP-пакетов

Вкладка **Широковещательные фильтры** содержит список правил фильтрации широковещательных IP-пакетов. Для каждого правила выводятся следующие составляющие:

Название столбца	Описание
1-й столбец не имеет названия	Флажок, указывающий на включение или отключение правила. Если правило включено (действует), то флажок установлен, иначе флажок снят.
Адрес отправителя	Условие для адреса отправителя пакета.
Адрес получателя	Условие для адреса получателя пакета.
Протокол	Условие для протокола, к которому должен принадлежать пакет.
Порт отправителя	Условие для порта отправителя пакета.
Порт получателя	Условие для порта получателя пакета.
Действие	Действие, которое нужно применить к пакету, параметры которого удовлетворяют условиям правила.
Расписание	Значок, указывающий на наличие расписания. При отсутствии расписания столбец пустой.

В режиме пользователя можно посмотреть любое правило в отдельном окне. Для этого выберите в списке правило и нажмите кнопку **Просмотреть.**

Чтобы получить актуальный список правил из файла конфигурации **firewall.conf**, нажмите кнопку **Обновить**. Эта кнопка присутствует на вкладке в любом режиме работы апплета.

В файле **firewall.conf** допустимы комплексные формы записи условий (списки протоколов, IP-адресов и т.д., группировка условий), которые невозможно отобразить в интерфейсе апплета. При просмотре правил с помощью апплета такие комплексные формы заменяются более простыми путем преобразования и/или декомпозиции правил,

так что просматриваемый список правил может отличаться от списка правил, заданного в файле **firewall.conf**. Если изменить и затем сохранить правила с помощью апплета, то в файл **firewall.conf** будет записан список правил в том виде, в котором он отображается в апплете. Подробнее о декомпозиции правил фильтрации см. документ "ViPNet Coordinator Linux. Руководство администратора".

Создание и изменение правил фильтрации широковещательных IP-пакетов

Для создания нового или изменения существующего правила фильтрации широковещательных IP-пакетов необходимо войти в режим администратора. Чтобы создать новое правило, нажмите кнопку **Добавить**. Чтобы изменить правило, выберите в списке правило и нажмите кнопку **Изменить**. Появится окно, содержащее параметры правила. Для нового правила все параметры установлены в значения по умолчанию (Рисунок 30).

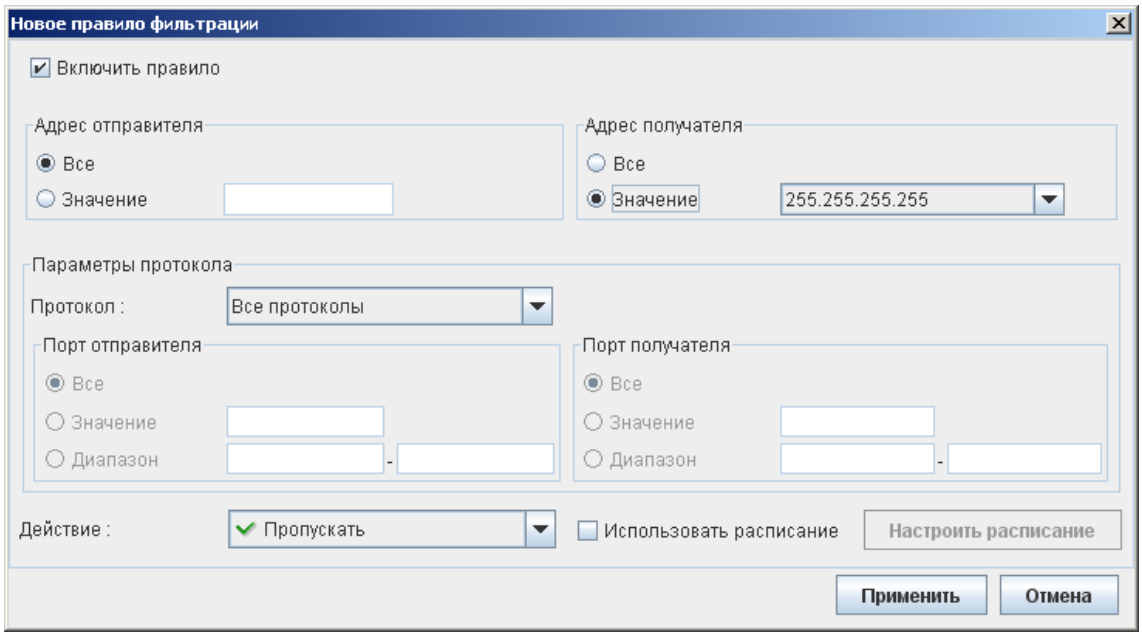

Рисунок 30. Создание правила фильтрации широковещательных IP-пакетов

В качестве адреса получателя (группа переключателей **Адрес получателя**) можно либо выбрать все широковещательные адреса (переключатель **Все**), либо задать один адрес (переключатель **Значение**). Значение единичного адреса выбирается из списка, который содержит адрес 255.255.255.255 и широковещательные адреса подсетей, непосредственно подключенных к сетевым интерфейсам сервера (эти широковещательные адреса вычисляются апплетом, исходя из IP-адресов и масок подсети для сетевых интерфейсов).

Значение протокола (поле **Протокол**) выбирается из списка, содержащего значения **Все протоколы**, **UDP**, **ICMP**. Для протокола **UDP** можно задать условия для портов в полях **Порт отправителя** и **Порт получателя**. При выборе значения **Все протоколы** эти поля становятся недоступными, т.к. не во всех протоколах есть понятие порта (в протоколе ICMP его нет). При выборе значения **ICMP** вместо полей для портов появятся поля **Тип сообщения ICMP** и **Код сообщения ICMP** (Рисунок 31). В качестве типа и кода сообщения ICMP можно либо указать все значения (переключатель **Все**), либо задать одно значение (переключатель **Значение**).

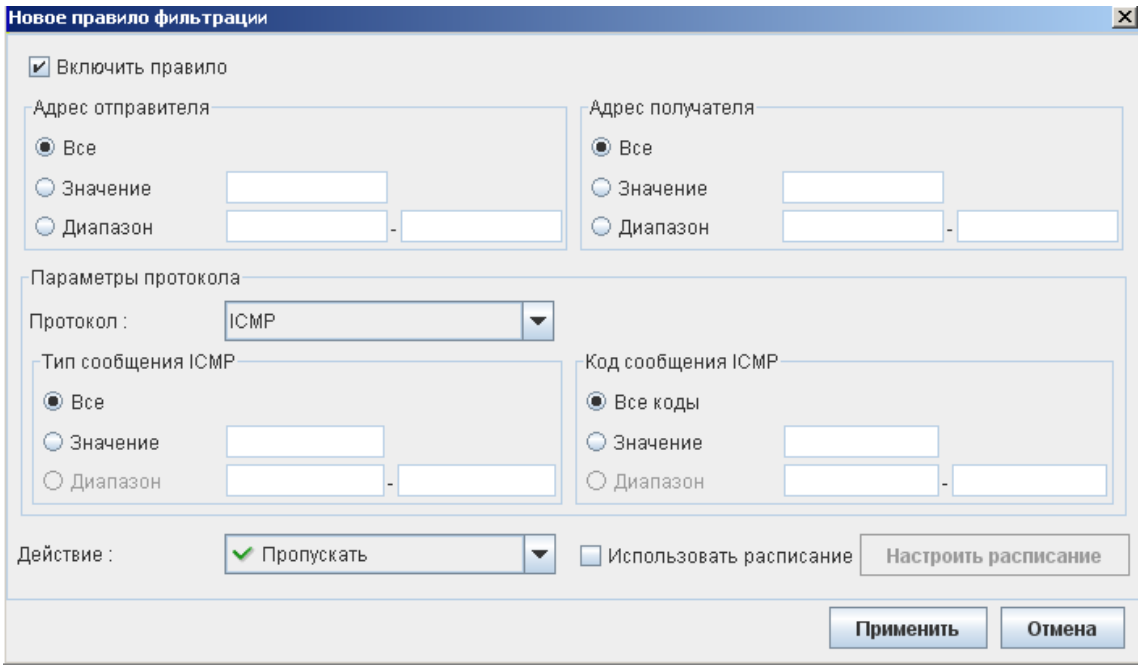

Рисунок 31. Создание широковещательного фильтра для протокола ICMP

Установите требуемые значения параметров и нажмите кнопку **Применить**. Чтобы отказаться от создания нового правила или изменения параметров существующего правила, нажмите кнопку **Отмена**.

Настройка расписания

Расписание позволяет задать временные интервалы, в течение которых действует правило. Для нового правила по умолчанию расписание отсутствует, т.е. правило действует постоянно. Если правило должно действовать по расписанию, в окне с параметрами правила установите флажок **Использовать расписание** и нажмите кнопку **Настроить расписание**. Появится окно, содержащие параметры для настройки расписания. Настройка расписания для правил фильтрации широковещательных IP-

пакетов выполняется так же, как для правил фильтрации транзитных IP-пакетов (см. Настройка расписания в разделе Настройка правил фильтрации транзитных IP-пакетов).

Настройка правил трансляции адресов

Правила трансляции адресов задают правила преобразования адреса отправителя или адреса получателя IP-пакетов. Эти правила содержатся в секции **[nat]** файла конфигурации координатора **firewall.conf**. Подробное описание файла **firewall.conf** и синтаксиса правил см. в документе "ViPNet Coordinator Linux. Руководство администратора".

С помощью апплета можно посмотреть правила трансляции адресов, а также настроить правила: создать новые правила, изменить и удалить существующие правила.

Настройка правил трансляции адресов выполняется на вкладке **Трансляция IP-адресов**. В режиме пользователя доступен только просмотр правил (Рисунок 32).

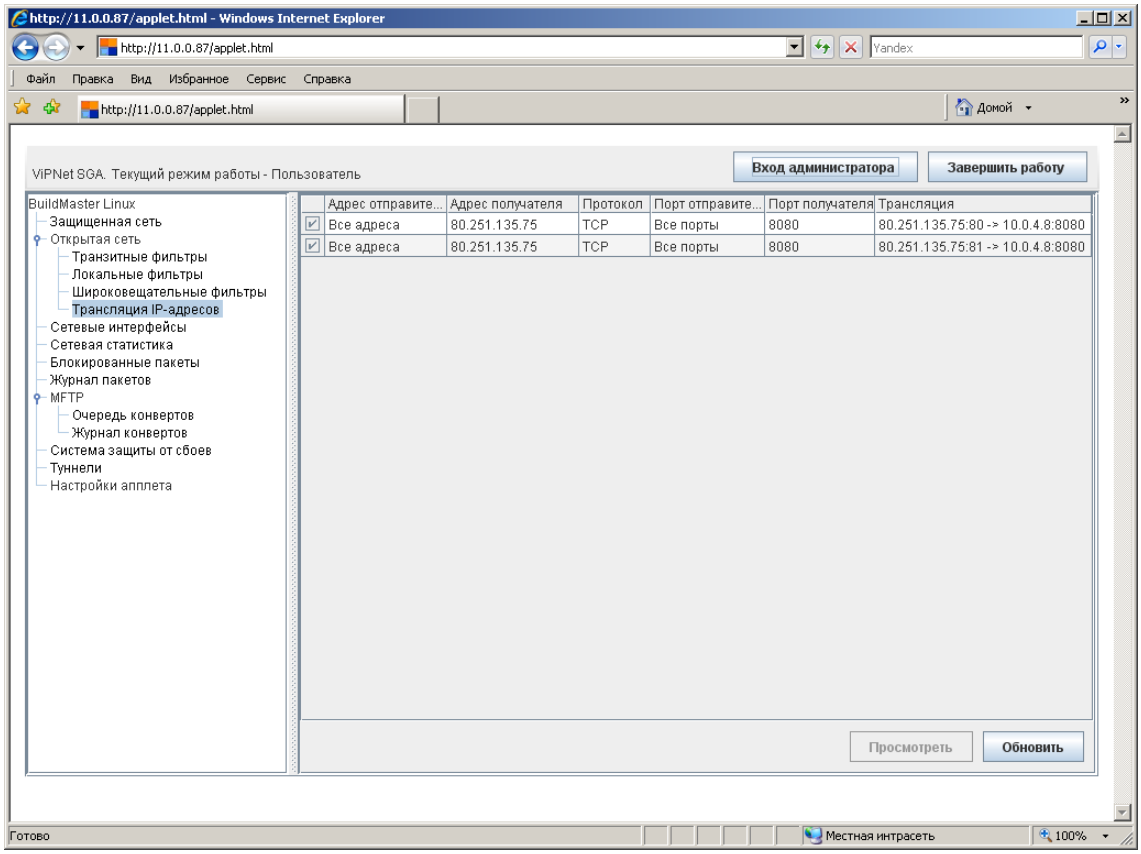

Рисунок 32.Правила трансляции адресов (режим пользователя)

В режиме администратора, помимо просмотра, доступны все действия по настройке правил трансляции адресов (Рисунок 33).

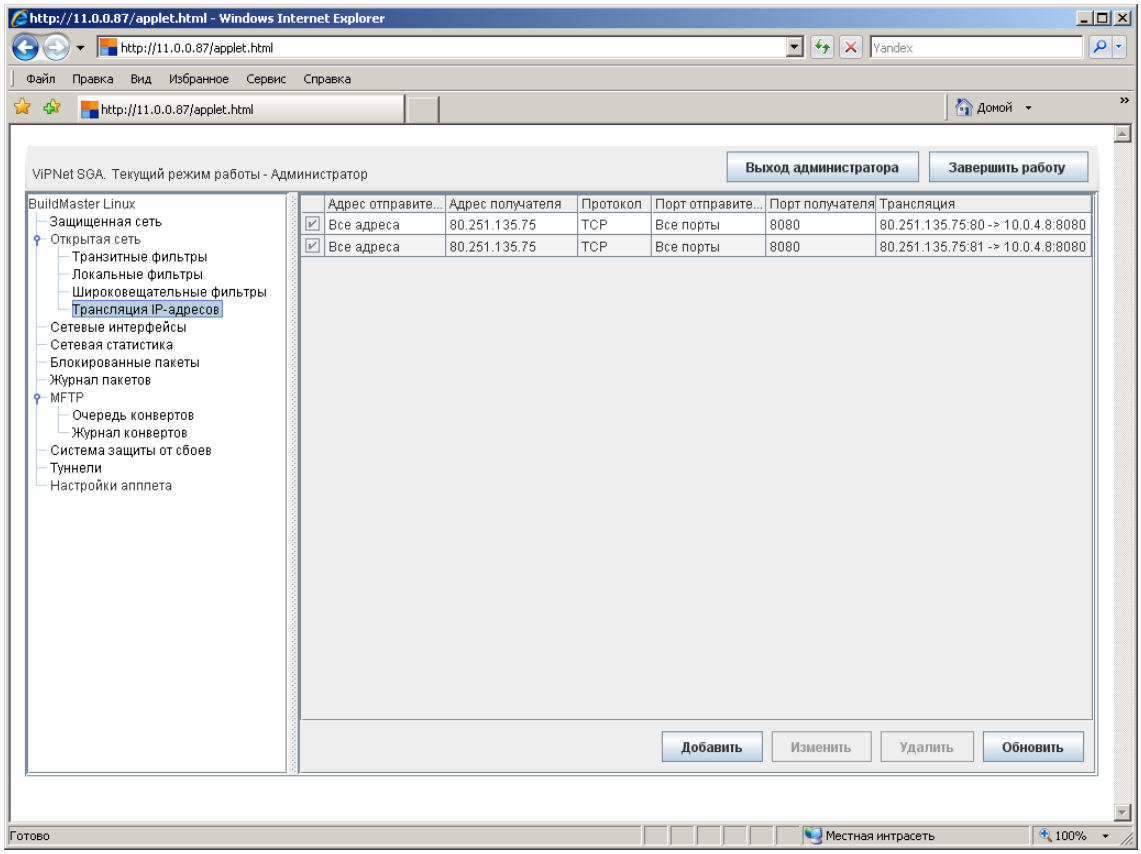

Рисунок 33. Правила трансляции адресов (режим администратора)

В режиме администратора доступны следующие элементы управления правилами:

- Кнопка **Добавить** для создания нового правила.
- Кнопка **Изменить** для изменения выбранного в списке правила.
- Кнопка **Удалить** для удаления выбранного в списке правила.

  Перед удалением правила появится запрос на подтверждение удаления (см. Рисунок 19). Для удаления правила нажмите кнопку **ОК**, для отмены удаления – кнопку **Cancel**.

Просмотр правил трансляции адресов

Вкладка **Трансляция IP-адресов** содержит список правил трансляции адресов. Для каждого правила выводятся следующие составляющие:

Название столбца	Описание
1-й столбец не имеет названия	Флажок, указывающий на включение или отключение правила. Если правило включено (действует), то флажок установлен, иначе флажок снят.
Адрес отправителя	Условие для адреса отправителя пакета.
Адрес получателя	Условие для адреса получателя пакета.
Протокол	Условие для протокола, к которому должен принадлежать пакет.
Порт отправителя	Условие для порта отправителя пакета.
Порт получателя	Условие для порта получателя пакета.
Трансляция	Преобразование адресов для пакетов, удовлетворяющих условиям правила (какие адреса заменяются и каким именно адресом).

В режиме пользователя можно посмотреть любое правило в отдельном окне. Для этого выберите в списке правило и нажмите кнопку **Просмотреть.**

Чтобы получить актуальный список правил из файла конфигурации **firewall.conf**, нажмите кнопку **Обновить**. Эта кнопка присутствует на вкладке в любом режиме работы апплета.

В файле **firewall.conf** допустимы комплексные формы записи условий (списки протоколов, IP-адресов и т.д.), которые невозможно отобразить в интерфейсе апплета. При просмотре правил с помощью апплета такие комплексные формы заменяются более простыми путем декомпозиции правил, так что просматриваемый список правил может отличаться от списка правил, заданного в файле **firewall.conf**. Если изменить и затем сохранить правила с помощью апплета, то в файл **firewall.conf** будет записан список правил в том виде, в котором он отображается в апплете. Подробнее о декомпозиции правил трансляции адресов см. документ "ViPNet Coordinator Linux. Руководство администратора".

Создание и изменение правил трансляции адресов

Для создания нового или изменения существующего правила трансляции адресов необходимо войти в режим администратора. Чтобы создать новое правило, нажмите кнопку **Добавить**. Чтобы изменить правило, выберите в списке правило и нажмите кнопку **Изменить**. Появится окно, содержащее параметры правила. Для нового правила все параметры установлены в значения по умолчанию (Рисунок 34).

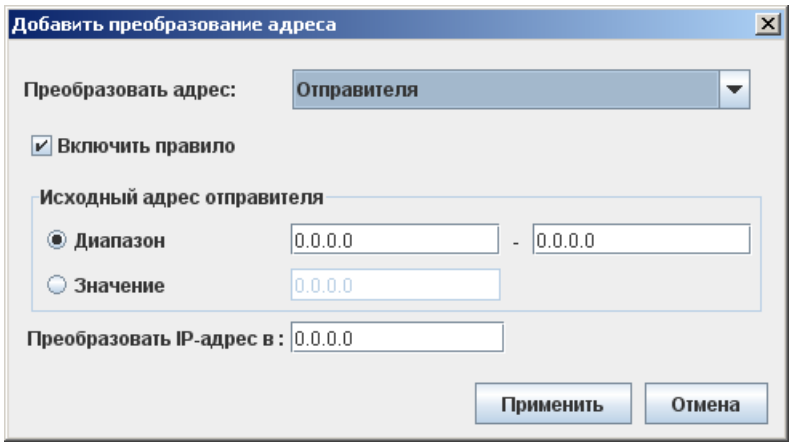

Рисунок 34. Создание правила трансляции адреса отправителя

Трансляция адреса может быть одного из двух типов – преобразование адреса отправителя (Рисунок 34) или преобразование адреса получателя (Рисунок 35). Для указания типа трансляции выберите нужное значение в списке **Преобразовать адрес**. Набор параметров правила зависит от используемого типа трансляции.

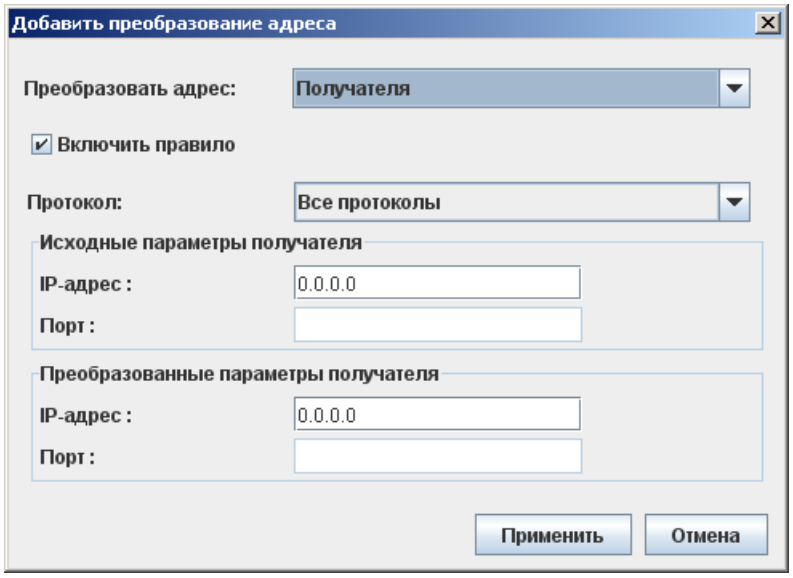

Рисунок 35. Создание правила трансляции адреса получателя

Для правила трансляции адреса получателя можно задать протокол. Значение протокола (поле **Протокол**) выбирается из списка, содержащего значения **Все протоколы**, **TCP**, **UDP**, **ICMP**. Для протоколов **TCP** и **UDP** можно задать условия для исходных и преобразованных портов в соответствующих полях **Порт**. При выборе значения **Все протоколы** эти поля становятся недоступными, т.к. не во всех протоколах есть понятие порта (в протоколе ICMP его нет).

Установите требуемые значения параметров и нажмите кнопку **Применить**. Чтобы отказаться от создания нового правила или изменения параметров существующего правила, нажмите кнопку **Отмена**.

Настройка параметров сетевых интерфейсов

Настройка параметров сетевых интерфейсов выполняется на вкладке **Сетевые интерфейсы** (Рисунок 36).

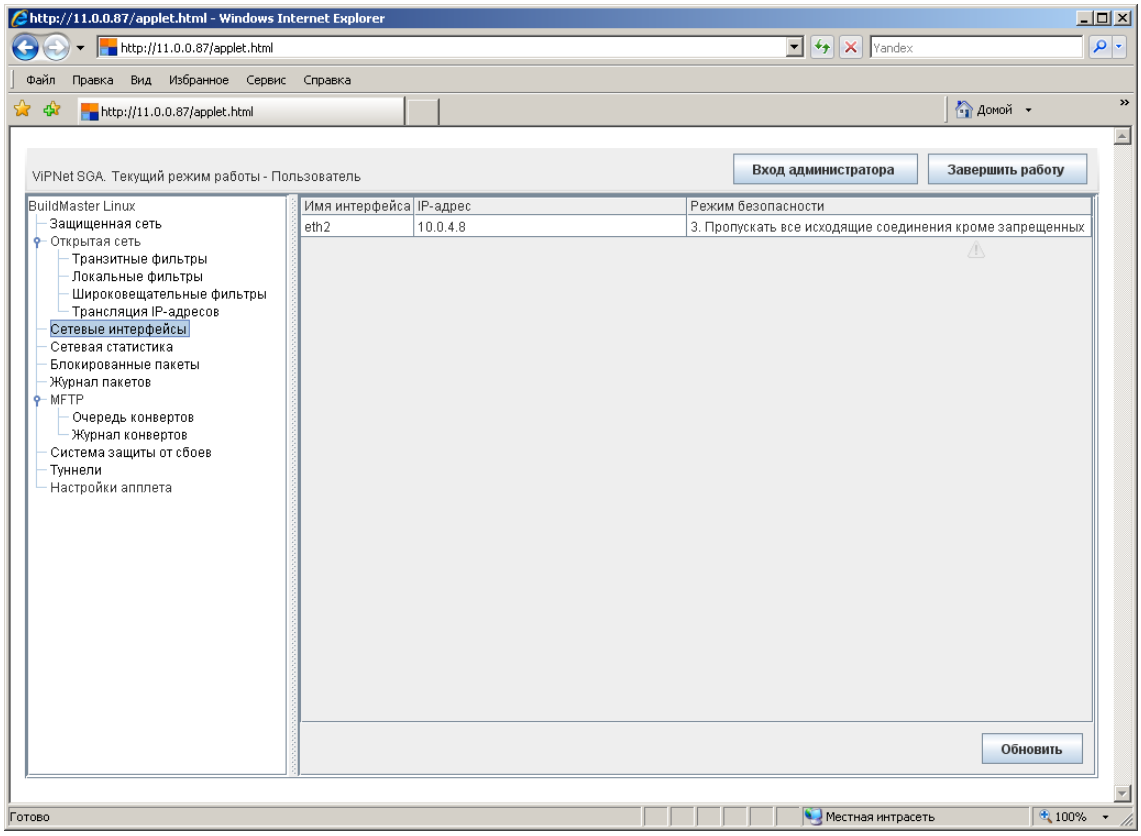

Рисунок 36. Сетевые интерфейсы

Вкладка **Сетевые интерфейсы** содержит список интерфейсов координатора. Для каждого интерфейса выводятся его параметры: имя сетевого интерфейса, его IP-адреса и текущий режим безопасности. Настройка параметров заключается в настройке режима безопасности на каждом из интерфейсов.

Изменить режим безопасности можно только в режиме администратора, в режиме пользователя доступен лишь просмотр параметров сетевых интерфейсов. В обоих

режимах на вкладке **Сетевые интерфейсы** присутствует кнопка **Обновить** для получения актуальных параметров сетевых интерфейсов.

При работе в режиме администратора на вкладке **Сетевые интерфейсы** появятся дополнительные кнопки **Применить** и **Отмена**. Чтобы изменить режим безопасности на каком-либо интерфейсе, щелкните мышью на его текущем режиме безопасности и выберите из списка требуемое значение (Рисунок 37).

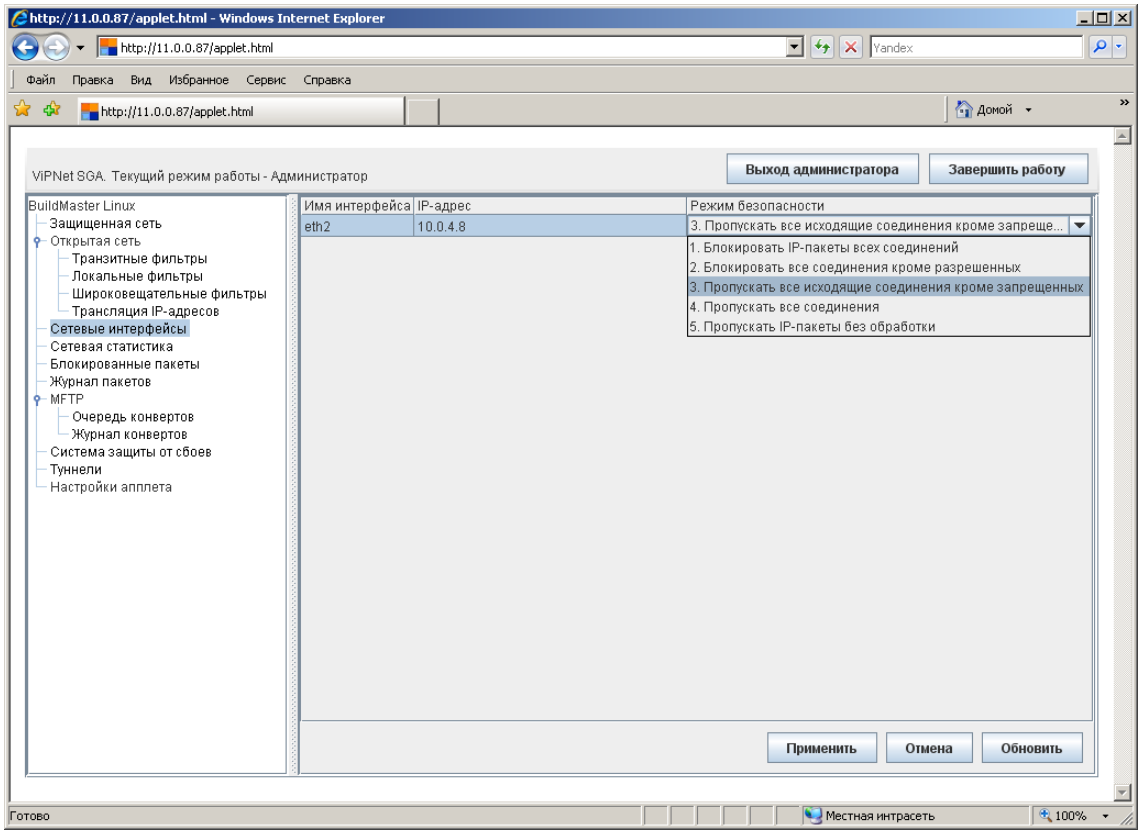

Рисунок 37. Изменение режима безопасности сетевого интерфейса

Чтобы внесенные изменения вступили в силу, нажмите кнопку **Применить**. Чтобы игнорировать все внесенные изменения, нажмите кнопку **Отмена**.

Просмотр статистики IP-пакетов по сетевым интерфейсам

Просмотр статистики IP-пакетов по сетевым интерфейсам координатора доступен на вкладке **Сетевая статистика** (Рисунок 38).

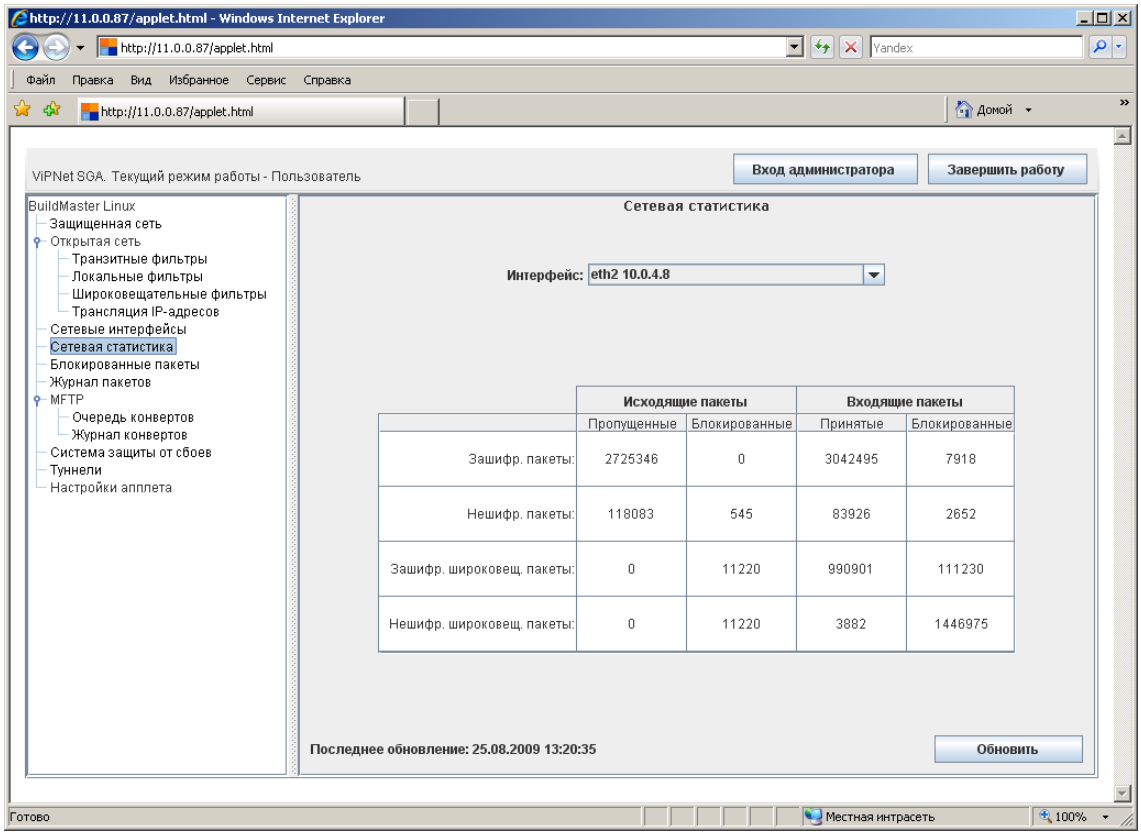

Рисунок 38. Сетевая статистика

На вкладке **Сетевая статистика** можно посмотреть статистику по любому сетевому интерфейсу. Для этого выберите из списка **Интерфейс** нужный интерфейс.

В нижней части вкладки отображаются дата и время последнего обновления статистики.

Сетевая статистика представлена в виде таблицы, содержащей следующие строки:

Название строки	Описание
Зашифр. пакеты	Статистика по зашифрованным IP-пакетам.
Нешифр. пакеты	Статистика по нешифрованным IP-пакетам.
Зашифр. широковещ. пакеты	Статистика по зашифрованным широковещательным IP-пакетам.
Нешифр. широковещ. пакеты	Статистика по нешифрованным широковещательным IP-пакетам.

По каждому типу пакетов (каждой строке таблицы) выводится следующая информация о количестве исходящих и входящих IP-пакетов:

Название столбца		Описание
Исходящие пакеты	Пропущенные	Количество успешно посланных пакетов
	Блокированные	Количество блокированных исходящих пакетов
Входящие пакеты	Принятые	Количество успешно принятых пакетов
	Блокированные	Количество блокированных входящих пакетов

На вкладке **Сетевая статистика** находится кнопка **Обновить** для получения актуальной статистики IP-пакетов по интерфейсу, выбранному в списке **Интерфейс**.

Просмотр информации о блокированных IP-пакетах

Просмотр информации о блокированных IP-пакетах доступен на вкладке **Блокированные пакеты** (Рисунок 39).

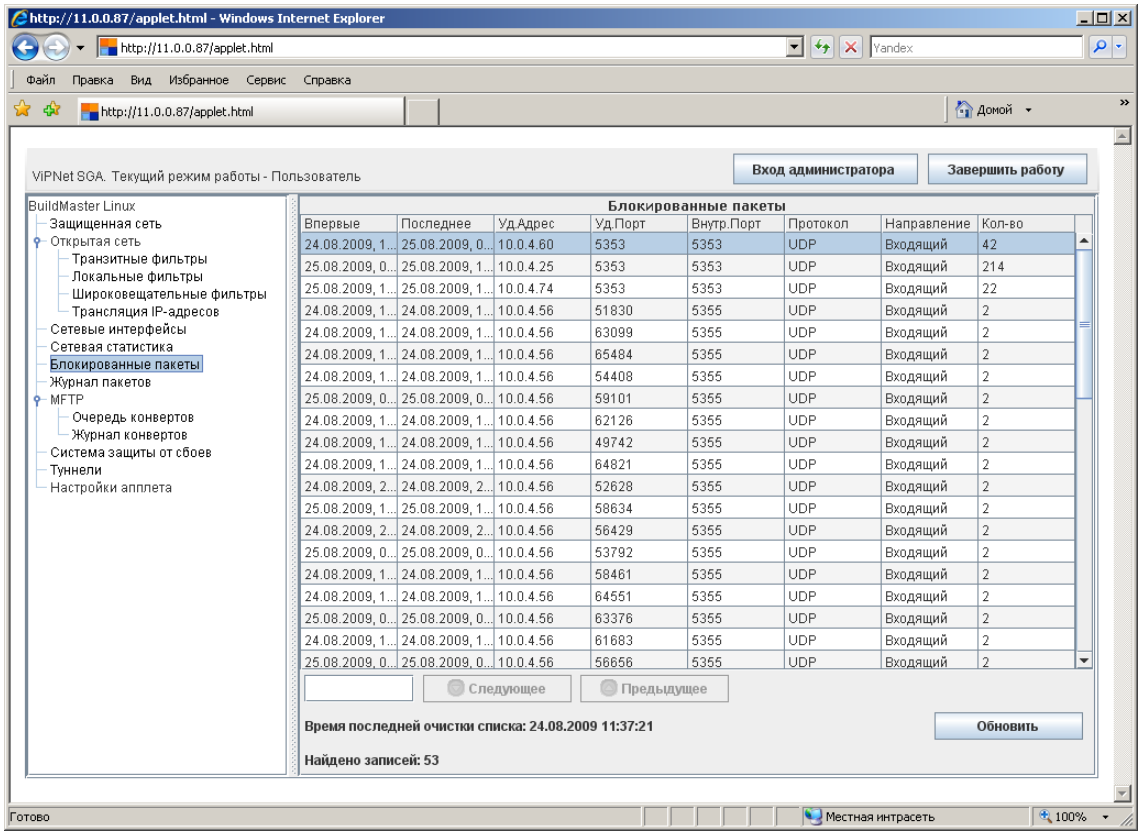

Рисунок 39. Блокированные пакеты

Вкладка **Блокированные пакеты** содержит список блокированных IP-пакетов. В нижней части вкладки отображаются дата и время последней очистки списка, а также количество записей в списке.

Для каждой записи списка выводится следующая информация:

Название столбца	Описание
Впервые	Дата и время создания записи при первом блокировании пакета с определенными характеристиками.
Последнее	Дата и время блокирования последнего пакета с такими же характеристиками.
Уд. Адрес	Значение внешнего IP-адреса, от которого пришли заблокированные пакеты или на который должны были быть отправлены заблокированные пакеты.
Уд. порт	Номер внешнего порта.
Внутр. порт	Номер локального порта.
Протокол	Протокол передачи блокированных пакетов.
Направление	Направление прохождения блокированных пакетов – входящие или исходящие.
Кол-во	Количество блокированных пакетов с одинаковыми характеристиками.

Записи можно отсортировать по любому столбцу (по возрастанию или убыванию, если в данном столбце числа; в алфавитном или обратном алфавитном порядке, если в данном столбце буквы). Для сортировки наведите указатель мыши на название столбца и щелкните левой кнопкой.

На вкладке **Блокированные пакеты** доступны следующие элементы управления:

- Поле ввода для поиска нужной записи по заданной подстроке. Поиск производится по всем столбцам.
- Кнопки перехода к следующей (кнопка **Следующее**) либо предыдущей (кнопка **Предыдущее**) записи, содержащей подстроку, указанную в поле поиска.
- Кнопка **Обновить** для получения актуальной информации о блокированных IP-пакетах.

При работе в режиме администратора на вкладке **Блокированные пакеты** появится дополнительная кнопка **Очистить** для очистки списка блокированных IP-пакетов.

Просмотр журнала регистрации IP-пакетов

Проходящий через ViPNet-координатор IP-трафик регистрируется в журнале IP-пакетов. Просмотр журнала доступен на вкладке **Журнал пакетов**. Перед просмотром необходимо задать условия отбора записей из журнала (Рисунок 40).

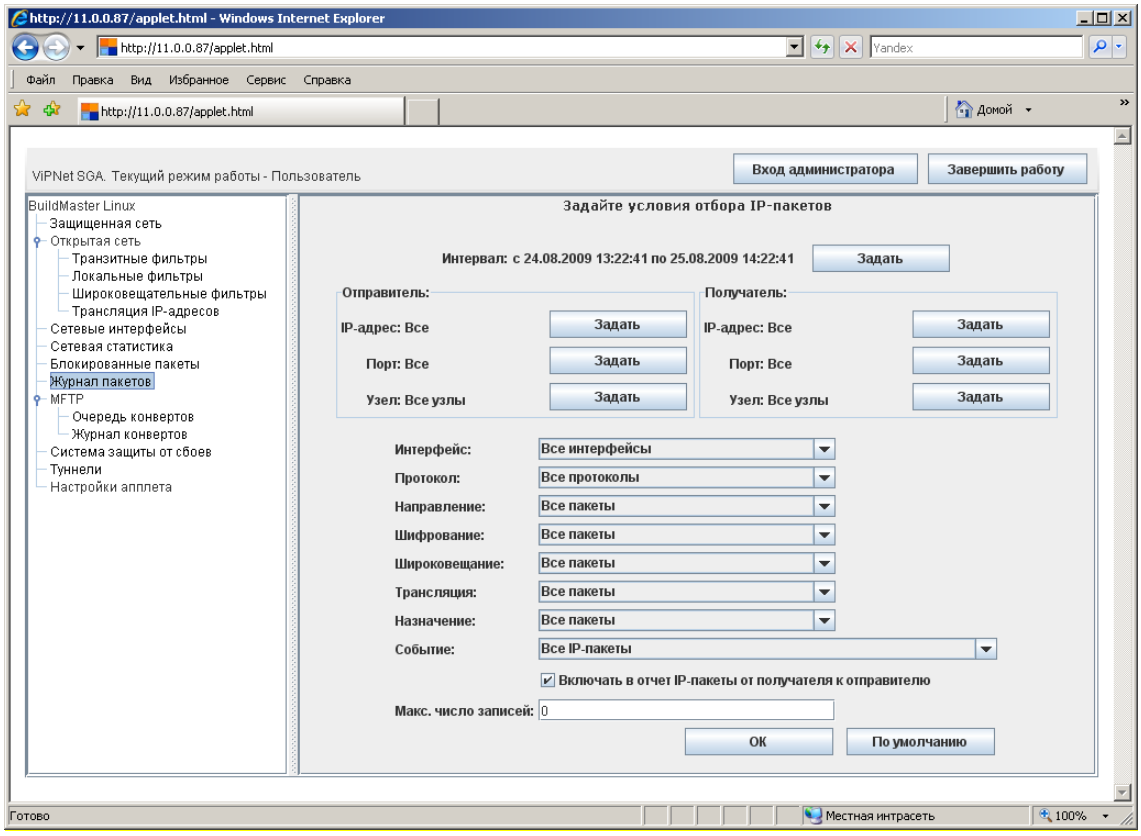

Рисунок 40. Параметры для отбора записей из журнала регистрации IP-пакетов

Первоначально все параметры, предусмотренные для отбора записей, установлены в значения по умолчанию. В этом случае для просмотра будут отобраны все записи журнала за последние сутки. Установить значения по умолчанию можно с помощью кнопки **По умолчанию**.

Для отбора записей по другим условиям можно задать следующие параметры:

- **Интервал** – выбор временного интервала для просмотра журнала. Значение по умолчанию - за сутки до момента просмотра. Для задания интервала нажмите кнопку **Задать.** Появится окно, в котором можно задать диапазон дат или последние несколько дней (Рисунок 41).

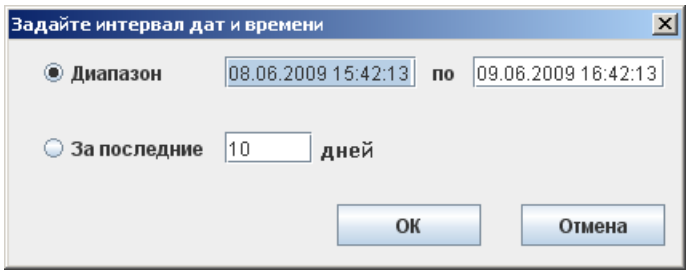

Рисунок 41.Задание интервала дат и времени

Установите переключатель в нужное положение, задайте интервал и нажмите кнопку **OK**.

- **IP-адрес отправителя** – фильтрация записей журнала по IP-адресу отправителя пакетов. Значение по умолчанию - все IP-адреса. Для задания IP-адреса нажмите кнопку **Задать.** Появится окно, в котором можно задать все адреса, или один адрес, или диапазон адресов (Рисунок 42).

Рисунок 42. Задание IP-адреса

Установите переключатель в нужное положение, задайте IP-адрес и нажмите кнопку **OK**.

- **Порт отправителя** – фильтрация записей журнала по номеру порта отправителя пакетов. Значение по умолчанию - все порты. Для задания порта нажмите кнопку **Задать**. Появится окно, в котором можно задать все порты, или один порт, или диапазон портов (Рисунок 43).

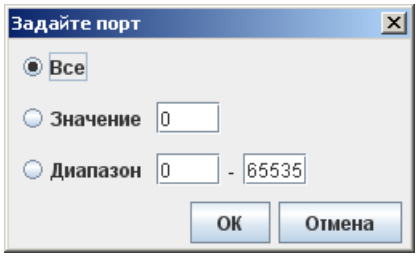

Рисунок 43. Задание номера порта

Установите переключатель в нужное положение, задайте порт и нажмите кнопку **OK**.

- **Узел отправителя** – фильтрация записей журнала по имени сетевого узла защищенной сети, являющегося отправителем пакетов. Значение по умолчанию - все узлы. Для задания узла нажмите кнопку **Задать**. Появится окно, в котором можно задать все узлы или один узел (Рисунок 44).

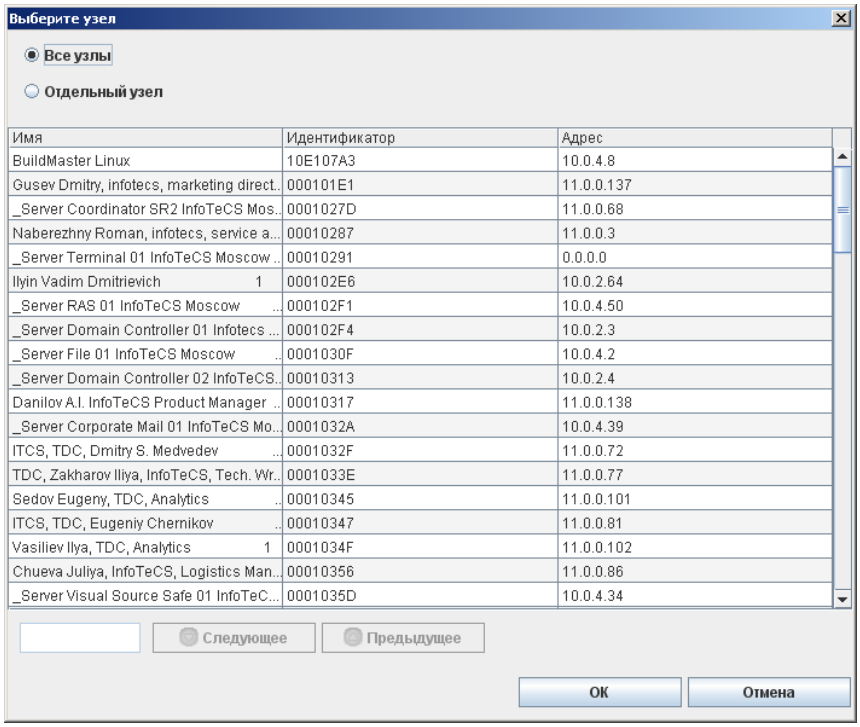

Рисунок 44. Задание узла отправителя

Для выбора конкретного сетевого узла установите переключатель в положение **Отдельный узел**, выберите в списке нужный узел и нажмите кнопку **OK**.

Под списком узлов расположено поле ввода для поиска нужного узла по заданной подстроке. Поиск производится по всем столбцам. С помощью кнопок **Следующее** и

Предыдущее можно перейти к следующей либо предыдущей записи, содержащей подстроку, указанную в поле поиска.

- **IP-адрес получателя** – фильтрация записей журнала по IP-адресу получателя пакетов. Значение по умолчанию - все IP-адреса. IP-адрес получателя задается так же, как IP-адрес отправителя (Рисунок 42).
- **Порт получателя** – фильтрация записей журнала по номеру порта получателя пакетов. Значение по умолчанию - все порты. Порт получателя задается так же, как порт отправителя (Рисунок 43).
- **Узел получателя** – фильтрация записей журнала по имени сетевого узла защищенной сети, являющегося получателем пакетов. Значение по умолчанию - все узлы. Узел получателя задается так же, как узел отправителя (Рисунок 44).
- **Интерфейс** – фильтрация записей журнала по интерфейсу, на котором зарегистрированы IP-пакеты. Значение по умолчанию - все интерфейсы. Для задания интерфейса выберите из списка нужный интерфейс или значение **Все интерфейсы**.
- **Протокол** – фильтрация записей журнала по протоколу, к которому принадлежат IP-пакеты. Значение по умолчанию - все протоколы. Для задания протокола выберите из списка нужный протокол или значение **Все протоколы**.
- **Направление** – фильтрация записей журнала по направлению трафика. Значение по умолчанию - все направления. Для задания направления выберите из списка нужное направление или значение **Все пакеты**.
- **Шифрование** – фильтрация записей журнала по признаку шифрования пакетов. Значение по умолчанию - все пакеты. Для задания признака шифрования выберите из списка нужное значение или значение **Все пакеты**.

  При выборе значения **Нешифрованные пакеты** нельзя задать параметры **Узел отправителя** и **Узел получателя** (для этих параметров автоматически устанавливаются значения по умолчанию **Все узлы**).
- **Широковещание** – фильтрация записей журнала по признаку широковещания. Значение по умолчанию - все пакеты. Для задания признака широковещания выберите из списка нужное значение или значение **Все пакеты**.
- **Трансляция** – фильтрация записей журнала по признаку трансляции адресов. Значение по умолчанию - все пакеты. Для задания признака трансляции выберите из списка нужное значение или значение **Все пакеты**.
- **Назначение** – фильтрация записей журнала по признаку локальности (назначению) пакетов. Значение по умолчанию - все пакеты. Для задания признака локальности выберите из списка нужное значение или значение **Все пакеты**.
- **Событие** – фильтрация записей журнала по событиям, которые ПО ViPNet Coordinator Linux присваивает каждому IP-пакету. Значение по умолчанию - все

пакеты. Для задания события выберите из списка нужное значение или значение **Все IP-пакеты**.

В качестве значения этого параметра можно выбрать как конкретное событие, так и группу событий. Если выбрана группа событий, то считается, что выбраны все события, входящие в группу. Описание событий, отслеживаемых ПО ViPNet Coordinator Linux, см. Приложение А. События, отслеживаемые ПО ViPNet Coordinator Linux.

- **Включать в отчет IP-пакеты от получателя к отправителю** – опция для включения/отключения отбора из журнала записей об ответных IP-пакетах. По умолчанию опция включена. При включенной опции из журнала дополнительно отбираются записи об IP-пакетах, направленных от указанного получателя к отправителю.

  Включенная опция имеет смысл, только если в качестве отправителя и/или получателя IP-пакетов (параметры **IP-адрес отправителя** и **IP-адрес получателя**) указан конкретный IP-адрес или диапазон адресов.

- **Макс. число записей** – максимальное число отображаемых записей журнала (от 0 до 65535). Значение по умолчанию - 0 (означает отсутствие ограничения на количество записей).

После задания значений параметров (или их установки в значения по умолчанию) нажмите кнопку **ОК**. Появится список найденных в журнале записей (Рисунок 45).

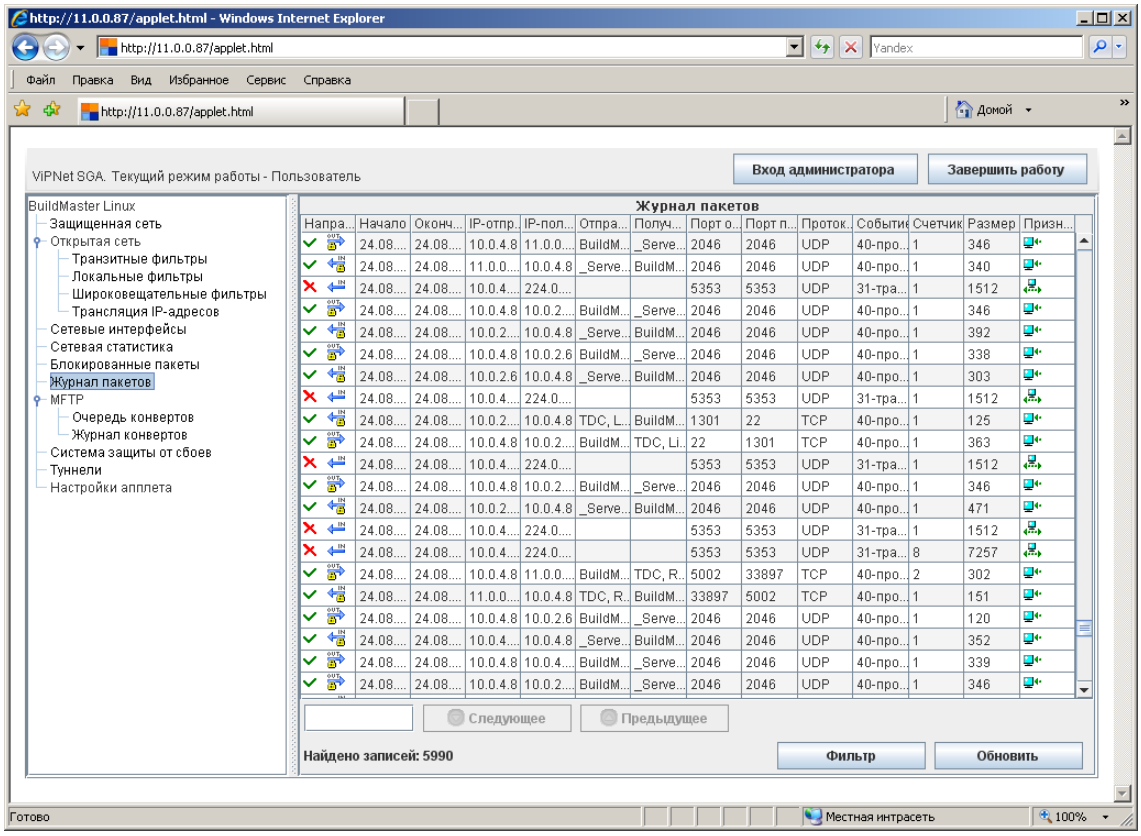

Рисунок 45. Журнал IP-пакетов

Для уменьшения объема журнала одинаковые записи о пакетах, зарегистрированные в течение короткого времени, объединяются в одну запись следующим образом:

- При регистрации пакета с определенными характеристиками (адресами, портами, протоколом и т.д.) создается новая запись, при этом дата и время создания записи фиксируются как начало записи (столбец **Начало**).
- Далее в течение времени, указанного в настройках координатора, подсчитывается количество пакетов с такими же характеристиками, при этом новая запись не создается. Количество пакетов отображается в столбце **Счетчик**.
- Дата и время регистрации последнего пакета с такими же характеристиками фиксируются как окончание записи (столбец **Окончание**). Окончание записи может измениться, пока не истечет указанное в настройках время.
- Подсчет пакетов с одинаковыми характеристиками заканчивается по истечении указанного в настройках времени. Если по истечении этого времени регистрируется очередной пакет с такими же характеристиками, то в журнале создается новая запись. Новая запись создается также при регистрации пакета с другими характеристиками

Для каждой записи журнала выводится следующая информация:

Название столбца	Описание
Направление	Столбец **Направление** содержит два значка. Первый значок указывает на тип события, присвоенного записи, второй значок указывает на направление IP-трафика. В журнале регистрируется четыре типа событий, которые отображаются следующими значками:  – IP-пакет пропущен (записи присвоено одно из событий группы **Все пропущенные IP-пакеты**);  – IP-пакет заблокирован (записи присвоено одно из событий группы **Блокированные IP-пакеты**);  – IP-пакет относится к группе событий **Служебные события**;  – IP-пакет блокирован системой обнаружения атак (записи присвоено одно из событий группы **События системы обнаружения атак**). Направление и признак шифрования IP-трафика отображаются следующими значками:  – открытые входящие IP-пакеты;  – открытые исходящие IP-пакеты;  – зашифрованные входящие IP-пакеты;  – зашифрованные исходящие IP-пакеты.
Начало	Дата и время создания записи.
Окончание	Дата и время окончания записи.
IP-отправителя	Значение IP-адреса, от которого пришел пакет.
IP-получателя	Значение IP-адреса, на который был отправлен пакет.

Название столбца	Описание
Отправитель	Имя сетевого узла, от которого пришел пакет.
Получатель	Имя сетевого узла, на который был отправлен пакет.
Порт отправителя	Номер порта, от которого пришел пакет.
Порт получателя	Номер порта, на который был отправлен пакет.
Протокол	Протокол передачи пакета.
Событие	Событие, присвоенное записи. Описание событий, отслеживаемых ПО ViPNet Coordinator Linux, см. Приложение А. События, отслеживаемые ПО ViPNet Coordinator Linux.
Счетчик	Количество IP-пакетов с одинаковыми характеристиками, объединенных в одну запись журнала.
Размер	Суммарный размер (в байтах) IP-пакетов с одинаковыми характеристиками, объединенных в одну запись журнала.
Признаки	В столбце **Признаки** отображаются признаки широковещания, трансляции и локальности IP-пакетов с помощью следующих значков:  – широковещательный IP-пакет; для обычного пакета ничего не отображается;  – транслированный IP-пакет; для нетранслированного пакета ничего не отображается;  – локальный пакет;  – транзитный пакет.

Записи можно отсортировать по любому столбцу (по возрастанию или убыванию, если в данном столбце числа; в алфавитном или обратном алфавитном порядке, если в данном столбце буквы). Для сортировки наведите указатель мыши на название столбца и щелкните левой кнопкой.

При просмотре журнала IP-пакетов доступны следующие элементы управления:

- Поле ввода для поиска нужной записи по заданной подстроке. Поиск производится по всем столбцам.
- Кнопки перехода к следующей (кнопка **Следующее**) либо предыдущей (кнопка **Предыдущее**) записи, содержащей подстроку, указанную в поле поиска.
- Кнопка **Фильтр** для возврата к заданию условий отбора IP-пакетов (Рисунок 40).
- Кнопка **Обновить** для получения актуальной информации из журнала IP-пакетов.

Просмотр очереди конвертов MFTP

Просмотр очереди конвертов MFTP доступен на вкладке **Очередь конвертов**. Перед просмотром необходимо задать условия отбора конвертов из очереди (Рисунок 46).

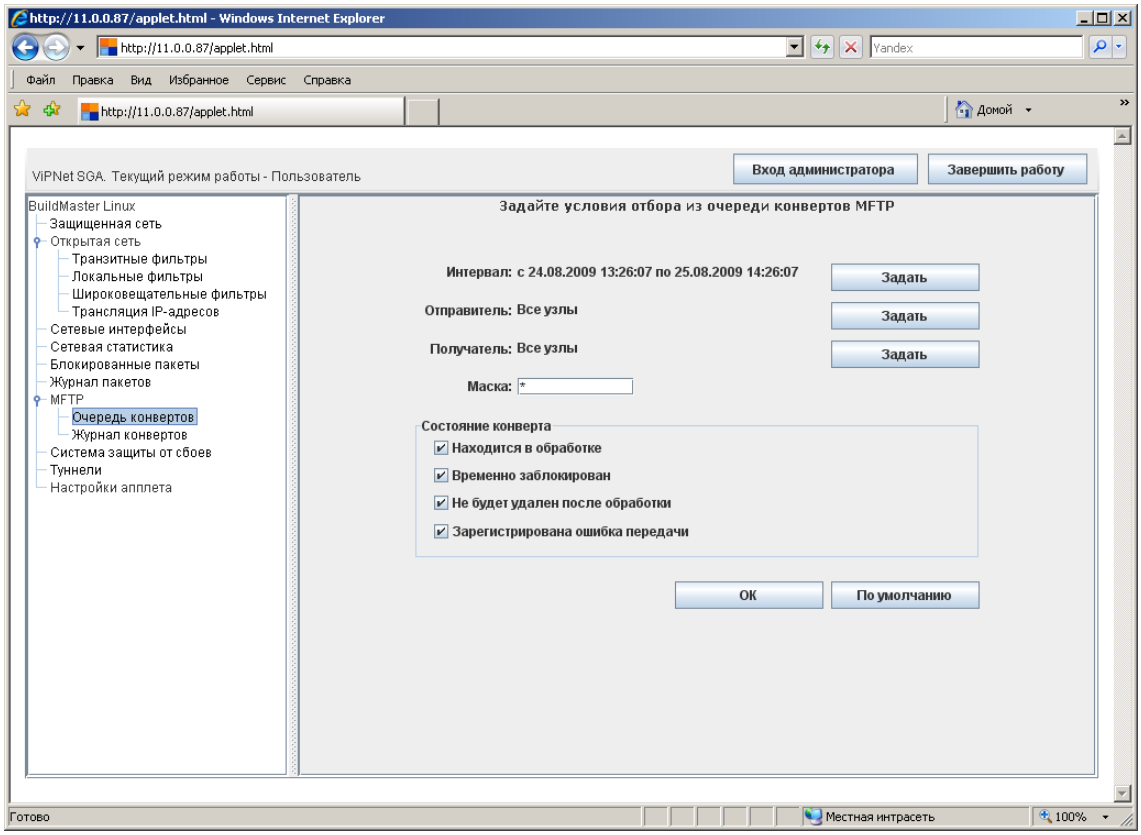

Рисунок 46. Параметры для отбора конвертов MFTP из очереди

Первоначально все параметры, предусмотренные для отбора конвертов, установлены в значения по умолчанию. В этом случае для просмотра будут отобраны все конверты из очереди за последние сутки. Установить значения по умолчанию можно с помощью кнопки **По умолчанию**.

Для отбора конвертов по другим условиям можно задать следующие параметры:

- **Интервал** – выбор временного интервала для просмотра очереди. Значение по умолчанию - за сутки до момента просмотра. Для задания интервала нажмите

кнопку **Задать**. Появится окно, в котором можно задать диапазон дат или последние несколько дней (см. Рисунок 41). Установите переключатель в нужное положение, задайте интервал и нажмите кнопку **OK**.

- **Отправитель** – фильтрация конвертов очереди по отправителю конвертов. Значение по умолчанию - все узлы. Для задания узла нажмите кнопку **Задать**. Появится окно, в котором можно задать все узлы или один узел (см. Рисунок 44). Для выбора конкретного узла установите переключатель в положение **Отдельный узел**, выберите в списке нужный узел и нажмите кнопку **OK**.

  Под списком узлов расположено поле ввода для поиска нужного узла по заданной подстроке. Поиск производится по всем столбцам. С помощью кнопок **Следующее** и **Предыдущее** можно перейти к следующей либо предыдущей записи, содержащей подстроку, указанную в поле поиска.

- **Получатель** – фильтрация конвертов очереди по получателю пакетов. Значение по умолчанию - все узлы. Узел получателя задается так же, как узел отправителя.

- **Маска** – фильтрация конвертов очереди по маске имени файла конверта. Значение по умолчанию - *****, что означает все конверты. Можно задать конкретное имя файла или только часть имени (с учетом регистра), заменив остальные символы значками ***** или **?**. Например, по маске ***2b3*.*** будут отобраны файлы, имена которых содержат подстроку **2b3**, по маске ***?2b3??.**** будут отобраны файлы, имена которых состоят из 6-ти символов и содержат подстроку **2b3**. При поиске файлов учитывается регистр символов, указанных в маске.

- **Состояние конверта** – фильтрация конвертов очереди по состоянию конверта. По умолчанию для просмотра отбираются конверты, находящиеся в любых состояниях. Для выбора нужных состояний установите или снимите соответствующие флажки:

  - **Находится в обработке** – в данный момент конверт передается либо поставлен в очередь на передачу при уже установленном соединении.
  - **Временно заблокирован** – в данный момент конверт временно заблокирован для обработки с целью резервирования очереди на пассивный сервер кластера горячего резервирования. Это состояние может присутствовать только в случае, если координатор работает в составе кластера горячего резервирования.
  - **Не будет удален после обработки** – входящий конверт не будет удален после обработки, будет произведена его маршрутизация в исходном виде (в случае одноадресного конверта).
  - **Зарегистрирована ошибка передачи** – была зарегистрирована ошибка передачи конверта, конверт временно не обрабатывается. Повторная попытка передачи конверта произойдет через таймаут, указанный в настройках транспортного модуля MFTP.

После задания значений параметров (или их установки в значения по умолчанию) нажмите кнопку **ОК**. Появится список найденных в очереди конвертов (Рисунок 47).

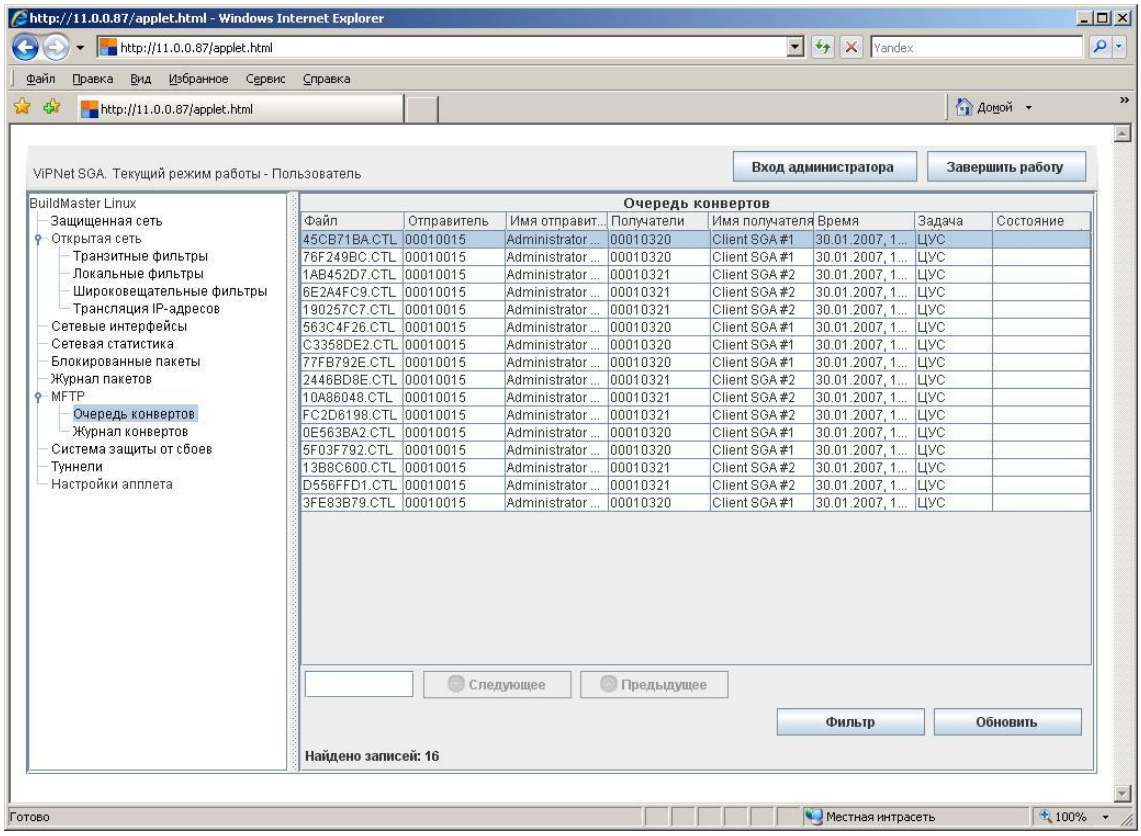

Рисунок 47. Очередь конвертов MFTP

Для каждого конверта выводится следующая информация:

Название столбца	Описание
Файл	Имя файла конверта, находящегося в очереди.
Отправитель	Идентификатор отправителя конверта.
Имя отправителя	Имя отправителя конверта (отображается при наличии связи между отправителем и ViPNet-координатором).
Получатель	Идентификатор получателя конверта.
Имя получателя	Имя получателя конверта (отображается при наличии связи между получателем и ViPNet-координатором).

Название столбца	Описание
Время	Время постановки конверта в очередь.
Задача	Программа ПО ViPNet, из которой отправлен конверт.
Состояние	Состояние конверта.

При просмотре очереди конвертов доступны следующие элементы управления:

- Поле ввода для поиска нужного конверта по заданной подстроке. Поиск производится по всем столбцам.
- Кнопки перехода к следующему (кнопка **Следующее**) либо предыдущему (кнопка **Предыдущее**) конверту, содержащему подстроку, указанную в поле поиска.
- Кнопка **Фильтр** для возврата к заданию условий отбора конвертов из очереди (Рисунок 46).
- Кнопка **Обновить** для получения актуальной информации об очереди конвертов MFTP.

Просмотр журнала конвертов MFTP

Просмотр журнала конвертов MFTP доступен на вкладке **Журнал конвертов**. Перед просмотром необходимо задать условия отбора записей из журнала (Рисунок 48).

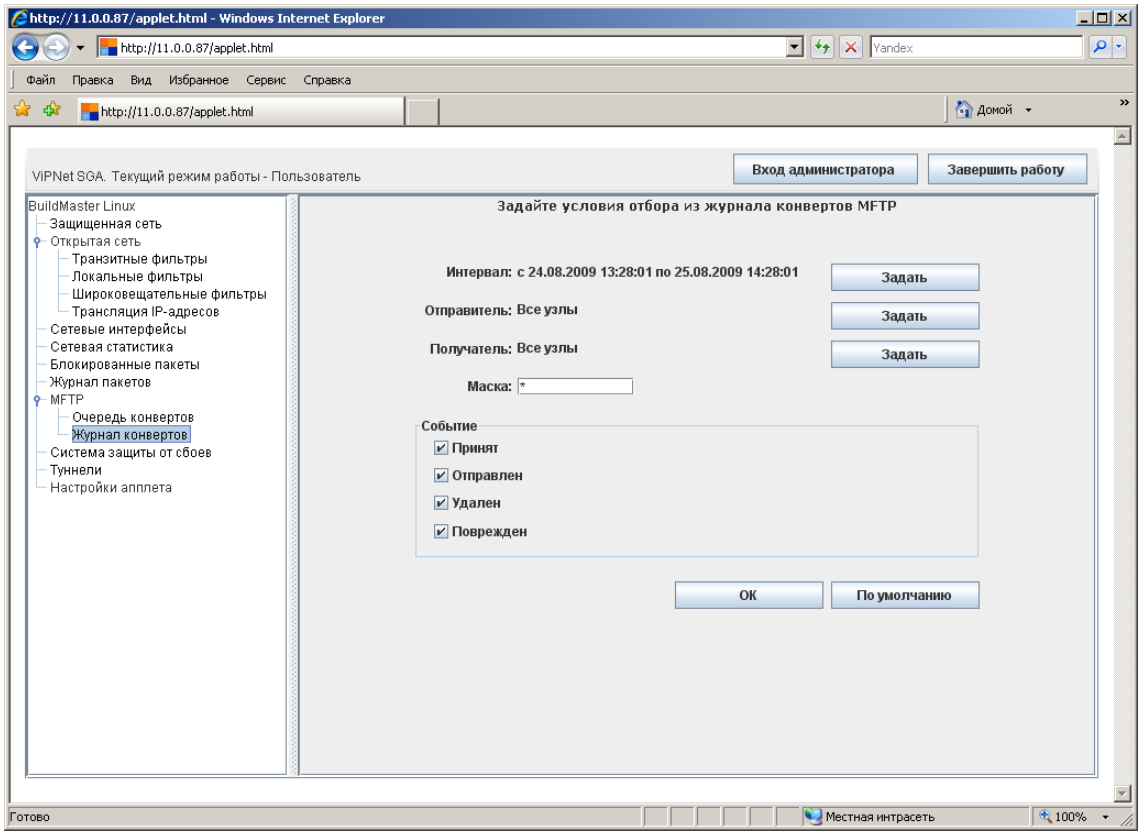

Рисунок 48. Параметры для отбора записей из журнала конвертов MFTP

Первоначально все параметры, предусмотренные для отбора записей, установлены в значения по умолчанию. В этом случае для просмотра будут отобраны все записи журнала за последние сутки.. Установить значения по умолчанию можно с помощью кнопки **По умолчанию**.

Для отбора по другим условиям можно задать следующие параметры:

- **Интервал** – выбор временного интервала для просмотра. Значение по умолчанию - за сутки до момента просмотра. Для задания интервала нажмите кнопку **Задать.**

Появится окно, в котором можно задать диапазон дат или последние несколько дней (см. Рисунок 41). Установите переключатель в нужное положение, задайте интервал и нажмите кнопку **OK**.

- **Отправитель** – фильтрация записей журнала по отправителю конвертов. Значение по умолчанию - все узлы. Для задания узла нажмите кнопку **Задать**. Появится окно, в котором можно задать все узлы или один узел (см. Рисунок 44). Для выбора конкретного узла установите переключатель в положение **Отдельный узел**, выберите в списке нужный узел и нажмите кнопку **OK**.

  Под списком узлов расположено поле ввода для поиска нужного узла по заданной подстроке. Поиск производится по всем столбцам. С помощью кнопок **Следующее** и **Предыдущее** можно перейти к следующей либо предыдущей записи, содержащей подстроку, указанную в поле поиска.

- **Получатель** – фильтрация записей журнала по получателю пакетов. Значение по умолчанию - все узлы. Узел получателя задается так же, как узел отправителя.

- **Маска** – фильтрация записей журнала по маске имени файла конверта. Значение по умолчанию - *****, что означает все конверты. Можно задать конкретное имя файла или только часть имени (с учетом регистра), заменив остальные символы значками ***** или **?**. Например, по маске ***2b3*.*** будут отобраны файлы, имена которых содержат подстроку **2b3**, по маске **?2b3??.*** будут отобраны файлы, имена которых состоят из 6-ти символов и содержат подстроку **2b3**. При поиске файлов учитывается регистр символов, указанных в маске.

- **Событие** – фильтрация записей журнала по событиям, произошедшим с конвертами. По умолчанию для просмотра отбираются записи с любыми событиями. Для выбора нужных событий установите или снимите соответствующие флажки:

  - **Принят** – конверт принят координатором.
  - **Отправлен** – конверт отправлен координатором.
  - **Удален** – конверт удален координатором.
  - **Поврежден** – конверт поврежден.

После задания значений параметров (или их установки в значения по умолчанию) нажмите кнопку **OK**. Появится список найденных в журнале записей (Рисунок 49).

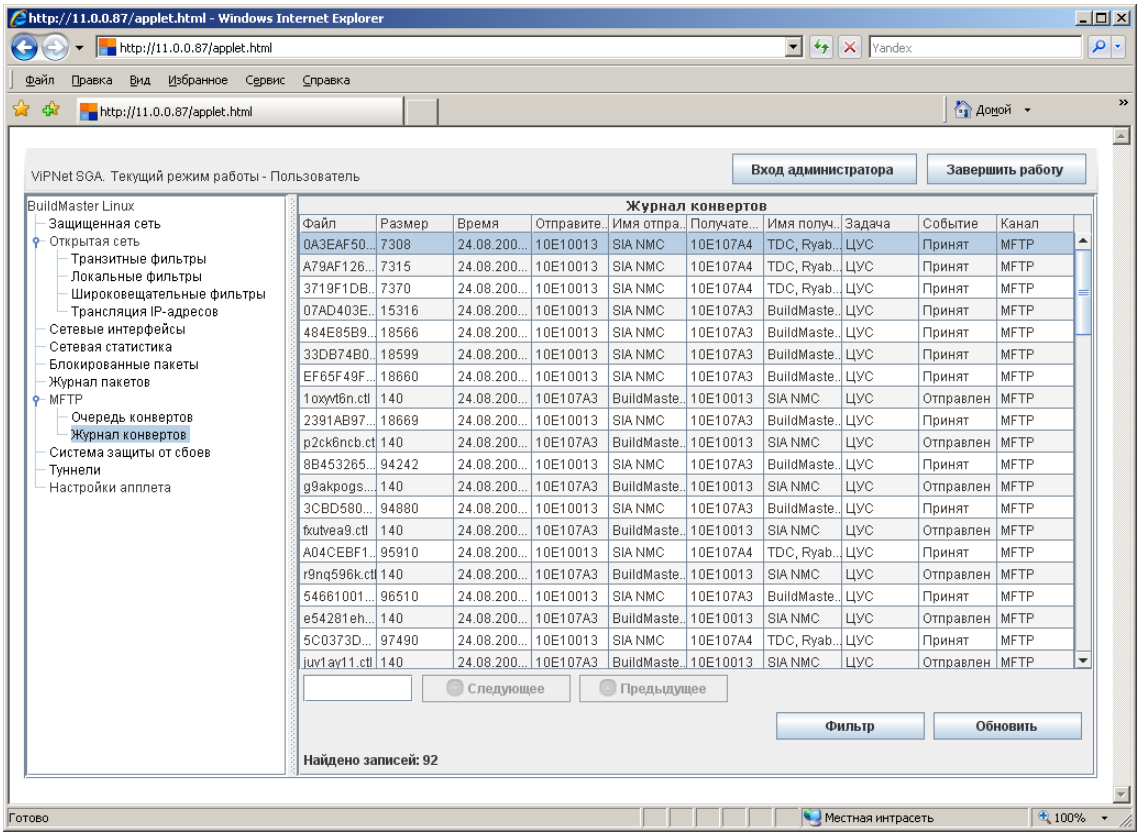

Рисунок 49. Журнал конвертов MFTP

Для каждой записи журнала выводится следующая информация:

Название столбца	Описание
Файл	Имя файла конверта.
Размер	Размер файла конверта.
Время	Время отправки либо получения конверта (в зависимости от типа события).
Отправитель	Идентификатор отправителя.
Имя отправителя	Имя отправителя конверта (отображается при наличии связи между отправителем и ViPNet-координатором).
Получатель	Идентификатор получателя конверта.
Имя получателя	Имя получателя конверта (отображается при наличии

Название столбца	Описание
	связи между получателем и ViPNet-координатором).
Задача	Программа ПО ViPNet, из которой отправлен конверт.
Событие	Событие, зафиксированное в журнале.
Канал	Канал, по которому отправлен либо получен конверт.

При просмотре журнала конвертов MFTP доступны следующие элементы управления:

- Поле ввода для поиска нужной записи по заданной подстроке. Поиск производится по всем столбцам.
- Кнопки перехода к следующей (кнопка **Следующее**) либо предыдущей (кнопка **Предыдущее**) записи, содержащей подстроку, указанную в поле поиска.
- Кнопка **Фильтр** для возврата к заданию условий отбора конвертов (Рисунок 48).
- Кнопка **Обновить** для получения актуальной информации из журнала конвертов MFTP.

Просмотр состояния системы защиты от сбоев

Для обеспечения отказоустойчивости ViPNet-координатор может быть развернут на кластере горячего резервирования, состоящем из двух взаимосвязанных компьютеров (серверов) с установленным на них ПО ViPNet Coordinator Linux. Сервер, на котором в текущий момент функционирует координатор, является активным сервером. Второй сервер находится в режиме ожидания и является пассивным сервером. В случае выхода из строя активного сервера его функции берет на себя второй (пассивный) сервер, который становится при этом активным, а сервер, бывший активным, перезагружается и становится пассивным.

В зависимости от того, используется кластер горячего резервирования или нет, различают два режима работы системы защиты от сбоев – **режим кластера** и **одиночный режим**. Одиночный режим работы означает, что ПО ViPNet Coordinator Linux установлено и функционирует на одном компьютере. Подробное описание принципов работы системы защиты от сбоев и ее режимов см. документ "ViPNet Coordinator Linux. Система защиты от сбоев. Руководство администратора".

Просмотр состояния системы защиты от сбоев доступен на вкладке **Система защиты от сбоев** (Рисунок 50). Режим работы системы (одиночный режим или режим кластера) выводится в верхней части вкладки.

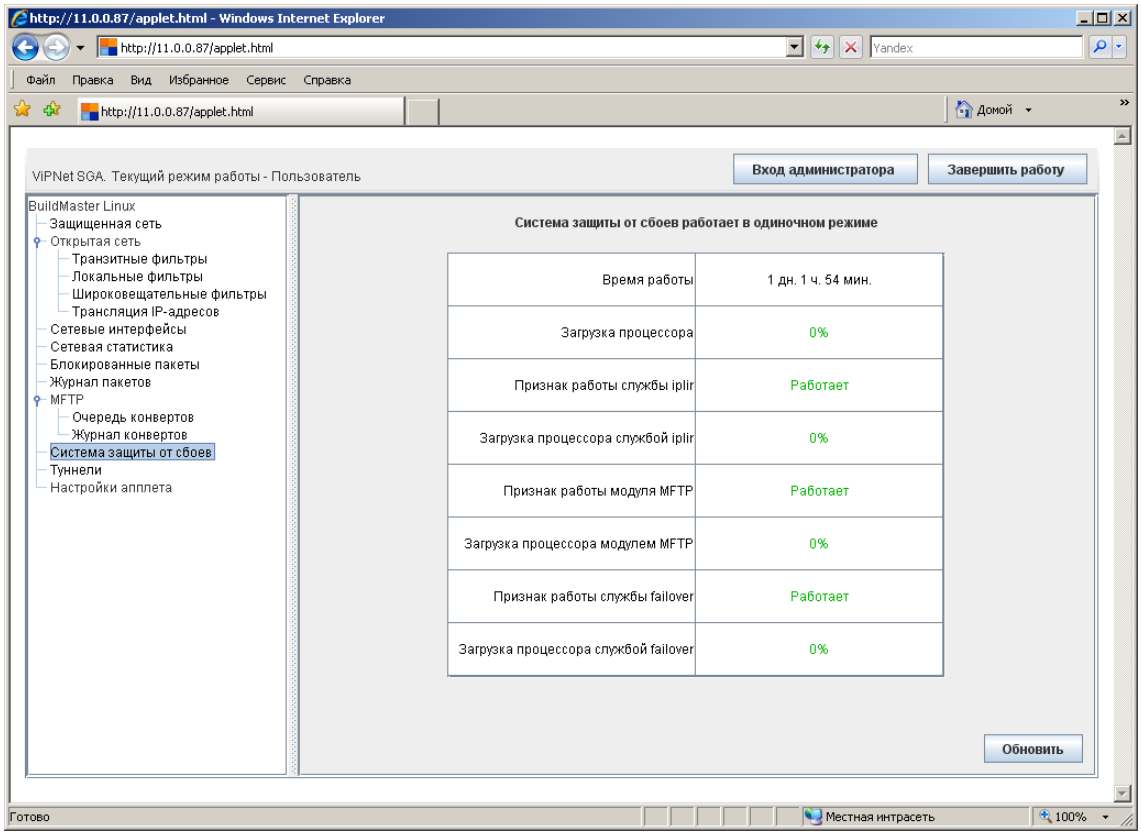

Рисунок 50. Состояние системы защиты от сбоев

Для просмотра доступна следующая информация:

- Время работы системы защиты от сбоев.
- Загрузка процессора (в процентах).
- Признак работы службы iplir (Работает/Не работает/Неизвестно).
- Загрузка процессора службой iplir (в процентах).
- Признак работы модуля MFTP (Работает/Не работает/Неизвестно).
- Загрузка процессора модулем MFTP (в процентах).
- Признак работы службы failover (Работает/Не работает/Неизвестно).
- Загрузка процессора службой failover (в процентах).

Если система защиты от сбоев работает в режиме кластера, то на вкладке **Система защиты от сбоев** выводится информация о состоянии как активного, так и пассивного сервера кластера.

На вкладке **Система защиты от сбоев** находится кнопка **Обновить** для получения актуальной информации о состоянии системы защиты от сбоев.

При работе в режиме администратора на вкладке **Система защиты от сбоев** появится дополнительная кнопка **Перезагрузить сервер** для перезагрузки сервера. Перед началом перезагрузки запрашивается подтверждение (Рисунок 51). Можно отменить перезагрузку, нажав кнопку **Отмена**.

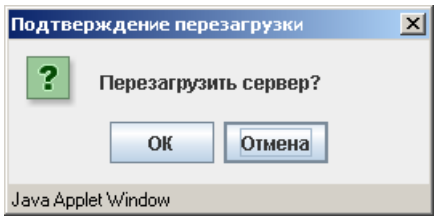

Рисунок 51. Запрос на подтверждение перезагрузки сервера

После подтверждения появится сообщение о начале перезагрузки (Рисунок 52). В этом сообщении нажмите кнопку **ОК**.

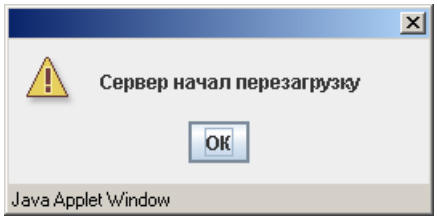

Рисунок 52. Начало перезагрузки сервера

При использовании кластера горячего резервирования может оказаться, что пассивный сервер кластера не готов принять нагрузку. В этом случае появится повторный запрос на подтверждение перезагрузки (Рисунок 53).

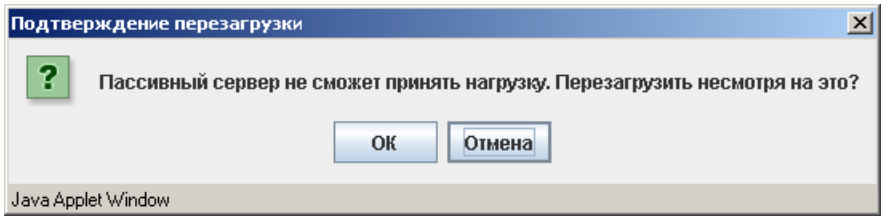

Рисунок 53. Повторный запрос на подтверждение перезагрузки сервера

При перезагрузке сервера апплет закрывает соединение со всеми службами, поэтому после начала перезагрузки появится сообщение об отсутствии соединения (см. Рисунок

5). Нажмите в этом сообщении кнопку **Присоединиться к узлу**, чтобы заново установить соединение со службами.

Просмотр переключений состояний в системе защиты от сбоев

События, происходящие в системе защиты от сбоев при ее работе в режиме кластера, фиксируются в журнале переключений состояний. Просмотр журнала переключений состояний доступен на вкладке **Журнал переключений**. Эта вкладка вложена во вкладку **Система защиты от сбоев** и отображается в дереве на левой панели только в случае, если система защиты от сбоев находится в режиме кластера.

Перед просмотром журнала переключений состояний необходимо задать условия отбора записей из журнала (Рисунок 54).

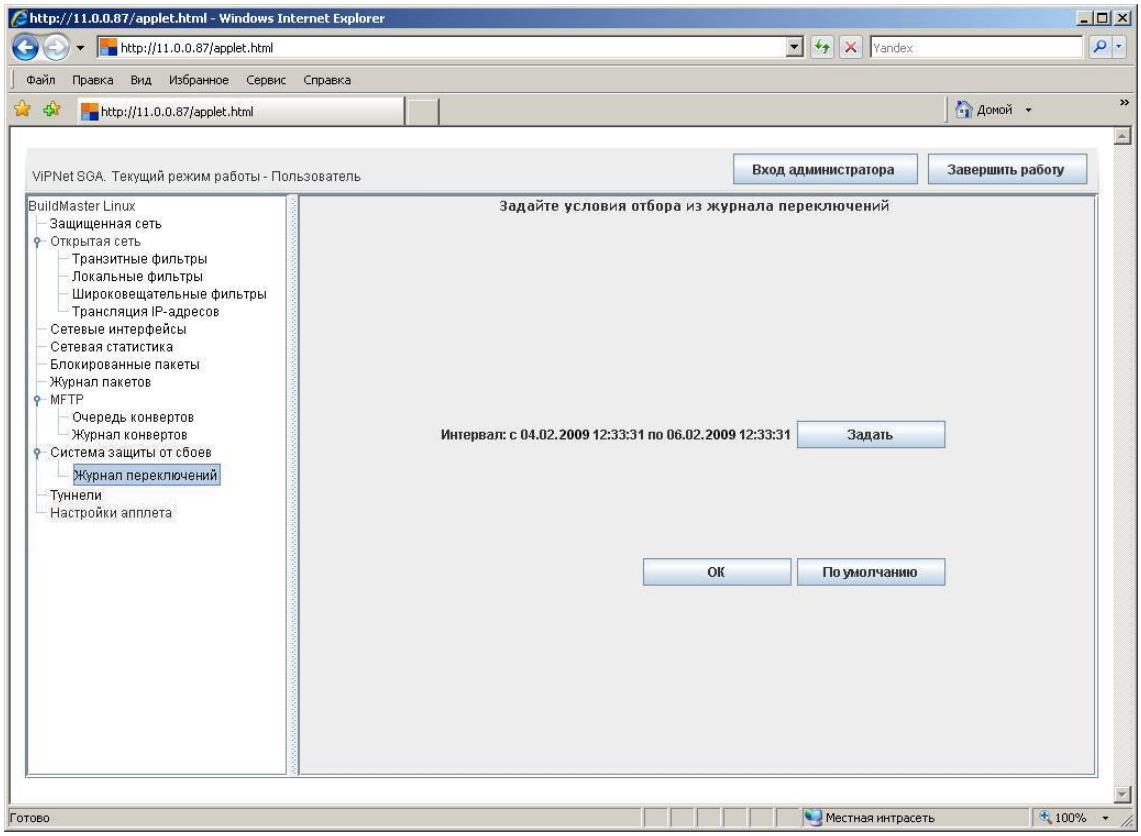

Рисунок 54. Условия отбора записей из журнала переключений состояний

В качестве условия отбора записей задается временной интервал. По умолчанию начало интервала устанавливается за сутки до момента просмотра, конец интервала – спустя

сутки после момента просмотра. Установить значение по умолчанию можно с помощью кнопки **По умолчанию**.

Для отбора записей за другой временной интервал нажмите кнопку **Задать**. Появится окно, в котором можно задать диапазон дат или последние несколько дней (см. Рисунок 41). Установите переключатель в нужное положение, задайте интервал и нажмите кнопку **ОК**.

После задания временного интервала (или его установки в значение по умолчанию) нажмите кнопку **ОК**. Появится список найденных в журнале записей (Рисунок 55).

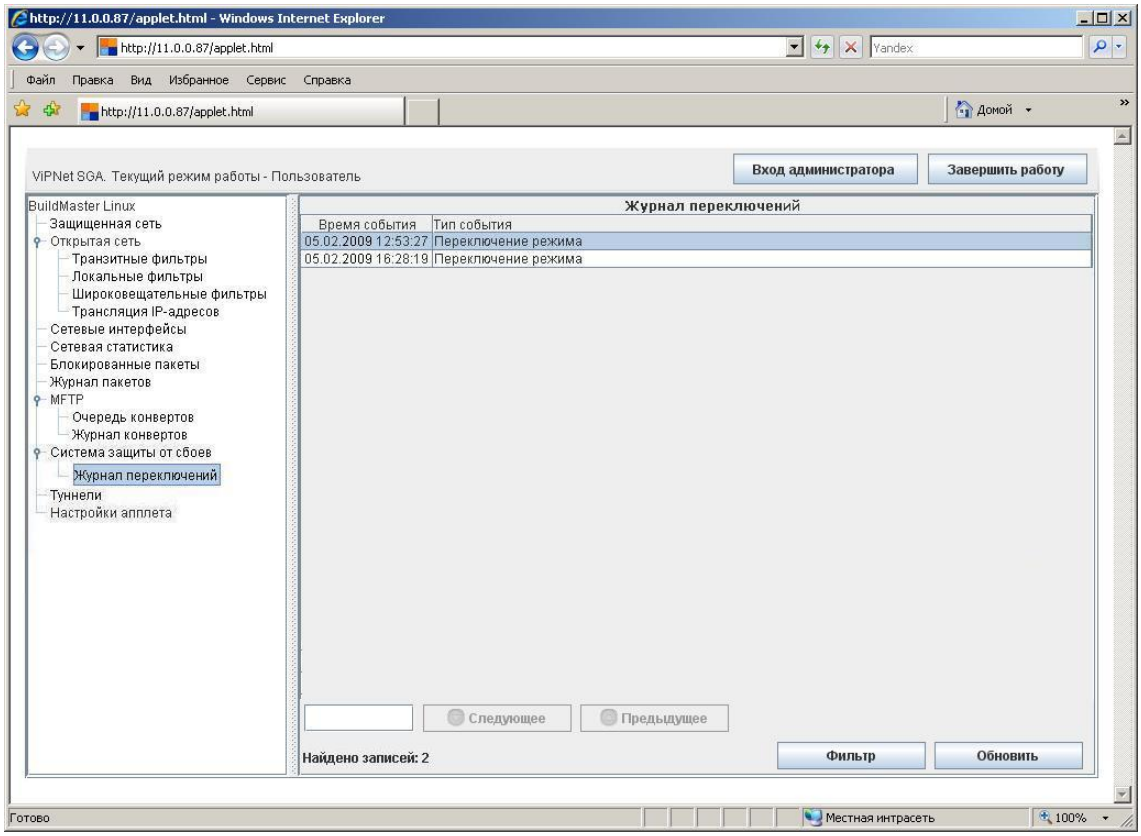

Рисунок 55. Журнал переключений состояний

Записи журнала содержат дату, время и тип событий, произошедших в системе защиты от сбоев в заданном интервале времени.

ViPNet-координатор фиксирует следующие типы событий:

- **Загрузка системы** – старт системы защиты от сбоев при загрузке операционной системы.

- **Переключение режима** – переключение режима сервера из пассивного в активный.
- **Старт в активном режиме** – старт сервера в активном режиме (запуск службы failover вручную в активном режиме).
- **Старт в пассивном режиме** – старт сервера в пассивном режиме (запуск службы failover вручную в пассивном режиме).

Журнал переключений состояний ведется на каждом из серверов кластера. С активного сервера журнал периодически передается на пассивный сервер, заменяя его журнал. При нормальной работе кластера журнал будет содержать только события переключения режима, т.к. события старта сервера в пассивном режиме будут потеряны при получении журнала с активного сервера.

В случае, когда сервер стартует в пассивном режиме, а затем, не получив журнал переключений от активного сервера, сам становится активным, журнал будет содержать события старта в пассивном режиме либо загрузки системы, из чего можно заключить, что второй сервер кластера неработоспособен (завис или отключен).

При просмотре журнала переключений состояний доступны следующие элементы управления:

- Поле ввода для поиска нужной записи по заданной подстроке. Поиск производится по всем столбцам.
- Кнопки перехода к следующей (кнопка **Следующее**) либо предыдущей (кнопка **Предыдущее**) записи, содержащей подстроку, указанную в поле поиска.
- Кнопка **Фильтр** для возврата к заданию условий отбора записей из журнала (Рисунок 54).
- Кнопка **Обновить** для получения актуальной информации из журнала переключений состояний.

Настройка туннелируемых адресов

ViPNet-координатор может выполнять туннелирование (защиту) трафика незащищенных узлов локальной сети (узлов, на которых не установлено ПО ViPNet). Для этого в лицензии должны быть разрешены туннелируемые соединения. Если туннелируемые соединения разрешены, на координаторе задаются IP-адреса, соединения с которыми должны туннелироваться. Максимальное число туннелируемых координатором адресов ограничено имеющейся лицензией.

Настройка туннелируемых адресов выполняется на вкладке **Туннели**. В режиме пользователя доступен только просмотр информации (Рисунок 56).

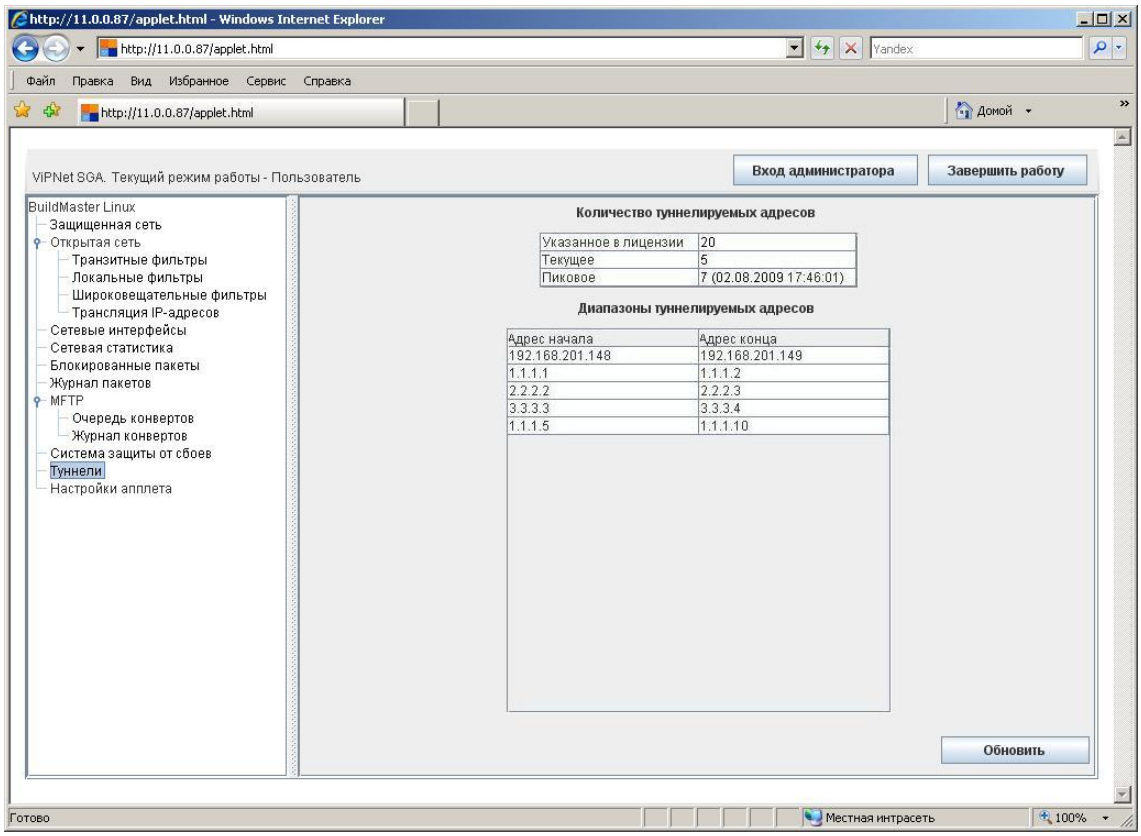

Рисунок 56. Туннели (режим пользователя)

В режиме администратора, помимо просмотра, доступны все действия по настройке туннелируемых адресов (Рисунок 57).

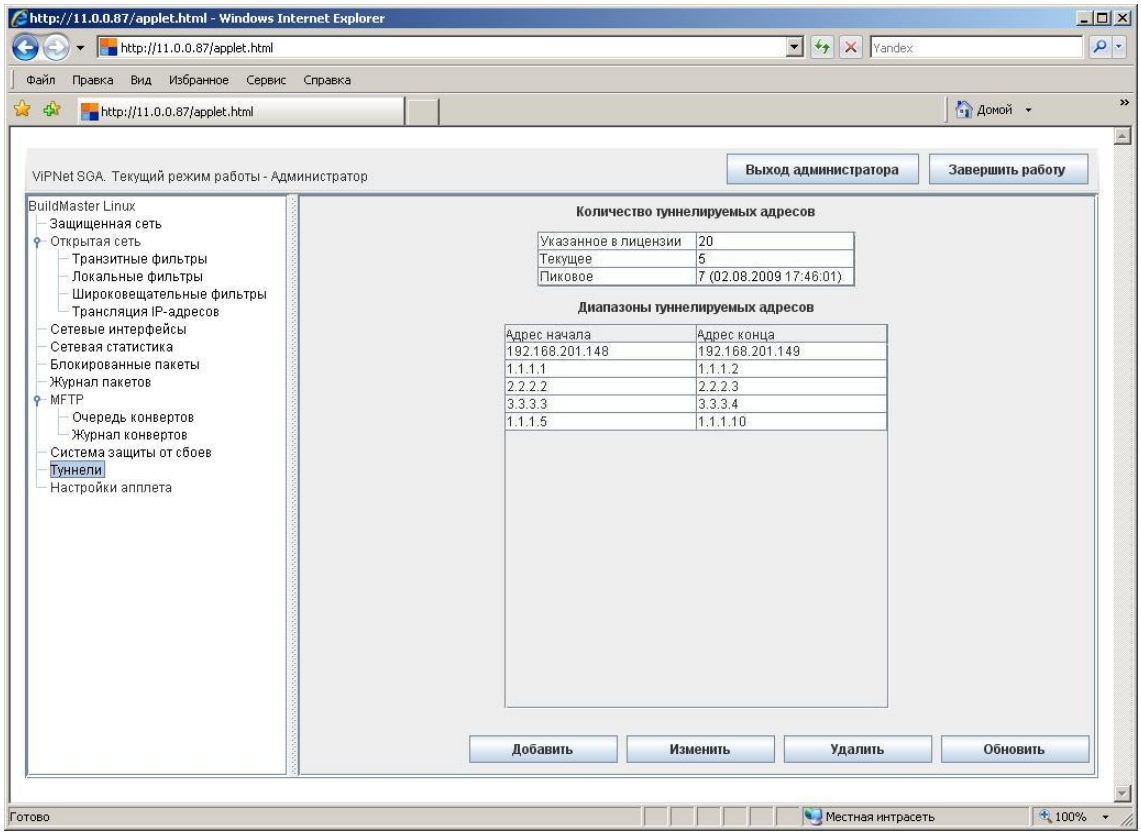

Рисунок 57. Туннели (режим администратора)

В верхней части вкладки **Туннели** выводится информация о количестве туннелируемых адресов:

- **Указанное в лицензии** - количество туннелируемых адресов, указанное в лицензии (максимально допустимое количество туннелируемых адресов).
- **Текущее** - текущее количество туннелируемых адресов.
- **Пиковое** – пиковое (максимальное зарегистрированное) количество туннелируемых адресов с указанием даты и времени его регистрации.

Список **Диапазоны туннелируемых адресов** содержит адрес начала и адрес конца каждого диапазона. В режиме администратора доступны следующие элементы управления диапазонами:

- Кнопка **Добавить** для создания нового диапазона.
- Кнопка **Удалить** для удаления выбранного в списке диапазона.

Перед удалением диапазона появится запрос на подтверждение удаления. Для удаления диапазона нажмите кнопку **ОК**, для отмены удаления – кнопку **Отмена**.

- Кнопка **Изменить** для изменения выбранного в списке диапазона.

Чтобы получить актуальную информацию о количестве и диапазонах туннелируемых адресов, нажмите кнопку **Обновить**. Эта кнопка присутствует на вкладке в любом режиме работы апплета.

Настройки системы автообновления

Система автообновления предназначена для автоматического обновления с заданной периодичностью информации, отображаемой на вкладках апплета. Автообновление применяется для вкладок **Защищенная сеть**, **Система защиты от сбоев**, **Сетевая статистика**, **Сетевые интерфейсы** и аналогично действию кнопки **Обновить** на этих вкладках.

Настройка системы автообновления выполняется на вкладке **Настройки апплета** (Рисунок 58).

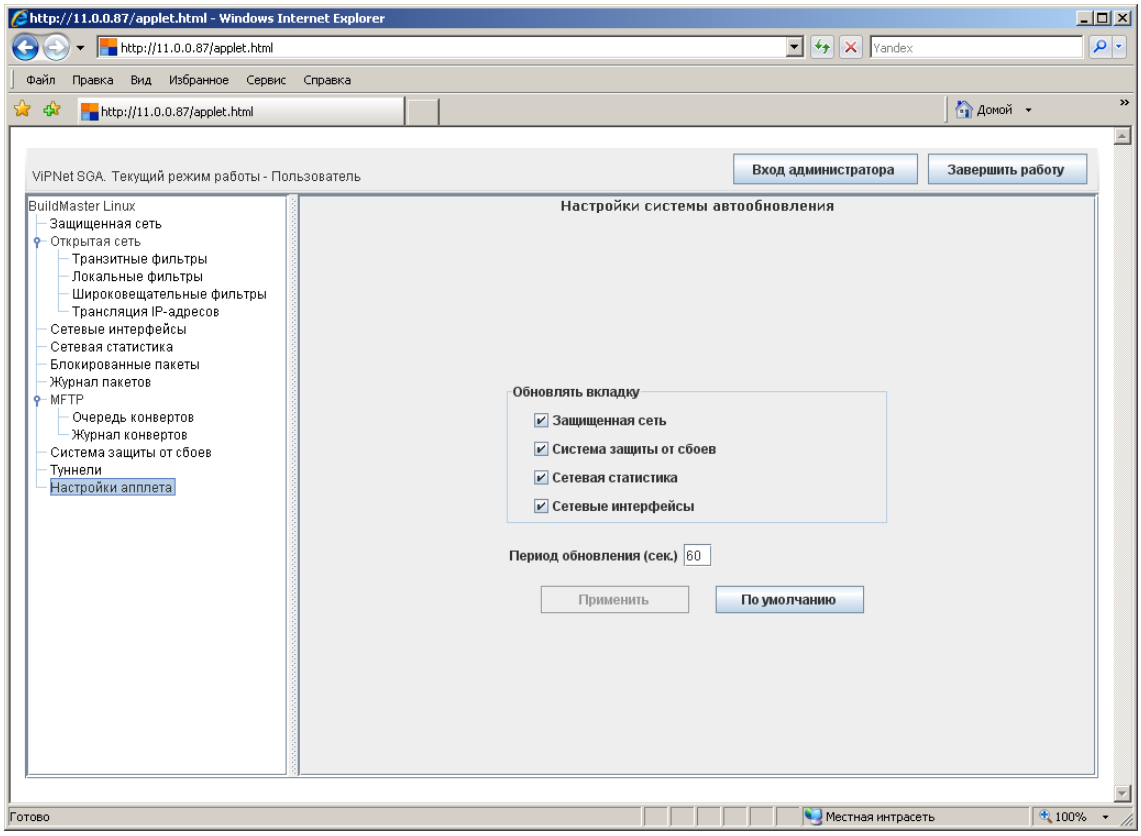

Рисунок 58. Настройки системы автообновления

Настройки системы автообновления содержат следующие параметры:

- Группа флажков **Обновлять вкладку**:

- **Защищенная сеть**
- **Система защиты от сбоев**
- **Сетевая статистика**
- **Сетевые интерфейсы**

Установленные флажки указывают, на каких вкладках следует производить автообновление. По умолчанию все флажки установлены.

Параметры **Защищенная сеть**, **Сетевая статистика** и **Сетевые интерфейсы** недоступны при отсутствии соединения со службой iplir. Параметр **Система защиты от сбоев** недоступен, если нет соединения со службой failover.

- **Период обновления** – периодичность обновления информации (в секундах). Допустимые значения от 10 до 600 секунд, значение по умолчанию 60 секунд. Этот параметр недоступен в случае, когда не установлен ни один из флажков группы **Обновлять вкладку**.

Для настройки системы автообновления установите требуемые значения параметров и нажмите кнопку **Применить**. Эта кнопка доступна только в случае изменения хотя бы одного параметра. После завершения настройки кнопка **Применить** становится недоступной до следующего изменения параметров.

Чтобы восстановить параметры, используемые по умолчанию, нажмите кнопку **По умолчанию**. При старте апплета все параметры установлены в значения по умолчанию: все флажки установлены и период обновления равен 60 секундам.

Приложения

Приложение А. События, отслеживаемые ПО ViPNet Coordinator Linux

События, отслеживаемые ПО ViPNet Coordinator Linux, разделены на группы и подгруппы (Рисунок 59).

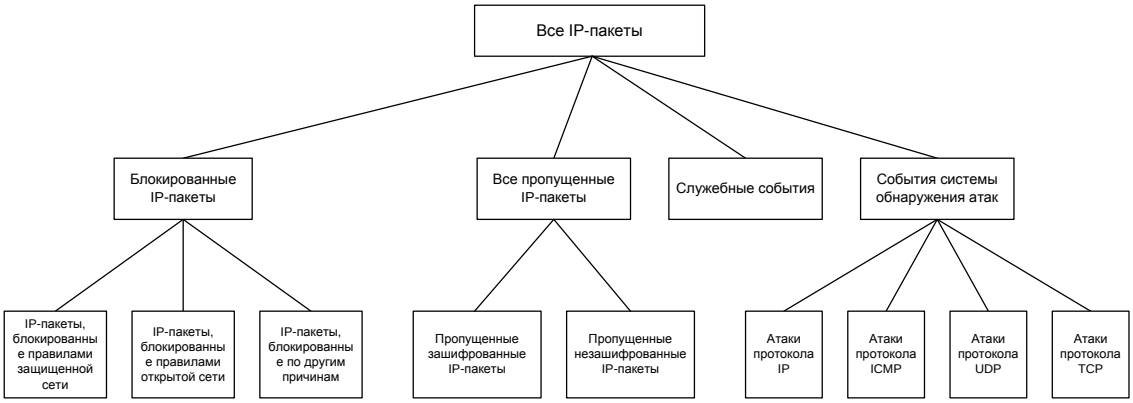

Рисунок 59. Иерархия групп и подгрупп событий

Таблицы Таблица 1 – Таблица 10 содержат списки событий, относящихся к разным группам и подгруппам.

Таблица 1. События подгруппы ***Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные правилами защищенной сети***

Номер события	Название события	Описание события
1	Не найден ключ для сетевого узла	Не найден ключ для связи с пользователем, идентификатор которого указан в пакете
2	Неверное значение имито	Защищаемые данные или открытая информация криптосистемы были изменены

Номер события	Название события	Описание события
3	IP-пакет блокирован фильтром защищенной сети	Согласно настройкам фильтров, входящий зашифрованный или предназначенный для шифрования исходящий открытый пакет был заблокирован
4	Слишком большая разница во времени	Пакет был отправлен раньше или позже даты, установленной на принимающем узле, на величину большую, чем указано в настройке допустимого времени приема пакетов.
5	Некорректная версия драйвера	Принят пакет, созданный несовместимой с текущей версией драйвера
6	Размер заголовка зашифрованного IP-пакета меньше минимально допустимого	Длина части пакета, необходимой для расшифрования, слишком мала для того, чтобы в ней могла быть размещена информация криптосистемы
7	Неизвестный метод шифрования	Не поддерживается метод шифрования, код которого указан во входящем пакете
8	Искаженный IP-пакет	Недопустимые параметры в расшифрованном пакете
9	Неизвестный идентификатор сетевого узла	Идентификатор отправителя в пакете неизвестен
10	IP-пакет блокирован главным фильтром защищенной сети	Пакет блокирован фильтром, относящимся к записи “IP-пакеты всех адресатов”
11	Сессия была неактивной слишком долго	Это событие не используется
12	Не найден MAC-адрес сетевого узла	Пакет не может быть перенаправлен получателю, т.к. тот не сообщил адрес своего сетевого адаптера серверу
13	Превышено время жизни IP-пакета	Пакет уничтожен из-за превышения лимита его нахождения в сети
14	Получен IP-пакет для другого сетевого узла	Принят пакет для другого адресата

Номер события	Название события	Описание события
15	Слишком много фрагментов для IP-пакета	Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов
16	Исчерпана лицензия на количество туннелируемых адресов	На ViPNet-координатор, осуществляющий туннелирование, одновременно пришли пакеты от компьютеров, число которых превышает число прописанных в лицензии туннелей
17	Неверный IP-адрес	В пришедшем зашифрованном пакете Ethernet свой, а IP-адрес чужой, и при этом пакет не является маршрутизируемым (событие 45)
18	Неизвестный IP-адрес получателя	Событие появляется в случае, если координатор не знает, на какой адрес перенаправить входящий пакет
19	Обнаружен конфликт адресов сетевых узлов	Это событие не используется
70	Транзитный IP-пакет блокирован фильтром защищенной сети	Транзитный зашифрованный IP-пакет заблокирован на координаторе фильтром защищенной сети

Таблица 2. События подгруппы ***Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные правилами открытой сети***

Номер события	Название события	Описание события
22	Незашифрованный IP-пакет от сетевого узла	От защищенного адресата пришел открытый пакет
23	Незашифрованный широковещательный IP-пакет от сетевого узла	От защищенного адресата пришел открытый широковещательный пакет
30	Локальный IP-пакет блокирован фильтром открытой сети	Найдено запрещающее правило фильтрации открытой сети в группе локальных правил

Номер события	Название события	Описание события
31	Транзитный IP-пакет блокирован фильтром открытой сети	Найдено запрещающее правило фильтрации открытой сети в группе транзитных правил
32	Широковещательный IP-пакет блокирован фильтром открытой сети	Найдено запрещающее правило фильтрации открытой сети в группе широковещательных правил
33	IP-пакет блокирован фильтром антиспуфинга	Найдено соответствующее правило в таблице антиспуфинга
34	Неподдерживаемый тип ICMP-сообщения	Получен ICMP-пакет, тип которого отличен от типа 8, кода 0
35	Превышено максимальное число защищаемых адресов	В течение заданного периода времени были получены пакеты от большего количества адресов, чем задано в лицензии
36	Передача пакета между двумя внешними интерфейсами запрещена	Это событие не используется

Таблица 3. События подгруппы ***Все IP-пакеты/Блокированные IP-пакеты/IP-пакеты, блокированные по другим причинам***

Номер события	Название события	Описание события
80	Размер IP-пакета меньше допустимого	Размер IP-пакета меньше минимально возможного
81	Недопустимая версия протокола IP	В данной версии поддерживается только протокол IP версии 4
82	Недопустимая длина заголовка IP	Длина заголовка протокола IP меньше минимально возможного
83	Недопустимая длина IP-пакета	Длина пакета меньше, чем указано в заголовке протокола IP
84	Несовпадение контрольной суммы IP	Подсчитанное значение контрольной суммы заголовка IP-пакета не совпадает со значением, указанным в пакете

Номер события	Название события	Описание события
85	Размер заголовка TCP меньше минимально допустимого	Недопустимо короткий заголовок протокола TCP
86	Размер заголовка UDP меньше минимально допустимого	Недопустимо короткий заголовок протокола UDP
87	Дефрагментация IP-пакета была отменена	Были обработаны не все фрагменты, образующие пакет
88	Широковещательный адрес отправителя IP-пакета	Адрес отправителя в пакете указан широковещательный
89	Фрагменты IP-пакета пересекаются между собой	Наиболее старый из пересекающихся фрагментов был отброшен
90	Недостаточно ресурсов для обработки IP-фрагмента	Пакет не может быть обработан из-за недостаточности свободных ресурсов. Если эта ошибка стабильно проявляется, то требуется обновление версии драйвера, использующего больше машинных ресурсов, или требуется более совершенная модель компьютера
91	IP-пакет получен во время инициализации драйвера	Блокировка всех пакетов во время инициализации драйвера
92	Слишком большой размер IP-пакета	Размер пакета ограничен размером 48 Кбайт
93	Превышено время сборки фрагментов IP-пакета	За допустимое время получены не все фрагменты IP-пакета
94	Недостаточно памяти	Для выполнения какой-либо операции требуется выделение памяти, но выделить память не удалось
95	Обнаружен сетевой узел с таким же идентификатором	Поступили пакеты с одинаковыми идентификаторами СУ, но разными IP-адресами
97	IP-пакет блокирован фильтром SQL	Соединение заблокировано Microsoft SQL фильтром

Номер события	Название события	Описание события
98	Недостаточно ресурсов для обработки IP-пакета	Для обработки IP-пакета требуется выделение ресурсов, но выделить ресурсы не удалось
100	Недопустимые флаги TCP	Это событие не используется
101	Не найден маршрут для транзитного IP-пакета	Не найдено правило для транзитного пакета в таблице маршрутов
102	Модуль прикладной обработки не загружен	Не загружен соответствующий модуль прикладной обработки
103	Превышено максимальное количество соединений	Количество уже установленных соединений превышает максимально допустимое, заданное в настройках координатора
104	Соединение уже существует	Для создаваемого соединения параметры исходящих пакетов (socketpair) совпадают с уже существующими, такое соединение блокируется
105	Не удалось выделить динамический порт для правила трансляции адресов	Не удалось выделить порт для динамической трансляции адресов (например, все порты в пуле закончились)

Таблица 4. События группы ***Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные зашифрованные IP-пакеты***

Номер события	Название события	Описание события
40	Пропущен зашифрованный IP-пакет	Разрешенный зашифрованный пакет
41	Пропущен зашифрованный широковещательный IP-пакет	Разрешенный зашифрованный широковещательный пакет
43	IP-пакет был перенаправлен другому сетевому узлу	Пакет перенаправлен на другой узел на том же самом интерфейсе

Номер события	Название события	Описание события
44	Осуществлена маршрутизация зашифрованного транзитного IP-пакета с изменением его адреса	Пакет направлен на другой узел путем подмены в нем адреса получателя
45	Осуществлена маршрутизация зашифрованного транзитного IP-пакета	Пакет пропущен, т.к. предназначен для другого компьютера

*Таблица 5. События группы **Все IP-пакеты/Все пропущенные IP-пакеты/Пропущенные незашифрованные IP-пакеты***

Номер события	Название события	Описание события
60	Пропущен незашифрованный локальный IP-пакет	Найдено разрешающее правило фильтрации открытой сети в группе локальных правил
61	Пропущен незашифрованный широковещательный IP-пакет	Найдено разрешающее правило фильтрации открытой сети в группе широковещательных правил
62	Пропущен незашифрованный транзитный IP-пакет	Найдено разрешающее правило фильтрации открытой сети в группе транзитных правил

*Таблица 6. События группы **Все IP-пакеты/Служебные события***

Номер события	Название события	Описание события
42	Изменился адрес сетевого узла	Драйвер обнаружил, что IP-адрес сетевого узла изменился и соответствующим образом скорректировал свои таблицы
46	Изменился адрес доступа к сетевому узлу	Событие предназначено для диагностики настройки правил NAT на межсетевых экранах, через которые работают другие узлы. Это событие может появиться, если данный узел не установлен в режим работы через ViPNet-координатор Событие формируется об узлах,

Номер события	Название события	Описание события
		установленных в режим работы через межсетевой экран (МЭ), в том случае, если на МЭ изменился адрес или порт доступа к этим узлам со стороны данного узла
47	Истек тайм-аут	Технологический код Формируется на узле в режиме **С динамической трансляцией адресов** при появлении инициативного трафика от удаленного узла, прошедшего через координатор узла в режиме **С динамической трансляцией адресов**
48	Адрес сетевого узла зарегистрирован из широковещательного пакета	Технологический код Формируется для удаленного узла, если этот узел становится доступным или перестает быть доступным по широковещательным пакетам

*Таблица 7. События подгруппы **Все IP-пакеты/События системы обнаружения атак/Атаки протокола IP***

Номер события	Название события	Описание события
1001	Атака Land	Попытка злоумышленника замедлить работу данного сетевого узла Атака использует уязвимость стека TCP/IP, заключающуюся в том, что путем передачи фальшивого TCP-пакета можно заставить атакуемый компьютер попытаться установить соединение самому с собой, путем отправки SYN-пакета с адресом отправителя, идентичным адресу атакуемого компьютера
1002	IP-опции нулевой длины	Попытка злоумышленника вывести из строя внешний сетевой экран путем посылки пакета с IP-опциями нулевой длины

Номер события	Название события	Описание события
1003	Пустой IP-фрагмент	Обнаружен пустой IP-фрагмент
1020	Атака Jolt2	Обнаружен пакет с некорректным смещением фрагмента, соответствующим атаке Jolt2 Атака заключается в посылке в течение короткого промежутка времени большого числа специально сформированных пакетов с целью замедлить атакуемую систему

*Таблица 8. События подгруппы **Все IP-пакеты/События системы обнаружения атак/Атаки протокола ICMP***

Номер события	Название события	Описание события
1101	Возможная атака Smurf	Обнаружен ICMP-запрос, отправленный на адрес подсети (x.x.x.0 или x.x.x.255) Такой запрос способен инициировать множественные эхо-ответы, которые могут перегрузить сеть или атакуемую систему
1104	ICMP-запрос маски подсети	Обнаружен запрос на получение значения маски подсети Такая информация может помочь хакеру собрать данные о конфигурации сети
1106	Фрагментация ICMP-заголовка	ICMP-заголовок был разбит на несколько фрагментов в попытке обойти сетевые экраны или системы обнаружения вторжений

*Таблица 9. События подгруппы **Все IP-пакеты/События системы обнаружения атак/Атаки протокола UDP***

Номер события	Название события	Описание события

Номер события	Название события	Описание события
1203	Урезанный UDP-заголовок	Обнаружен UDP-пакет с аномально коротким заголовком
1204	Возможная атака Fraggle	Обнаружен UDP-пакет, отправленный на адрес подсети (x.x.x.0 или x.x.x.255) и предназначенный для одного из "отражающих" портов Такой пакет способен инициировать множество ответов, которые могут перегрузить сеть или атакуемую систему
1205	Зацикливание портов UDP	Обнаружен UDP-пакет, зацикленный между двумя "отражающими" портами Такие пакеты могут отражаться бесконечное число раз, перегружая сеть и ресурсы вовлеченных систем
1206	Атака Snork	Попытка вызова отказа в обслуживании

Таблица 10. События подгруппы ***Все IP-пакеты/События системы обнаружения атак/Атаки протокола TCP***

Номер события	Название события	Описание события
1302	Фрагментация TCP-заголовка	TCP-заголовок был разбит на несколько фрагментов в попытке обойти сетевые экраны или системы обнаружения вторжений
1303	Урезанный TCP-заголовок	Обнаружен TCP-пакет с аномально коротким TCP-заголовком
1304	Неправильное смещение Urgent в TCP-заголовке	Множество таких пакетов могут вызвать "зависание" у некоторых реализаций TCP/IP
1305	Атака WinNuke	Попытка привести операционную систему к перезагрузке Атака использует ошибку реализации стека

Номер события	Название события	Описание события
		TCP/IP при посылке пакета Out of Band
1306	TCP-опции нулевой длины	Попытка злоумышленника вывести из строя внешний сетевой экран с помощью посылки пакета с TCP-опциями нулевой длины
1307	Сканирование TCP XMAS	Обнаружен TCP-пакет с установленными битами FIN, URG и PUSH Злоумышленник пытается определить наличие доступных служб в системе, посылая такие специально сформированные пакеты
1308	Сканирование TCP null	Обнаружен TCP-пакет со всеми сброшенными управляющими битами Злоумышленник пытается определить наличие доступных служб в системе, посылая такие специально сформированные пакеты

Приложение Б. Возможные неполадки при работе с апплетом и способы их устранения

В данном приложении приведены возможные неполадки при работе с апплетом и способы их устранения.

Не удается отобразить в Интернет-браузере стартовую страницу для запуска апплета

Описание:

- При попытке отобразить стартовую страницу для запуска апплета Интернет-браузер сообщает, что данная страница не найдена или сервер не найден.

Проверьте:

- Устанавливается ли связь между ViPNet-клиентом и сервером посредством проверки соединения из программы ViPNet Client [Монитор] или с помощью команды ping. Если соединение отсутствует (ICMP-ответы не приходят), проверьте правильность задания связи между узлами в ViPNet ЦУС, а также корректность настроек на обоих сетевых узлах.
- В случае обращения по DNS-имени, корректно ли осуществляется преобразование DNS-имени сервера в IP-адрес, а также совпадает ли выдаваемый DNS-сервером IP-адрес с текущим адресом видимости узла. Если нет, то необходимо правильно настроить службу DNS..
- Имеет ли web-сервер права на чтение всех файлов, необходимых для работы апплета, а также права на исполнение для всех вложенных каталогов. При необходимости измените права.

Сообщение "Соединение с данным сервером не разрешено"

Описание:

- При попытке запустить апплет выдается сообщение об отсутствии разрешения на мониторинг и управление ViPNet-координатором.

Причина:

- ViPNet-клиент, установленный на данном компьютере, не зарегистрирован в прикладной задаче "Клиент SGA". Необходимо зарегистрировать ViPNet-клиент в указанной задаче с помощью ViPNet ЦУС.
- ViPNet-клиент, установленный на данном компьютере, зарегистрирован в прикладной задаче "Клиент SGA", однако доступ к мониторингу и управлению запрещен этому узлу настройками, заданными в файле конфигурации **sga.conf**. Необходимо локально на сервере изменить настройки в файле **sga.conf**. Подробнее о настройке доступа ViPNet-клиентов к удаленному мониторингу и управлению см. документ "Апплет мониторинга и управления ViPNet-координатором. Руководство администратора".

Сообщение "Отсутствует соединение со всеми службами"

Описание:

- При попытке запустить апплет выдается сообщение об отсутствии соединения со всеми службами.

Причина:

- Службы ПО ViPNet не запущены на сервере. Необходимо локально на сервере проверить состояние служб и при необходимости запустить их.

Сообщение "Сессия администратора уже установлена"

Описание:

- При попытке перейти в режим администратора выдается сообщение, что сессия администратора уже установлена, и апплет остается в режиме пользователя.

Причина:

- В случае одновременной работы с апплетом на нескольких узлах на одном из них уже установлен режим администратора. При необходимости выйдите из режима администратора на том узле, где он установлен.