ViPNet Personal Firewall

Руководство администратора

infotecs

ФРКЕ.00220-01 32 01

Версия продукта 4.5

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: https://infotecs.ru/

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение **5**
О документе 6
Для кого предназначен документ 6
Соглашения документа 6
О программе 7
Системные требования 8
Комплект поставки 9
Обратная связь 10

Глава 1. Общие сведения **11**
Основные возможности 12
Разграничение полномочий на основе ролей 13
Лицензирование 15

Глава 2. Установка и начало работы с программой ViPNet Personal Firewall **16**
Последовательность действий 17
Установка и обновление программы 18
Установка в ОС Windows 18
Установка в ОС на базе ядра Linux 19
Запуск и завершение работы с программой 20
Интерфейс программы 22
Смена пользователя 24
Установка лицензии 26
Активация лицензии 27

Глава 3. Настройка параметров сетевого экрана **29**
Общие сведения о правилах фильтрации трафика 30
Управление режимами работы 35
Управление справочниками 36
Протоколы 40
Адреса и сети 43
Расписание 45
Управление сетевыми фильтрами 47
Запрет входящих соединений на указанные порты 52
Централизованное обновление настроек сетевых фильтров 54

Выгрузка настроек в файл 54
Загрузка настроек из файла 55
Автоматическое обновление настроек из файла 55

Глава 4. Мониторинг событий 57
Отслеживание и блокировка активных соединений 58
Просмотр журнала регистрации трафика и создание сетевых фильтров на основе событий журнала 60
Самотестирование 63
Аудит 65
Просмотр журнала аудита 65
Настройка срока хранения и параметров ротации записей журнала аудита 67

Глава 5. Управление и настройка ViPNet Personal Firewall 68
Настройка блокировки трафика при отключении защитного функционала антивируса 69
Управление учетными записями пользователей 70
Обновление лицензии 73

Приложение А. Глоссарий 74

Введение

О документе 6

О программе 7

Обратная связь 10

О документе

Для кого предназначен документ

Документ предназначен для администраторов программного комплекса (далее — программы) ViPNet Personal Firewall. В руководстве содержится информация, необходимая для установки, настройки и использования программы ViPNet Personal Firewall.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

О программе

Современный мир невозможно представить без многочисленных компьютерных сетей (в том числе — Интернета), которые объединяют пользователей из различных организаций и всех уголков мира. При этом компьютер каждого пользователя подвержен разного рода опасностям: доступ нежелательных лиц, распространение компьютерных вирусов и так далее.

Чтобы обеспечить безопасность компьютера, пользователь может установить на него программу ViPNet Personal Firewall (далее — ViPNet Personal Firewall). ViPNet Personal Firewall является персональным сетевым экраном (см. глоссарий, стр. 75) и выполняет функции контроля и фильтрации трафика, проходящего через компьютер пользователя (см. Общие сведения о правилах фильтрации трафика на стр. 30).

Контроль сетевой активности приложений позволяет обнаруживать все активные сетевые соединения на компьютере пользователя. Пользователь видит список активных соединений и может разрешить или запретить нужные соединения.

Фильтрация трафика производится в соответствии с режимом работы программы и сетевыми фильтрами, предустановленными программой или заданными пользователем. Выбор режима позволяет настроить определенный уровень защиты компьютера, начиная с полной блокировки доступа к компьютеру (и компьютера к сетевым ресурсам) и заканчивая полным разрешением доступа. Сетевые фильтры позволяют задать более тонкие настройки доступа по определенным адресам, портам и протоколам. Для HTTP-трафика могут быть созданы сетевые фильтры прикладного уровня, позволяющие осуществлять фильтрацию сетевых ресурсов, путем запрета определенных команд HTTP-протокола и передачи мобильного кода в виде файлов HTTP-протокола следующих типов: JavaScript, PDF, Flash. Под мобильным кодом подразумевается контент, который выполняется на компьютере пользователя при использовании сетевого ресурса.

В результате будет обеспечена надежная защита пользовательского компьютера в сети.

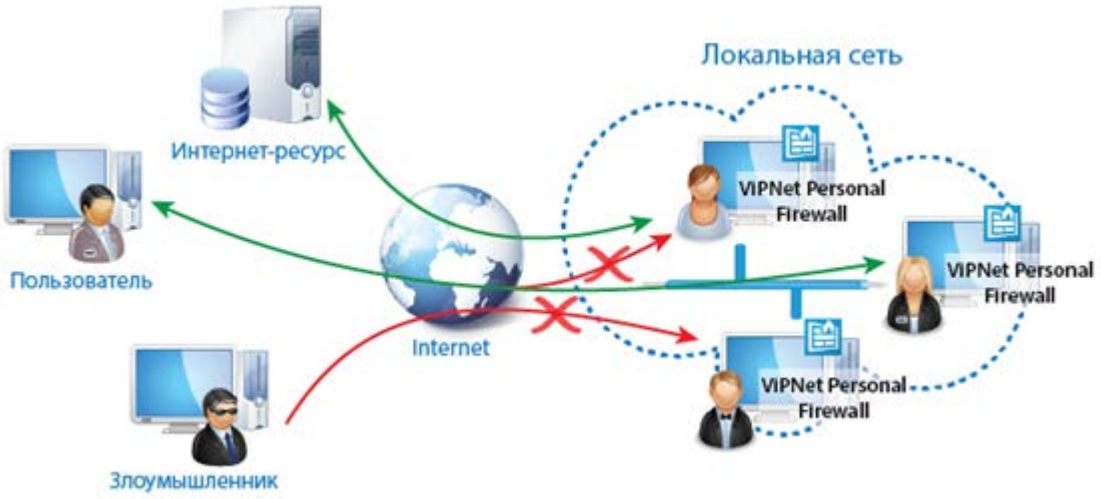

Рисунок 1. Защита компьютеров пользователей с помощью ViPNet Personal Firewall

ViPNet Personal Firewall обеспечивает нейтрализацию следующих угроз безопасности информации:

- несанкционированного доступа к информации, содержащейся на компьютере пользователя;
- DoS-атак;
- несанкционированной передачи информации;
- несанкционированного воздействия на программу ViPNet Personal Firewall, целью которого является нарушение ее функционирования и безопасности компьютера пользователя.

Системные требования

Требования к компьютеру для установки программы ViPNet Personal Firewall:

- Процессор — Intel Core 2 Quad или другой схожий по производительности x86-совместимый процессор с количеством ядер 4 и более.
- Объем оперативной памяти — не менее 4 Гбайт.
- Свободное место на жестком диске — не менее 100 Гбайт.
- Операционная система (далее — ОС):
    - Windows Server 2008 R2 Standard (64-разрядная);
    - Windows Server 2008 R2 Enterprise (64-разрядная);
    - Windows 7 Professional (32/64-разрядная);
    - Windows 7 Enterprise (32/64-разрядная);
    - Windows 8.1 Professional (32/64-разрядная);
    - Windows 8.1 Enterprise (32/64-разрядная);
    - Windows Server 2012 Standard (64-разрядная);
    - Windows Server 2012 R2 Standard (64-разрядная);
    - Windows Server 2012 R2 Datacenter (64-разрядная);
    - Windows 10 (32/64-разрядная) версия 1709 и ниже.
    - Windows Server 2016 (64-разрядная);
    - Astra Linux Special Edition 1.5 (релиз «Смоленск»);
    - Альт Линукс СПТ 7.0 Рабочая станция (64-разрядная);
    - Debian 8.7 (64-разрядная).

  Для ОС должен быть установлен самый последний пакет обновлений.

Комплект поставки

В комплект поставки программы ViPNet Personal Firewall входят:

- Установочные файлы программы ViPNet Personal Firewall для установки в ОС Windows и в ОС на базе ядра Linux.
- Установочный файл программы ViPNet IDS HS Агент Linux — AgentSetup.deb;
- Документ «ViPNet Personal Firewall. Руководство администратора» в формате PDF.

Обратная связь

Дополнительная информация

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

- Информация о продуктах ViPNet https://infotecs.ru/product/.
- Информация о решениях ViPNet https://infotecs.ru/resheniya/.
- Часто задаваемые вопросы https://infotecs.ru/support/faq/.
- Форум пользователей продуктов ViPNet https://infotecs.ru/forum/.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт https://infotecs.ru/support/request/.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

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

1

Общие сведения

Основные возможности 12

Разграничение полномочий на основе ролей 13

Лицензирование 15

Основные возможности

Программа ViPNet Personal Firewall обладает следующими возможностями:

- Выбор определенного уровня защиты компьютера с помощью режимов работы (см. Управление режимами работы на стр. 35). Блокировка всего проходящего IP-трафика в случае необходимости.
- Обеспечение защиты компьютера сразу после выбора режима.
- Гибкая настройка фильтрации трафика по множеству параметров (см. Общие сведения о правилах фильтрации трафика на стр. 30).
- Обеспечение контроля сетевой активности приложений (см. Отслеживание и блокировка активных соединений на стр. 58).
- Ведение следующих журналов:
  - Журнал регистрации IP-трафика (см. Просмотр журнала регистрации трафика и создание сетевых фильтров на основе событий журнала на стр. 60).
  - Журнал сетевой активности приложений (см. Отслеживание и блокировка активных соединений на стр. 58).
  - Журнал аудита (событий по изменению настроек безопасности в программе) (см. Аудит на стр. 65).
- Разграничение полномочий пользователей на основе ролей (см. Разграничение полномочий на основе ролей на стр. 13).
- Управление учетными записями пользователей (на стр. 70).
- Централизованное обновление настроек сетевых фильтров (на стр. 54).
- Настройка блокировки трафика при отключении защитного функционала антивируса (на стр. 69). Настройка совместима только с антивирусом Kaspersky Endpoint Security 10.
- Контроль работоспособности программы (см. Самотестирование на стр. 63).

Разграничение полномочий на основе ролей

Управление ViPNet Personal Firewall реализовано с помощью ролевой модели доступа. Роль определяет полномочия пользователя и задается при создании соответствующей учетной записи.

В ViPNet Personal Firewall существуют следующие роли:

- Администратор. Обладает максимальными полномочиями. Доступны все действия.
- Пользователь. Имеет доступ только к изменению режимов работы программы.
- Аудитор. Управляет журналом аудита.

Учетная запись первого администратора создается при установке программы ViPNet Personal Firewall (см. Установка и обновление программы на стр. 18). Остальные учетные записи создаются администратором в программе ViPNet Personal Firewall (см. Управление учетными записями пользователей на стр. 70).

Список действий, которые доступны для каждой роли, приведен в таблице ниже.

Таблица 3. Доступные действия для ролей администратор (Адм), пользователь (Польз) и аудитор (Ауд)

Действие	Адм	Польз	Ауд	Ссылка
Изменение режимов работы	+	+	+	Управление режимами работы (на стр. 35)
Создание и просмотр сетевых фильтров	+	-	+	Общие сведения о правилах фильтрации трафика (на стр. 30) Управление сетевыми фильтрами (на стр. 47)
Управление справочниками	+	-	-	Управление справочниками (на стр. 36)
Обновление настроек сетевых фильтров из файла	+	-	-	Централизованное обновление настроек сетевых фильтров (на стр. 54)
Отслеживание активных соединений	+	-	+	Отслеживание и блокировка активных соединений (на стр. 58)
Просмотр журнала регистрации трафика	+	-	+	Просмотр журнала регистрации трафика и создание сетевых фильтров на основе событий журнала (на стр. 60)
Запуск самотестирования	+	-	-	Самотестирование (на стр. 63)
Управление журналом аудита	+	-	+	Аудит (на стр. 65)
Управление учетными записями	+	-	-	Управление учетными записями пользователей (на стр. 70)
Настройка блокировки трафика при отключении антивируса	+	-	-	Настройка блокировки трафика при отключении защитного функционала антивируса (на стр. 69)
Загрузка и активация лицензий	+	-	-	Установка лицензии (на стр. 26) Активация лицензии (на стр. 27)

Лицензирование

Лицензия дает вам право на легальное использование программы ViPNet Personal Firewall и подтверждает, что программа поддерживается производителем.

После установки ViPNet Personal Firewall необходимо установить и активировать лицензию (см. Установка лицензии на стр. 26). Для приобретения лицензии обратитесь в отдел продаж ОАО "ИнфоТеКС".

Внимание! Без установленной и активированной лицензии программа ViPNet Personal Firewall неработоспособна.

Лицензия может быть бессрочной или иметь срок действия. Лицензия содержит ограничение на версию программы ViPNet Personal Firewall, до которой возможно обновление.

По истечении срока действия лицензии ее необходимо обновить.

В процессе работы вы можете просмотреть информацию об установленной лицензии, а также при необходимости установить новую лицензию (см. Обновление лицензии на стр. 73).

2

Установка и начало работы с программой ViPNet Personal Firewall

Последовательность действий 17

Установка и обновление программы 18

Запуск и завершение работы с программой 20

Установка лицензии 26

Активация лицензии 27

Последовательность действий

Чтобы начать использование ViPNet Personal Firewall, выполните все действия из приведенного ниже списка:

Таблица 4. Порядок действий для подготовки ViPNet Personal Firewall к работе:

	Действие	Ссылка
☐	Установите программу ViPNet Personal Firewall на компьютер	Установка и обновление программы (на стр. 18)
☐	Запустите консоль управления программой	Запуск и завершение работы с программой (на стр. 20)
☐	Установите лицензию	Установка лицензии (на стр. 26)
☐	Активируйте лицензию	Активация лицензии (на стр. 27)
☐	Выберите режим работы программы для задания уровня безопасности вашего компьютера	Управление режимами работы (на стр. 35)
☐	При необходимости настройте сетевые фильтры для контроля трафика, который отправляет и принимает компьютер, по определенным параметрам	Управление сетевыми фильтрами (на стр. 47)

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

Установка и обновление программы

Перед установкой ViPNet Personal Firewall убедитесь, что на компьютере выполнены сетевые настройки и правильно заданы часовой пояс, дата и время.

Вы можете установить ViPNet Personal Firewall на компьютер с ОС Windows (см. Установка в ОС Windows на стр. 18) или с ОС на базе ядра Linux (см. Установка в ОС на базе ядра Linux на стр. 19).

Установка в ОС Windows

Для установки ViPNet Personal Firewall на компьютер с ОС Windows вам потребуется установочный EXE-файл программы и файл с лицензией.

Для установки ViPNet Personal Firewall выполните следующие действия:

1. Запустите установочный EXE-файл  .
2. Ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок.
3. Нажмите кнопку **Установить**. Запустится процесс подготовки к установке программы.
4. Следуйте указаниям мастера установки.
5. На странице **Настройка** задайте имя и пароль учетной записи администратора ViPNet Personal Firewall (см. Разграничение полномочий на основе ролей на стр. 13) в соответствии с требованиями безопасности вашей организации. По умолчанию будет использоваться имя учетной записи и пароль администратора — `admin`.

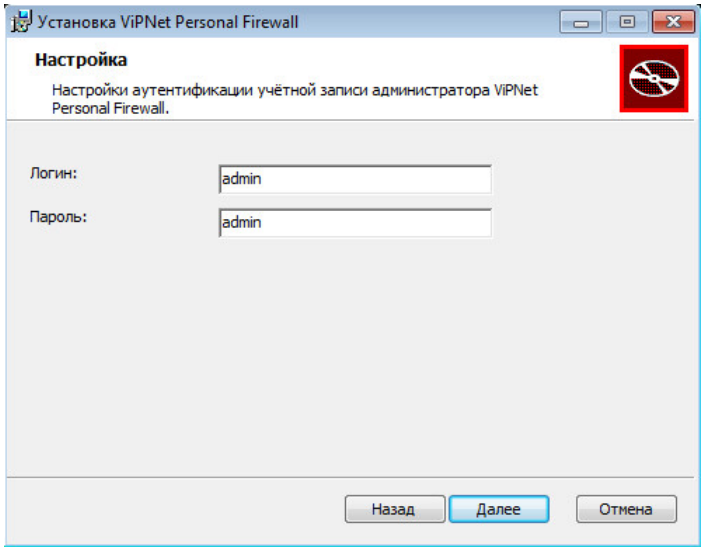

Рисунок 2. Настройка учетной записи администратора

6 Нажмите кнопку **Далее** и следуйте указаниям мастера установки.

В результате программа ViPNet Personal Firewall будет установлена на ваш компьютер и запущена. Теперь вы можете установить и активировать лицензию (см. Установка лицензии на стр. 26).

Установка в ОС на базе ядра Linux

Для установки ViPNet Personal Firewall на компьютер с ОС на базе ядра Linux (далее — ViPNet Personal Firewall Linux) вам потребуется установочный DEB-пакет (для установки в ОС Debian и Astra Linux), RPM-пакет (для установки в ОС Альт Линукс) и файл с лицензией.

Перед установкой ViPNet Personal Firewall установите программу ViPNet IDS HS Агент Linux (см. документ "ViPNet IDS HS. Руководство администратора"), входящую в комплект поставки, и перезагрузите компьютер .

Для установки ViPNet Personal Firewall в зависимости от типа ОС выполните следующие действия:

- При установке на компьютер с ОС Debian и Astra Linux запустите команду:

  `sudo dpkg -i /абсолютный путь к DEB-пакету`

- При установке на компьютер с ОС Альт Линукс запустите команду:

  `rpm -i /абсолютный путь к RPM-пакету`

  Дождитесь окончания установки и перезагрузите компьютер.

Программа ViPNet Personal Firewall будет установлена на ваш компьютер.

Запуск и завершение работы с программой

Программа ViPNet Personal Firewall запускается автоматически после установки и при загрузке ОС. Чтобы запустить консоль управления программой:

1 Выполните одно из действий:

- Если вы используете ОС Windows 7, Windows 10 или Windows Server 2008 R2, в меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Personal Firewall Console** > **ViPNet Personal Firewall Console**.
- Если вы используете ОС Windows 8.1, Windows Server 2012 или более поздней версии, на начальном экране откройте список приложений и выберите **ViPNet** > **ViPNet Personal Firewall Console**.
- Дважды щелкните ярлык программы  на рабочем столе.

  Откроется окно входа в программу.

2 Введите имя пользователя и пароль вашей учетной записи. При первом входе в консоль управления введите имя и пароль учетной записи администратора, заданные при установке программы (см. Установка и обновление программы на стр. 18).

3 Чтобы при последующем запуске программы не вводить пароль учетной записи, установите флажок **Запомнить меня**.

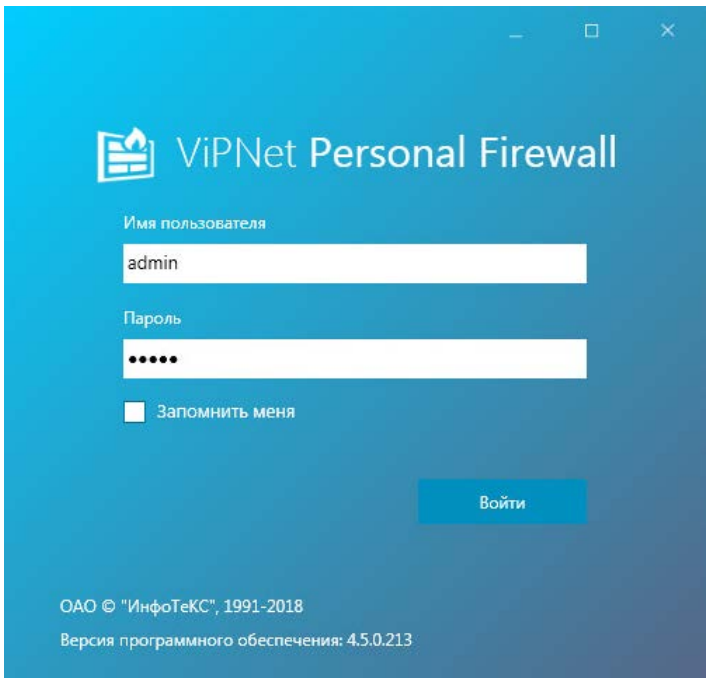

Рисунок 3. Вход в программу ViPNet Personal Firewall

4 Нажмите кнопку **Войти**.

Внимание! Если вы три раза подряд введете неверные данные для входа в программу, ваша учетная запись будет заблокирована на три минуты.

Откроется окно консоли управления программой с простыми настройками (**Режим работы**). В области уведомлений на панели задач появится значок программы (соответствует изображению установленного режима работы (см. Управление режимами работы на стр. 35)).

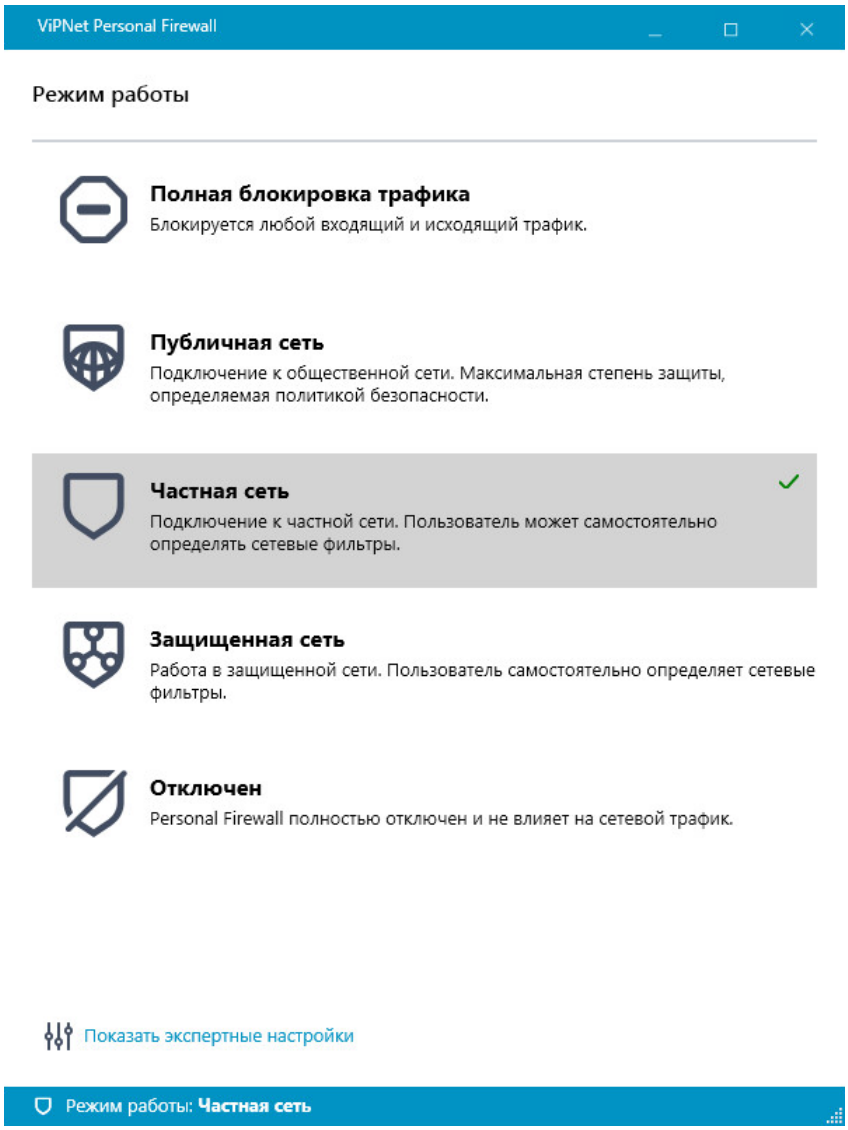

Рисунок 4. Простые настройки ViPNet Personal Firewall

Примечание. Для доступа к остальным настройкам ViPNet Personal Firewall (см. Интерфейс программы на стр. 22) в нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**. Если вы вошли в консоль управления с правами пользователя, то экспертные настройки будут недоступны.

Чтобы свернуть окно консоли управления ViPNet Personal Firewall в область уведомлений, нажмите кнопку **Закрыть**. Чтобы вновь открыть окно консоли управления, в области уведомлений в контекстном меню программы выберите пункт **Открыть ViPNet Personal Firewall** или два раза щелкните значок программы.

Чтобы завершить работу с консолью управления ViPNet Personal Firewall, правой кнопкой мыши щелкните значок программы в области уведомлений и в контекстном меню выберите пункт **Выход**.

Интерфейс программы

На рисунке ниже представлен интерфейс консоли управления программы ViPNet Personal Firewall, установленной на компьютер с ОС Windows (см. Установка в ОС Windows на стр. 18), после отображения экспертных настроек (см. Запуск и завершение работы с программой на стр. 20).

Внимание! Интерфейс и возможности консоли управления ViPNet Personal Firewall Linux могут отличаться от представленных в документе. Важные различия отмечены по ходу описания сценариев использования программы.

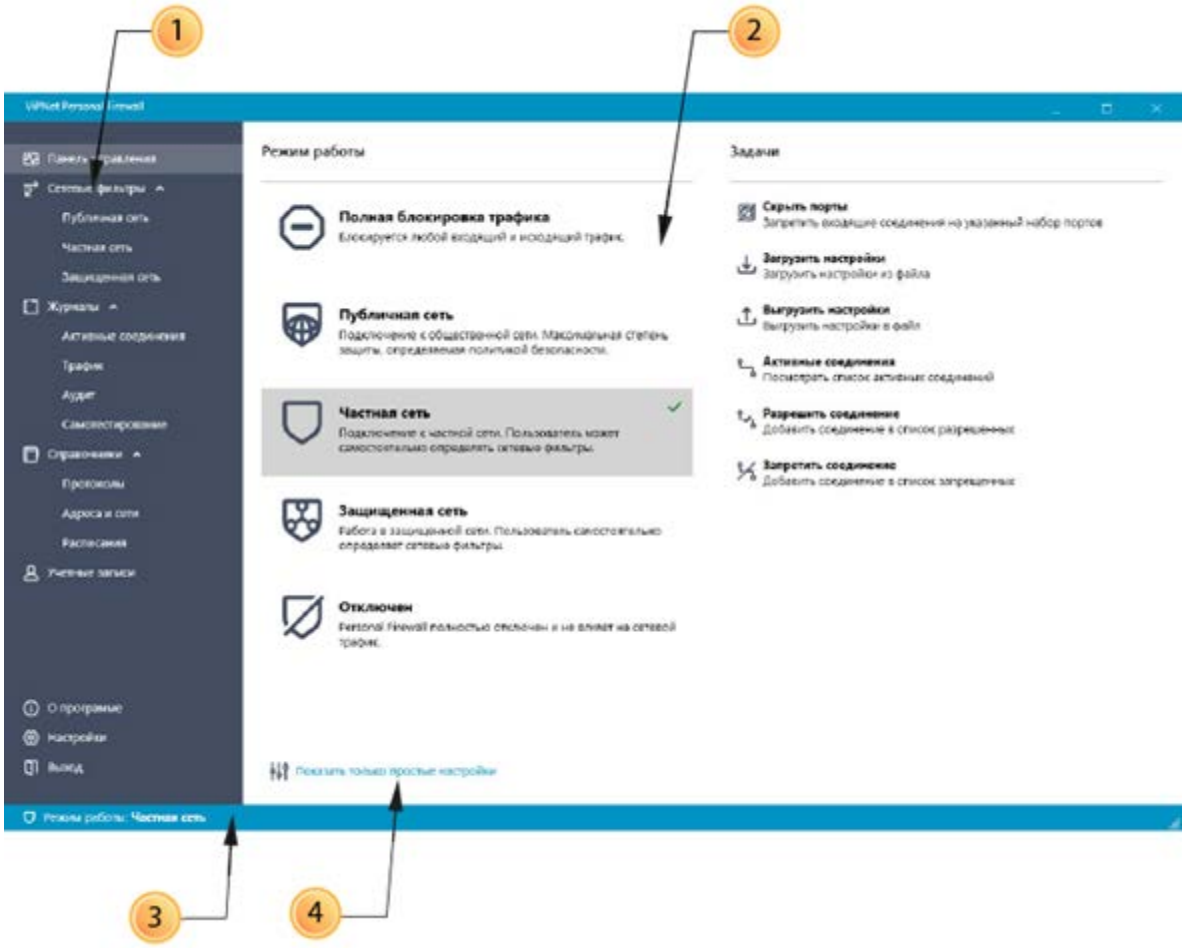

Рисунок 5. Интерфейс консоли управления ViPNet Personal Firewall (экспертные настройки)

Цифрами на рисунке обозначены:

1 Панель навигации — содержит набор разделов для настройки ViPNet Personal Firewall и просмотра результатов работы:

- **Панель управления** — предназначен для переключения режимов работы (см. Управление режимами работы на стр. 35) и решения следующих задач:
  - **Скрыть порты** — настройка запрета входящих соединений на указанные порты (см. Запрет входящих соединений на указанные порты на стр. 52).
  - **Загрузить настройки** — загрузка настроек сетевых фильтров из файла (см. Загрузка настроек из файла на стр. 55).
  - **Выгрузить настройки** — выгрузка настроек сетевых фильтров в файл (см. Выгрузка настроек в файл на стр. 54).
  - **Активные соединения** — просмотр списка активных соединений (см. Отслеживание и блокировка активных соединений на стр. 58).
  - **Разрешить соединение** — создание разрешающего сетевого фильтра (см. Управление сетевыми фильтрами на стр. 47).
  - **Запретить соединение** — создание запрещающего сетевого фильтра (см. Управление сетевыми фильтрами на стр. 47).
- **Сетевые фильтры** (см. Общие сведения о правилах фильтрации трафика на стр. 30) — предназначен для настройки и просмотра сетевых фильтров для следующих режимов работы (см. Управление сетевыми фильтрами на стр. 47):
  - **Публичная сеть** — сетевые фильтры для режима работы **Публичная сеть** (только просмотр фильтров).
  - **Частная сеть** — сетевые фильтры для режима работы **Частная сеть**.
  - **Защищенная сеть** — сетевые фильтры для режима работы **Защищенная сеть**.
- **Журналы** — содержит следующие подразделы:
  - **Активные соединения** — предназначен для просмотра активных в настоящий момент соединений и их блокировки (см. Отслеживание и блокировка активных соединений на стр. 58).
  - **Трафик** — предназначен для просмотра журнала регистрации трафика и создания сетевых фильтров на основе событий журнала (см. Просмотр журнала регистрации трафика и создание сетевых фильтров на основе событий журнала на стр. 60).
  - **Аудит** — предназначен для просмотра журнала аудита (см. Аудит на стр. 65).
  - **Самотестирование** — предназначен для запуска самотестирования и просмотра отчетов о выполненных проверках (см. Самотестирование на стр. 63).
- **Справочники** — содержит подразделы со списками объектов, которые могут быть использованы при создании сетевых фильтров (см. Управление справочниками на стр. 36):
  - **Протоколы** — управление справочниками протоколов и их параметрами (см. Протоколы на стр. 40).

- **Адреса и сети** — управление справочниками адресов (см. Адреса и сети на стр. 43).
- **Расписания** — управление справочниками расписаний действия фильтров (см. Расписание на стр. 45).

o **Учетные записи** — предназначен для управления учетными записями пользователей (см. Управление учетными записями пользователей на стр. 70).

o **О программе** — предназначен для установки (см. Установка лицензии на стр. 26) и активации лицензии (см. Активация лицензии на стр. 27) и просмотра информации о продукте и установленной лицензии.

o **Настройки** — предназначен для выполнения следующих действий:

- Настройка автоматического обновления сетевых фильтров из файла (см. Автоматическое обновление настроек из файла на стр. 55).
- Настройка срока хранения и параметров ротации записей журнала аудита (на стр. 67).
- Настройка периода автоматического запуска самотестирования (см. Самотестирование на стр. 63).
- Настройка блокировки трафика при отключении защитного функционала антивируса (на стр. 69).

o **Выход** — завершение работы с консолью управления ViPNet Personal Firewall (см. Запуск и завершение работы с программой на стр. 20).

2 Панель просмотра — страница отображает содержимое раздела, выбранного на панели навигации (1).

3 Нижняя панель — содержит информацию о текущем режиме работы (см. Общие сведения о правилах фильтрации трафика на стр. 30).

4 Кнопка переключения между простыми (доступно только изменение режима) и экспертными настройками (доступны все настройки в соответствии с ролью пользователя (см. Разграничение полномочий на основе ролей на стр. 13)).

Смена пользователя

Если в ViPNet Personal Firewall задано несколько учетных записей пользователей с разными ролями, вы можете сменить пользователя, не перезапуская программу. Для этого выполните следующие действия:

1 Откройте экспертные настройки, если они еще не открыты. Для этого в нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.

Внимание! Если вы вошли в консоль управления с правами пользователя, то при попытке открыть экспертные настройки будет предложено войти в консоль управления под другой учетной записью. Нажмите кнопку **Да** и вы сможете сменить пользователя.

---

2 На панели навигации нажмите **Выход**. Откроется окно входа в консоль управления.

3 Введите нужное имя пользователя, пароль и нажмите **Войти**.

Откроется окно консоли управления программой, где вам будут доступны действия в соответствии с ролью учетной записи, под которой вы вошли (см. Разграничение полномочий на основе ролей на стр. 13).

Установка лицензии

Для получения лицензии обратитесь в отдел продаж ОАО "ИнфоТеКС".

Чтобы установить лицензию, выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **О программе**.
4. На вкладке **Данные** нажмите кнопку **Загрузить новый файл лицензии** и выберите файл лицензии (`*.itcslic`).

В результате после проверки лицензия будет установлена и автоматически активирована через Интернет. На странице **О программе** отобразится информация о лицензии. В ViPNet Personal Firewall Linux автоматическая активация не выполняется, поэтому далее активируйте лицензию (см. Активация лицензии на стр. 27).

Внимание! Если автоматическая активация не выполнилась или на вашем компьютере нет доступа в Интернет, активируйте лицензию вручную (см. Активация лицензии на стр. 27).

Активация лицензии

Если лицензия не была автоматически активирована сразу после установки, ее необходимо активировать вручную. Вы можете активировать лицензию через Интернет в режиме реального времени или с помощью отправки запроса на активацию письмом и последующего ввода полученного регистрационного кода. Если компьютер имеет доступ в Интернет, используйте первый способ.

Чтобы активировать лицензию, выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **О программе**.
4. Если на вашем компьютере есть доступ в Интернет, на вкладке **Данные** нажмите кнопку **Активировать лицензию** и из появившегося меню выберите **Активировать через Интернет**. Лицензия будет активирована в течение 30 секунд. Если активация не произошла, через какое-то время вы можете снова попытаться активировать лицензию через Интернет, выбрав из меню **Повторить активацию через Интернет**.

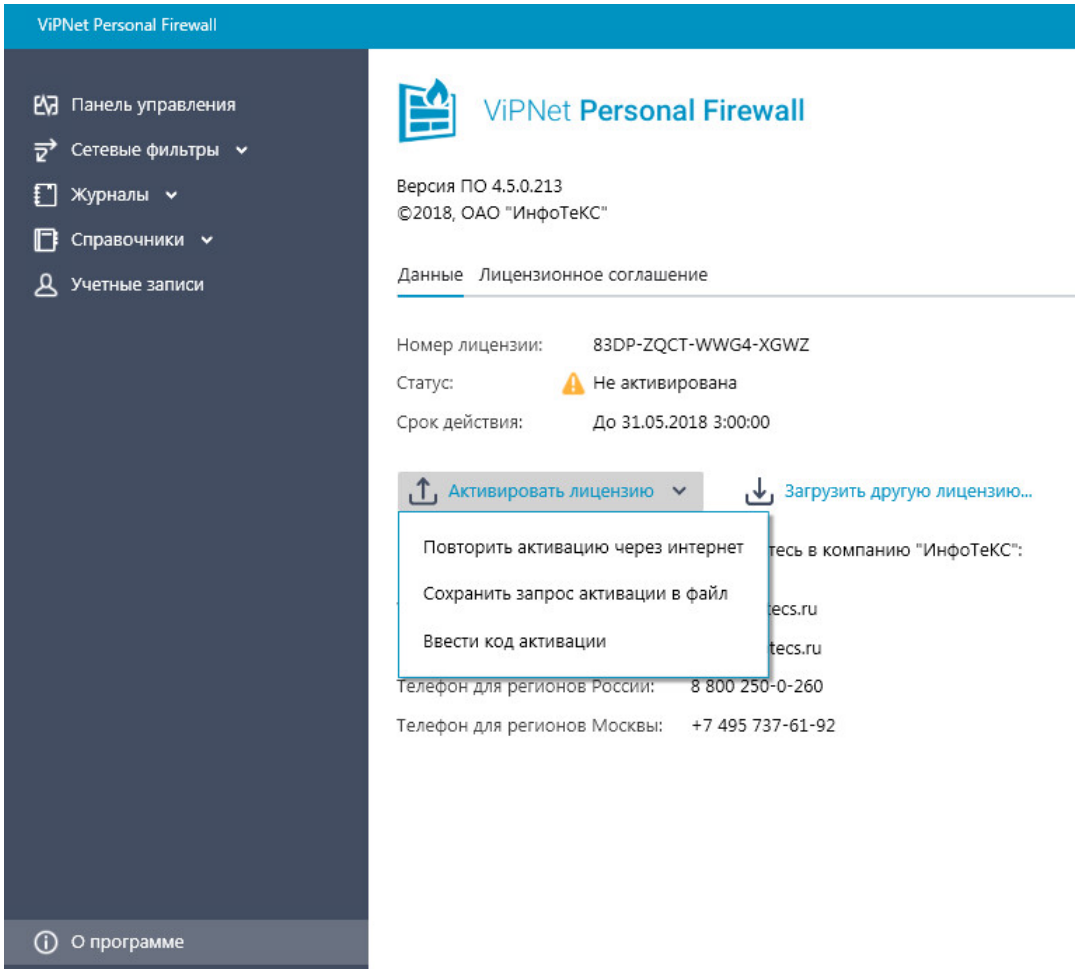

Рисунок 6. Активация лицензии

5 Если активация через Интернет не происходит или на вашем компьютере нет доступа в Интернет, выполните следующие действия:

5.1 На вкладке **Данные** нажмите кнопку **Активировать лицензию** и из появившегося меню выберите **Сохранить запрос на активацию в файл.**

5.2 Сохраните файл с запросом.

5.3 Отправьте письмо на электронный адрес `reg@infotecs.biz`, прикрепив к нему файл с запросом.

5.4 Дождитесь ответного письма. В нем будет указан регистрационный код ViPNet Personal Firewall для активации лицензии.

5.5 На вкладке **Данные** нажмите кнопку **Активировать лицензию** и из появившегося меню выберите **Ввести код активации.**

5.6 В открывшемся окне введите регистрационный код, указанный в полученном письме, и нажмите кнопку **Сохранить**.

В результате лицензия будет активирована и на странице **О программе** отобразится соответствующая информация.

3

Настройка параметров сетевого экрана

Общие сведения о правилах фильтрации трафика 30

Управление режимами работы 35

Управление справочниками 36

Управление сетевыми фильтрами 47

Запрет входящих соединений на указанные порты 52

Централизованное обновление настроек сетевых фильтров 54

Общие сведения о правилах фильтрации трафика

В программе ViPNet Personal Firewall фильтрации подвергается весь трафик, который проходит через компьютер. Наибольшую опасность может представлять трафик из Интернета, где при умелом действии атакующего источник атаки очень сложно обнаружить. Чтобы правильно настроить правила фильтрации, необходимо понимать основные принципы фильтрации трафика в ViPNet Personal Firewall.

Правила фильтрации трафика являются результатом действия:

- выбранного режима работы (см. Управление режимами работы на стр. 35);
- сетевых фильтров, предустановленных в программе и заданных пользователем (см. Управление сетевыми фильтрами на стр. 47). Сетевые фильтры могут быть настроены для фильтрации трафика по следующим параметрам IP-пакетов: портам и протоколам передачи, IP-адресам источника и назначения, направлению передачи. Сетевые фильтры прикладного уровня могут быть настроены для фильтрации HTTP-трафика также по командам HTTP-протокола и типам файлов мобильного кода (JavaScript, PDF, Flash). Параметры IP-пакетов для создания сетевых фильтров задаются в справочниках (см. Управление справочниками на стр. 36).

Внимание! Для эффективного применения сетевых фильтров, запрещающих передачу мобильного кода, возможно понижение скорости канала Интернет.

Предустановленные фильтры задаются автоматически при установке программы ViPNet Personal Firewall. Выбор режимов и задание сетевых фильтров происходит в консоли управления программой.

Доступны следующие режимы работы:

- **Полная блокировка трафика** — это режим максимальной защиты вашего компьютера, при котором блокируются любые входящие и исходящие соединения. Компьютер полностью отключен от внешней сети.
- **Публичная сеть** — в этом режиме блокируются все входящие и исходящие соединения, кроме разрешенных политиками безопасности вашей сети. Режим рекомендуется использовать при работе в общественной сети.
- **Частная сеть** — в этом режиме по умолчанию пропускаются все исходящие соединения, и блокируются все входящие соединения, за исключением разрешенных политиками безопасности вашей сети. Для более тонких настроек вы можете добавить собственные сетевые фильтры. Режим рекомендуется использовать при работе в частной сети, например, из дома.

- **Защищенная сеть** — в этом режиме по умолчанию пропускаются все исходящие и входящие соединения за исключением соединений, запрещенных предустановленными сетевыми фильтрами. Обеспечить дополнительную безопасность компьютера вы можете с помощью настройки сетевых фильтров. Режим рекомендуется использовать при работе в защищенной сети, где относительно низкий уровень угроз безопасности.
- **Отключен** (**Сетевой экран отключен**) — в этом режиме программа ViPNet Personal Firewall полностью отключена и не влияет на сетевой трафик. Никакие правила фильтрации не действуют. Режим предназначен для кратковременного использования для тестовых целей. Этот режим установлен по умолчанию.

Сетевые фильтры могут быть заданы пользователем (или предустановлены программой) только для следующих режимов работы: **Частная сеть** и **Защищенная сеть**. Для каждого режима работы настраивается свой список сетевых фильтров, которые разделены на следующие категории:

- Фильтры политик безопасности — фильтры, загруженные в составе политик безопасности сети. Эти фильтры заданы только для режимов **Публичная сеть** и **Частная сеть**. Их нельзя редактировать, удалять и отключать. Поскольку в текущей версии обновление политик безопасности не реализовано, фильтры политик безопасности задаются автоматически при установке программы и в процессе работы не изменяются.
- Пользовательские фильтры — предустановленные фильтры и фильтры, заданные пользователем. Данные фильтры заданы и могут быть добавлены пользователем только для режимов **Защищенная сеть** и **Частная сеть**. Пользователь может отредактировать или удалить фильтр, а также перемещать фильтры внутри категории (для настройки порядка срабатывания фильтров) и задать расписание работы фильтра.
- Фильтр по умолчанию — предустановленный фильтр, который в зависимости от режима блокирует или пропускают трафик, не соответствующий условиям ни одного из предыдущих фильтров. Этот фильтр отображается только для режимов **Публичная сеть, Частная сеть** и **Защищенная сеть**. Фильтр недоступен для редактирования. Для режимов **Публичная сеть** и **Частная сеть** фильтр по умолчанию блокирует трафик, а для режима **Защищенная сеть** — пропускает.

Все входящие и исходящие IP-пакеты проходят комплексную проверку в соответствии с режимами и настроенными сетевыми фильтрами в порядке их отображения в окне консоли управления сверху вниз. Если IP-пакет не был заблокирован заданным режимом работы и соответствует параметрам одного из имеющихся для выбранного режима работы сетевого фильтра, то он пропускается или блокируется в соответствии с этим фильтром. При этом фильтры, расположенные ниже, не применяются. Если IP-пакет был пропущен одним из фильтров, то ответные IP-пакеты в рамках текущего соединения будут пропускаться автоматически. Если пакет не соответствует ни одному из заданных фильтров, то он блокируется или пропускается в соответствии с фильтром по умолчанию для выбранного режима. Сетевые фильтры прикладного уровня для HTTP-трафика применяются после применения сетевых фильтров для всех типов трафика. Такой способ фильтрации обеспечивает высокий уровень безопасности, разрешая соединения только с нужными узлами по заданным протоколам и портам.

Схематично последовательность фильтрации IP-пакетов представлена ниже.

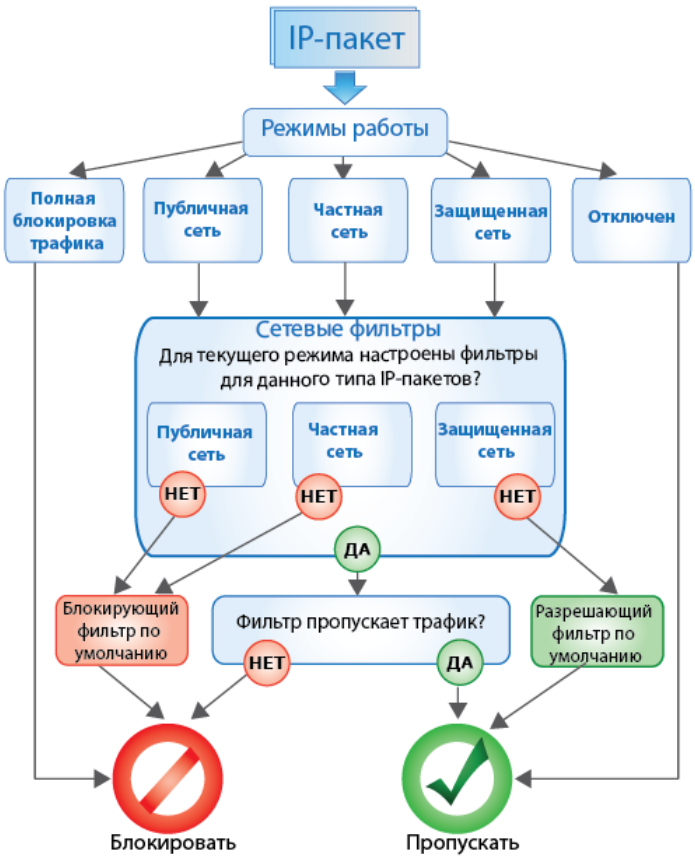

Рисунок 7. Фильтрация IP-трафика

Списки сетевых фильтров для режимов работы **Публичная сеть**, **Частная сеть** и **Защищенная сеть** представлены в консоли управления ViPNet Personal Firewall на панели просмотра в разделе **Сетевые фильтры** в подразделах с названием соответствующего режима.

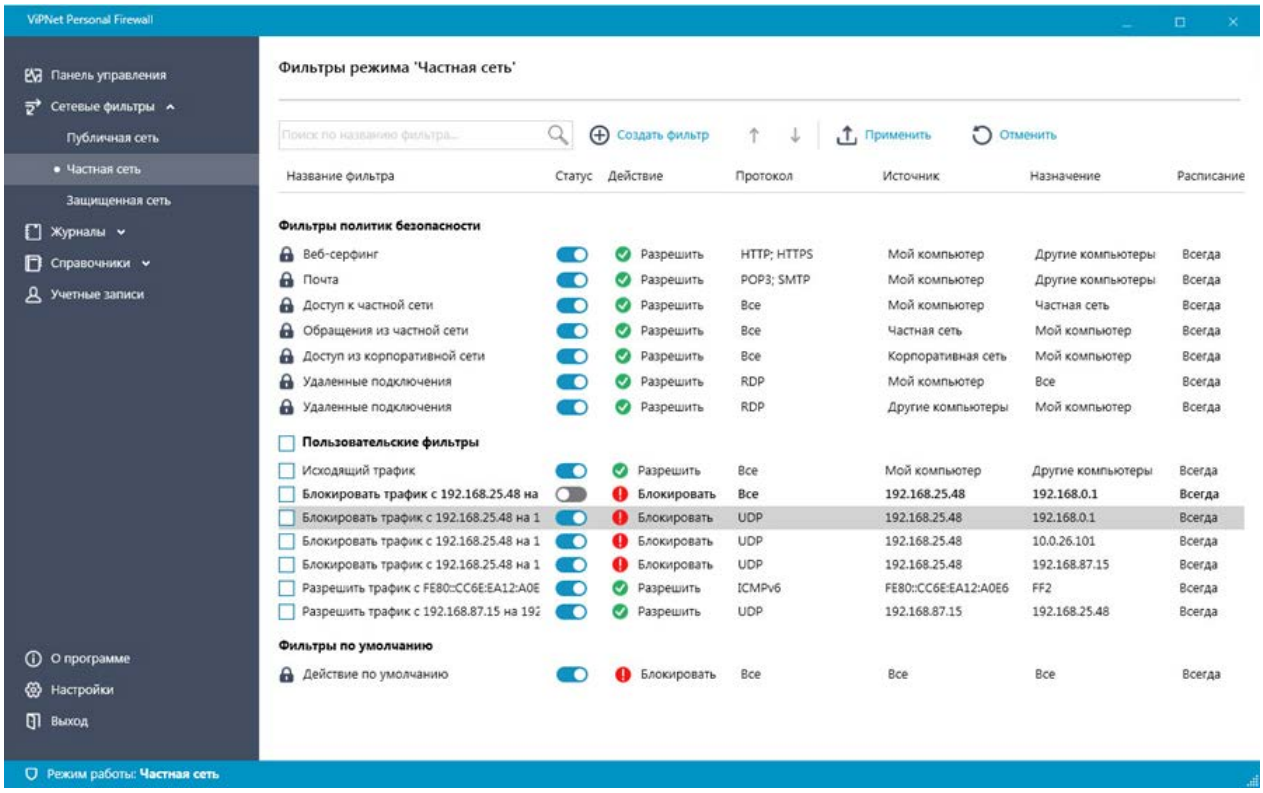

Рисунок 8. Пример отображения сетевых фильтров для режима "Частная сеть"

Фильтры различных категорий в списках фильтров отображаются в соответствующих группах и располагаются в порядке их применения. Последовательность применения сетевых фильтров: сверху вниз.

Сетевые фильтры имеют следующие особенности:

Для каждого фильтра можно настроить:

- Действие — разрешить (), блокировать () IP-пакеты, соответствующие заданным параметрам.
- Источник и назначение задают отправителя и получателя IP-пакетов.
- Протоколы фильтрации IP-пакетов.
- Расписание действия фильтра на трафик.

Для задания параметров фильтра используются справочники (см. Управление справочниками на стр. 36).

Фильтры, созданные пользователем, влияют как на новые, так и на уже существующие соединения. Таким образом, если фильтр, блокирующий трафик соединения, добавлен после установки соединения, то оно будет разорвано.

IP-пакеты проверяются в соответствии с расположением фильтров в списке, по порядку сверху вниз. Когда пакет блокируется или пропускается первым подходящим фильтром, последующие фильтры уже не оказывают никакого влияния на данный пакет.

Порядок фильтров категории **Фильтры политик безопасности** и **Фильтры по умолчанию** изменить нельзя. Порядок фильтров категории **Пользовательские фильтры** вы можете изменять с помощью кнопок ↑ и ↓.

Фильтры, которые нельзя отредактировать и удалить, отмечены значком 🔒.

Чтобы изменить действие фильтра, двойным щелчком откройте свойства фильтра и на вкладке **Основные** в списке **Действие** выберите нужное значение. Чтобы включить или отключить фильтр, в свойствах фильтра на вкладке **Основные** установите переключатель **Фильтрация активна** в нужное положение. Нажмите кнопку **OK**.

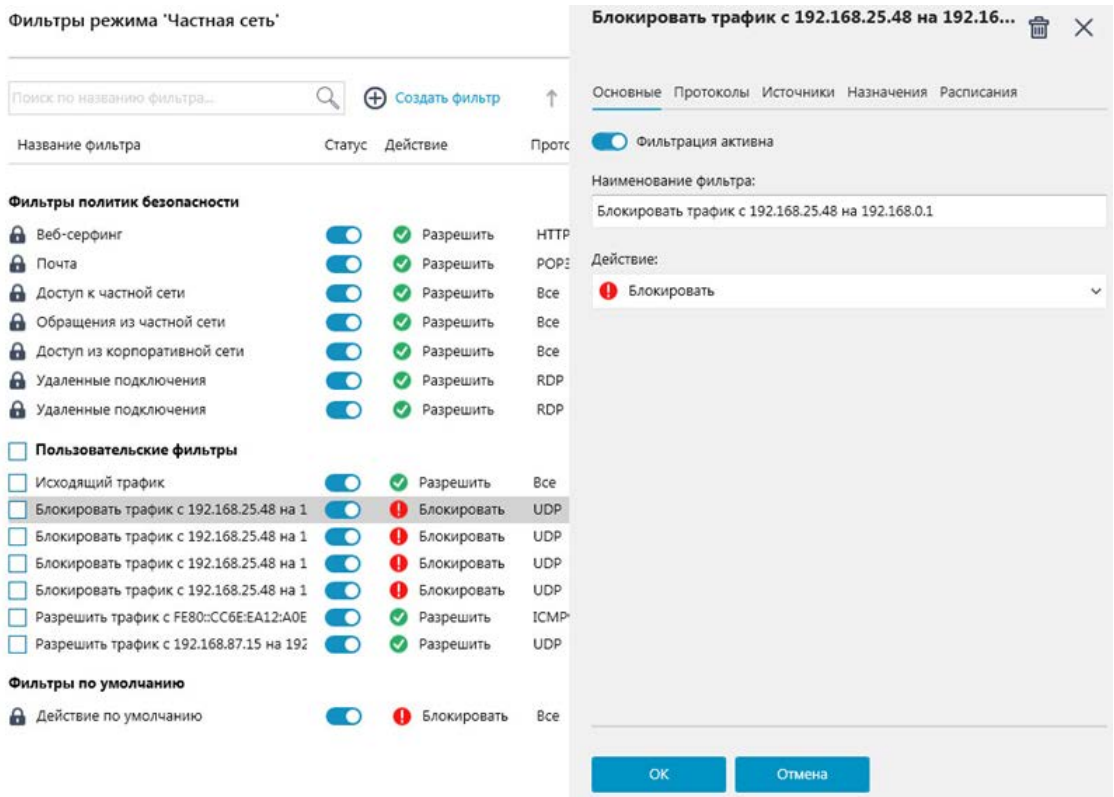

Рисунок 9. Редактирование сетевого фильтра

При изменении настроек сетевых фильтров или создании новых фильтров на панели навигации перед названием раздела, в котором производятся настройки, будет отображена "точка" (см. Рисунок 8 на стр. 33). Измененные или новые фильтры не вступят в действие до тех пор, пока вы не нажмете кнопку **Применить**.

Если вам не требуется сохранять новые настройки фильтров, нажмите кнопку **Отменить** (см. Рисунок 8 на стр. 33). В этом случае произойдет возврат к тем настройкам фильтров, которые действовали на момент их изменения.

Управление режимами работы

После установки программы выберите нужный режим работы программы в соответствии с рекомендациями из раздела Общие сведения о правилах фильтрации трафика (на стр. 30). В процессе работы вы можете сменить режим работы программы, например, в случае подключения к сети с другим уровнем безопасности.

Для изменения режима работы выполните следующие действия:

1 Войдите в консоль управления программой ViPNet Personal Firewall под любой учетной записью (см. Запуск и завершение работы с программой на стр. 20).

2 Выполните одно из следующих действий:

- В появившемся окне консоли управления в группе **Режим работы** щелкните нужный режим.

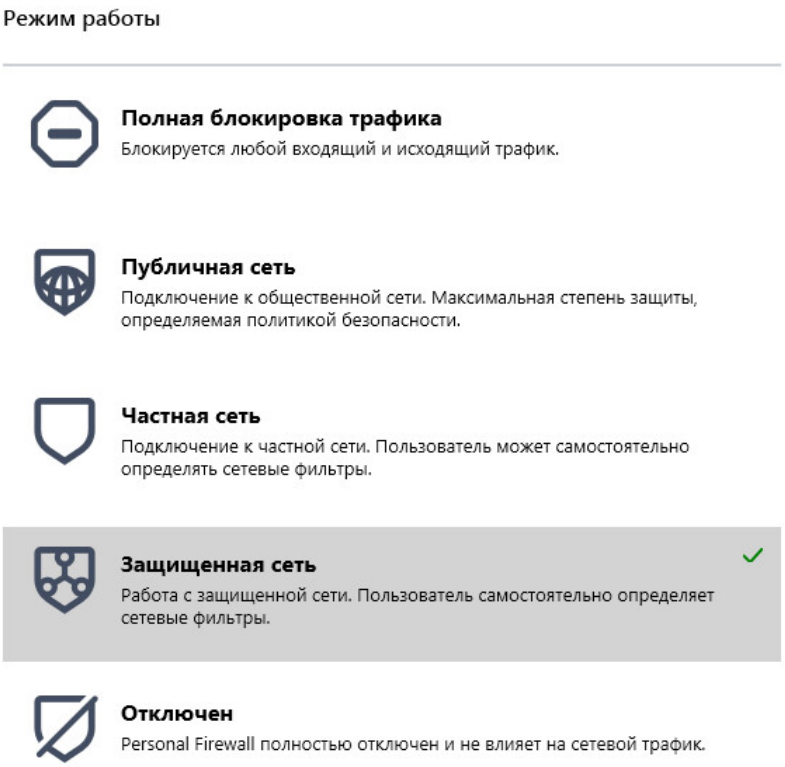

Рисунок 10. Выбор режима работы

- В области уведомлений в контекстном меню программы выберите пункт с названием нужного режима.

В результате режим работы будет изменен и начнут действовать правила фильтрации выбранного режима. В списке режимов выбранный режим будет выделен цветом и отмечен флажком.

Управление справочниками

Справочники позволяют упростить процессы создания и изменения сетевых фильтров в ViPNet Personal Firewall. Каждый справочник объединяет несколько объектов одного типа (например, IP-адреса или протоколы), а также могут быть заданы исключения. Справочники указываются при задании параметров сетевого фильтра (см. Управление сетевыми фильтрами на стр. 47) вместо перечисления отдельных объектов. Также справочники могут быть использованы для создания других справочников.

В зависимости от типа объединяемых объектов различаются следующие виды справочников:

- Протоколы — содержат любую комбинацию сетевых протоколов и их параметров.
- Адреса и сети — содержат любую комбинацию IP-адресов или диапазонов IP-адресов. Доступно задание IPv4- и IPv6-адресов.
- Расписания — содержат любую комбинацию параметров, определяющих время применения сетевого фильтра.

Управление справочниками доступно в окне консоли управления ViPNet Personal Firewall на панели просмотра в разделах **Справочники** > **Протоколы**, **Адреса и сети** и **Расписания** соответственно.

Справочники могут быть созданы пользователем. Также в составе ViPNet Personal Firewall имеются следующие справочники, настроенные по умолчанию:

- Протоколы — содержит справочники с прикладными протоколами, которые наиболее часто используются при создании сетевых фильтров.
- Адреса и сети — содержит справочники:
  - Другие компьютеры — включает любые IP-адреса, кроме принадлежащих своему компьютеру.
  - Корпоративная сеть — включает IP-адреса корпоративных ресурсов.
  - Мой компьютер — включает IP-адреса своего компьютера. Выбор этого справочника в настройке сетевого фильтра в качестве адреса источника (см. Управление сетевыми фильтрами на стр. 47) будет означать исходящий трафик. Выбор в качестве адреса назначения — входящий.
  - Частная сеть — включает частные IP-адреса своего компьютера.
- Расписания — содержит справочники расписаний применения сетевых фильтров:
  - Выходные дни — включает выходные дни недели (субботу и воскресенье).
  - Рабочие дни — включает рабочие дни недели (с понедельника по пятницу).

Чтобы создать справочник, выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.

3 На панели навигации перейдите в раздел **Справочники** в подраздел с названием вида справочника, который вы хотите создать.

4 На панели инструментов нажмите **Создать справочник**.

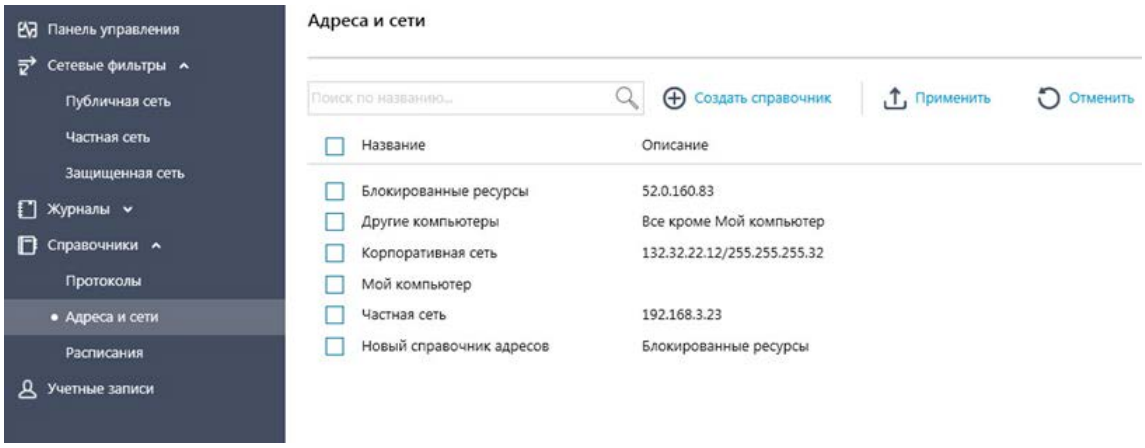

Рисунок 11. Список справочников адресов

5 В появившемся мастере создания справочников на странице **Состав** определите, какие объекты будут входить в состав справочника, и задайте параметры каждого выбранного объекта.

Примечание. В ViPNet Personal Firewall Linux на первой странице мастера создания справочников следует указать название справочника, а состав справочника указывается на следующих страницах.

---

6 На странице **Исключения** определите, какие объекты будут исключены из состава справочника.

Для настройки состава и исключений из справочника в зависимости от вида создаваемого справочника воспользуйтесь рекомендациями соответствующего раздела:

- Протоколы (на стр. 40).
- Адреса и сети (на стр. 43).
- Расписание (на стр. 45).

Примечание. После добавления или исключения хотя бы одного объекта для добавления следующего объекта на странице **Состав** или **Исключение** соответственно нажмите кнопку **Добавить** и из меню выберите пункт с названием нужного объекта.

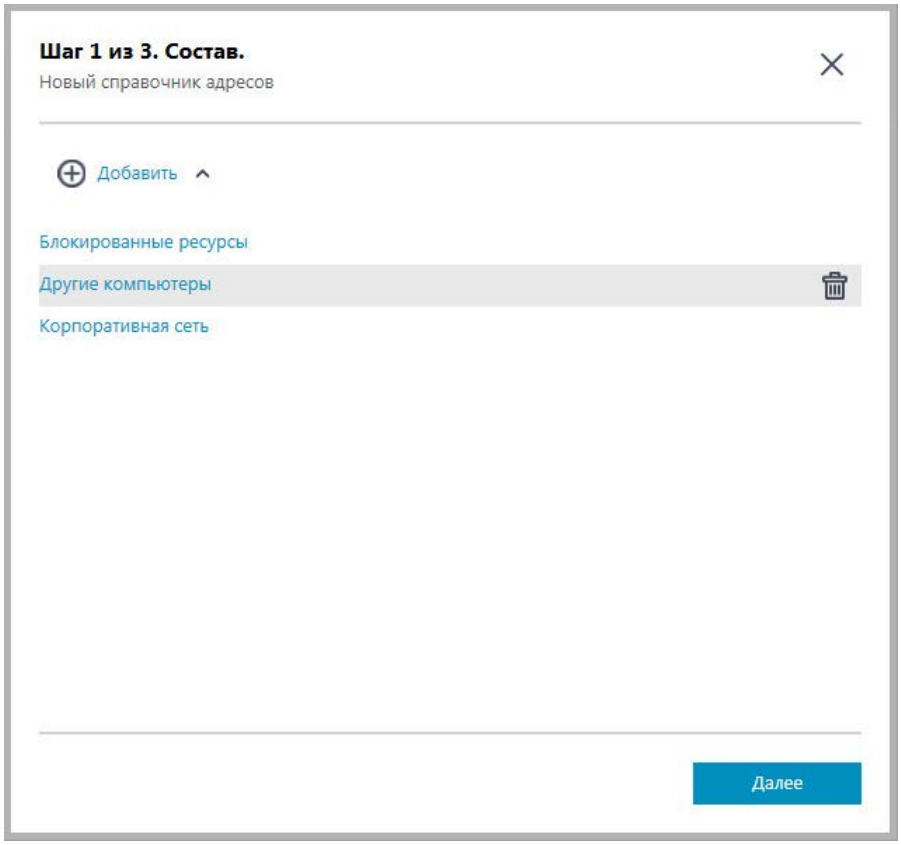

Рисунок 12. Настройка состава справочника адресов

Примечание. Чтобы удалить объект, который вы уже добавили в состав или исключение из справочника, наведите указатель мыши на этот объект и нажмите появившуюся кнопку **Удалить**.

---

7 На странице **Подтверждение** введите название справочника и проверьте заданные настройки справочника. При необходимости внесения изменений нажмите кнопку напротив того объекта, который нужно изменить, и внесите изменения в соответствии с рекомендациями из вышеуказанных разделов.

Примечание. В ViPNet Personal Firewall Linux нет страницы подтверждения. Для внесения изменений перейдите на нужную страницу мастера создания справочников.

---

8 Нажмите кнопку **Готово**.

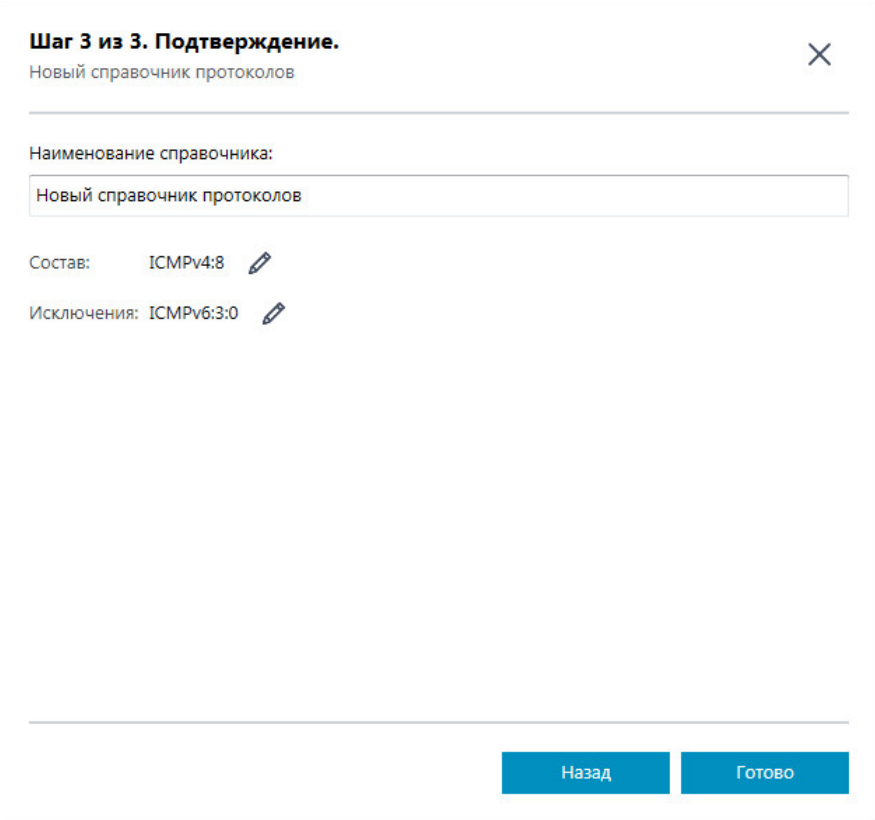

Рисунок 13. Страница подтверждения настройки сетевого фильтра

В результате будет создан справочник выбранного вида и отобразится на странице с названием вида справочника (см. Рисунок 11 на стр. 37).

9 Чтобы изменения вступили в силу, на странице с названием вида справочника (см. Рисунок 11 на стр. 37) на панели инструментов нажмите кнопку **Применить**.

Если вам не требуется сохранять созданные справочники нажмите кнопку **Отменить**. В этом случае произойдет возврат к тем спискам справочников, которые были на момент их изменения.

Чтобы изменить настройки справочника, в списке справочников два раза щелкните строку с нужным справочником и на появившейся панели на вкладках **Состав** и **Исключения** внесите необходимые изменения в соответствии с приведенным выше описанием. На вкладке **Основные** вы можете изменить название справочника.

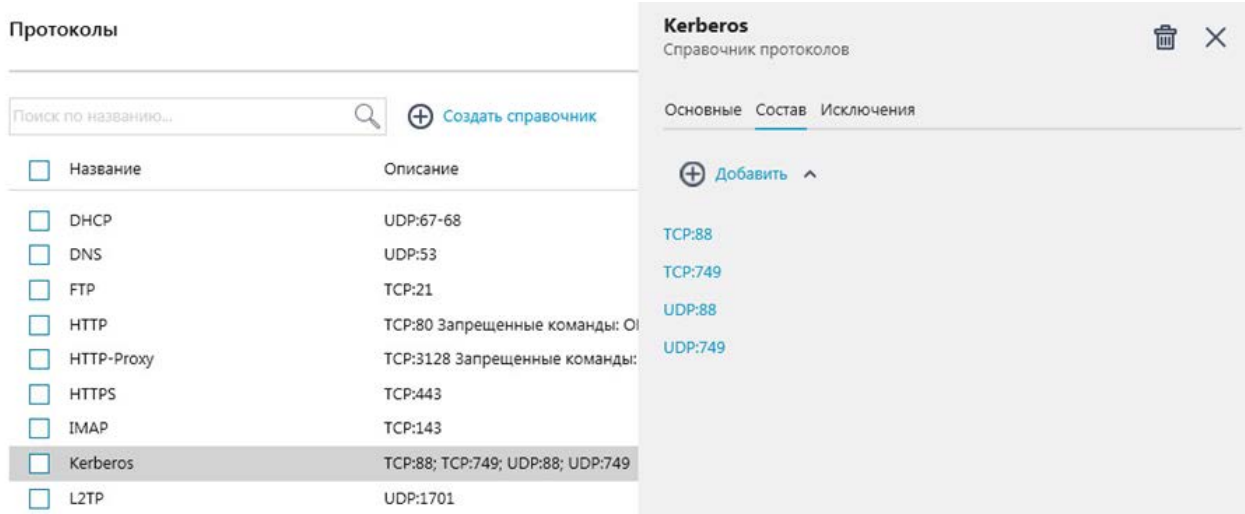

Рисунок 14. Редактирование справочника протоколов

Чтобы удалить справочник, нажмите кнопку **Удалить**. Если справочник используется хотя бы в одном сетевом фильтре, то удалить его невозможно. Список сетевых фильтров, в которых используется справочник, вы можете посмотреть на вкладке **Основные** в разделе **Применение в других объектах**.

Примечание. Вы можете удалить сразу несколько справочников, для этого установите флажки напротив нужных справочников и на появившейся панели нажмите кнопку **Удалить**. Данная возможность недоступна в ViPNet Personal Firewall Linux.

Протоколы

При создании или изменении справочника протоколов (см. Управление справочниками на стр. 36) вы можете добавить или исключить следующие объекты:

- Протокол TCP.
- Протокол UDP.
- Сообщение ICMP.
- Сообщение ICMPv6.
- Существующий справочник протоколов.

Примечание. В ViPNet Personal Firewall Linux существуют следующие отличия при создании справочника протоколов:

- Настройки для протоколов TCP и UDP объединены в одно окно.
- Сообщения ICMP также настраиваются в одном окне. При этом настройка типов и кодов сообщений недоступна.
- Недоступно использование существующего справочника протоколов.

Чтобы добавить или исключить объект, в мастере создания справочника **Протоколы** на странице **Состав** или **Исключение** соответственно выполните следующие действия:

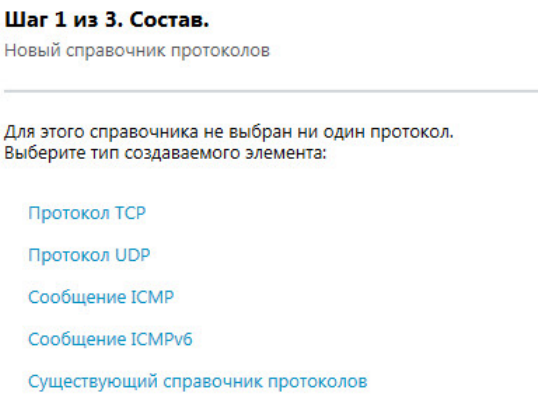

Рисунок 15. Выбор объекта для добавления в справочник

1 Если вы хотите добавить или исключить протокол TCP, щелкните соответствующую строку и в появившемся окне настройте порты источника, приемника, укажите команды, которые должны быть запрещены, а также запрет на передачу мобильного кода в виде файлов различных типов и нажмите **Сохранить**.

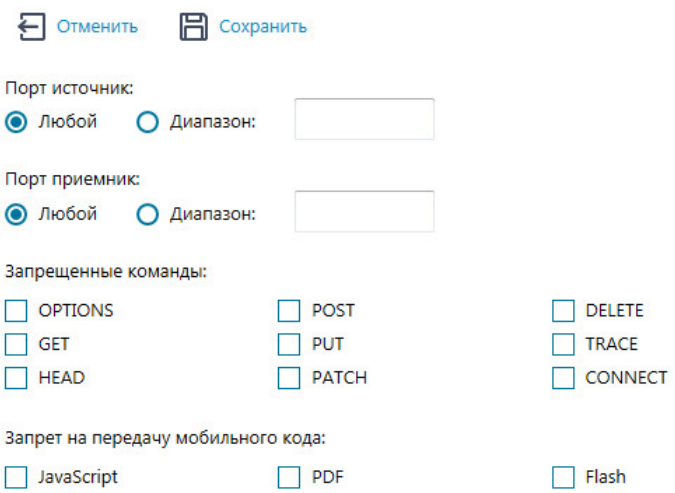

Рисунок 16. Настройка параметров протокола TCP

2 Если вы хотите добавить или исключить протокол UDP, щелкните соответствующую строку и в появившемся окне настройте порты источника, приемника и нажмите **Сохранить**.

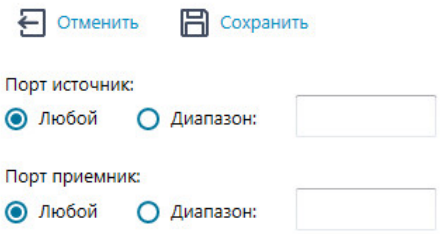

Рисунок 17. Настройка параметров протокола UDP

3 Если вы хотите добавить или исключить протокол ICMP, щелкните соответствующую строку и в появившемся окне выберите в списке нужный тип ICMP-сообщений и при необходимости их код, и нажмите **Сохранить**.

Рисунок 18. Настройка параметров протокола ICMP

4 Если вы хотите добавить или исключить протокол ICMP для IPv6, щелкните строку ICMPv6 и в появившемся окне выберите в списке нужный тип ICMP-сообщений и при необходимости их код, и нажмите **Сохранить**.

Рисунок 19. Настройка параметров протокола ICMPv6

5 Если вы хотите добавить или исключить существующий справочник протоколов, щелкните соответствующую строку и в появившемся окне включите переключатели нужных справочников протоколов, и нажмите **Сохранить**.

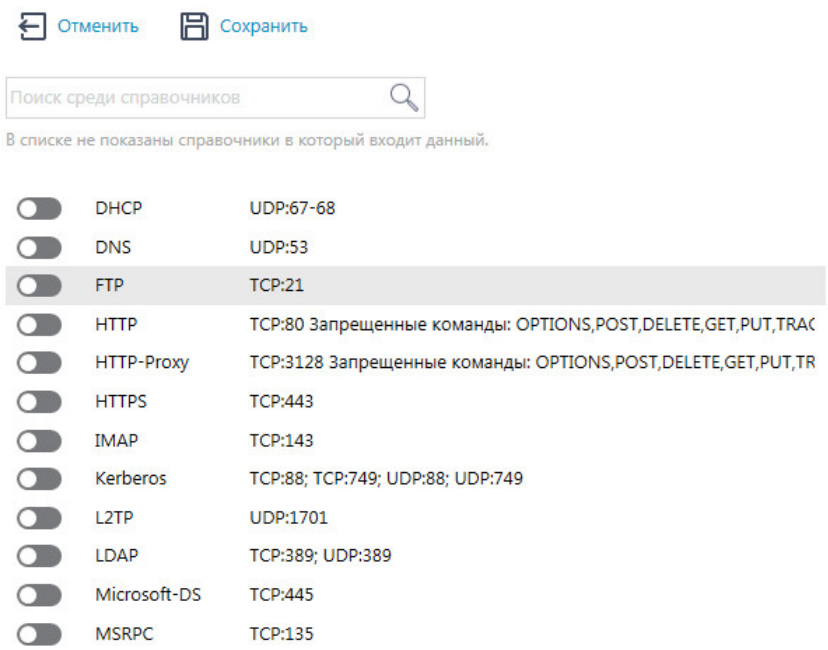

Рисунок 20. Выбор существующих справочников

Адреса и сети

При создании или изменении справочника адресов вы можете добавить или исключить следующие объекты:

- Адрес IPv4.
- Адрес IPv6.
- Существующий справочник адресов.

Примечание. В ViPNet Personal Firewall Linux при создании справочников адресов недоступно использование существующего справочника адресов.

Чтобы добавить или исключить объект, в мастере создания справочника **Адреса и сети** на странице **Состав** или **Исключение** соответственно выполните следующие действия:

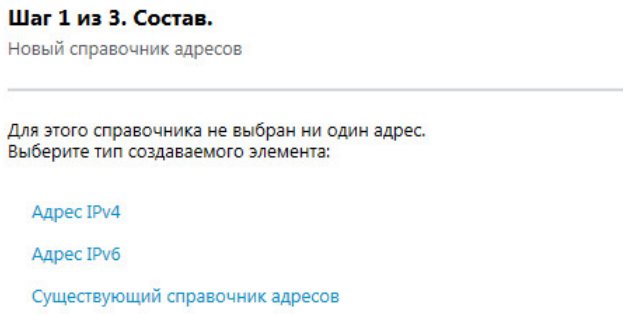

Рисунок 21. Выбор объекта для добавления в справочник

1 Если вы хотите добавить или исключить IPv4-адреса (единичный IP-адрес, подсеть или диапазон IP-адресов), щелкните соответствующую строку и в появившемся окне выполните одну из настроек:

   - для задания одного IP-адреса установите переключатель в положение **IP-адрес** и укажите IP-адрес;
   - для задания адреса подсети установите переключатель в положение **Подсеть** и укажите адрес и маску подсети;
   - для задания диапазона IP-адресов установите переключатель в положение **Диапазон адресов** и укажите начальный и конечный IP-адреса диапазона.

   Нажмите **Сохранить**.

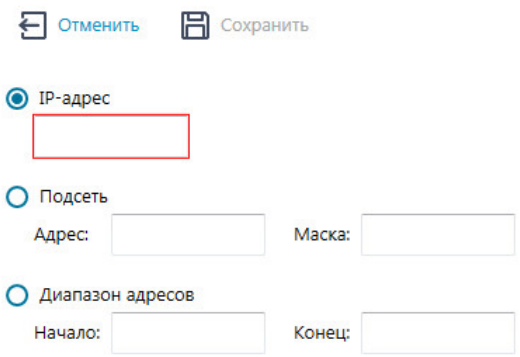

Рисунок 22. Настройка IPv4-адресов

2 Если вы хотите добавить или исключить IPv6-адреса (единичный или подсеть), щелкните соответствующую строку и в появившемся окне укажите IP-адрес в формате IPv6, например `2001:db80:0000:a000:c000:d000:b000:e2f0`, а для указания подсети — длину префикса подсети.

   Нажмите **Сохранить**

Рисунок 23. Настройка IPv6-адресов

3 Если вы хотите добавить или исключить существующий справочник адресов, щелкните соответствующую строку и в появившемся окне включите переключатели нужных справочников адресов, и нажмите **Сохранить**.

Расписание

При создании или изменении справочника расписаний применения фильтров вы можете добавить или исключить следующие объекты:

- Новое расписание.
- Существующий справочник расписаний.

Примечание. В ViPNet Personal Firewall Linux при создании справочников расписаний недоступно использование существующего справочника расписаний.

Чтобы добавить или исключить объект, в мастере создания справочника **Расписания** на странице **Состав** или **Исключение** соответственно выполните следующие действия:

1 Если вы хотите добавить или исключить новое расписание, щелкните соответствующую строку и в появившемся окне выполните следующие действия:

   - чтобы расписание выполнялось в определенное время суток, установите флажок **Выполнять только в указанное время** и укажите время выполнения;
   - чтобы расписание выполнялось каждый день, установите переключатель в положение **Ежедневно**, а для ограничения периода выполнения расписания установите флажок периода и укажите интервал дат, в который расписание будет выполняться;

   Примечание. В ViPNet Personal Firewall Linux недоступна настройка периода выполнения расписания.

   - чтобы расписание выполнялось в определенные дни недели, установите переключатель в положение **Еженедельно** и установите флажки рядом с нужными днями недели.

   Нажмите **Сохранить**.

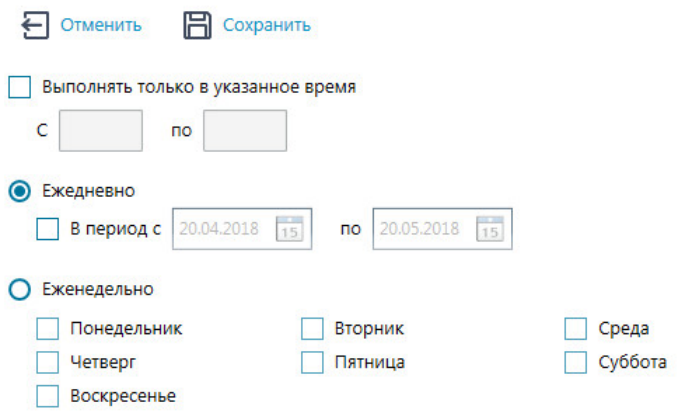

Рисунок 24. Настройка справочника расписаний

2 Если вы хотите добавить или исключить существующий справочник расписаний, щелкните соответствующую строку и в появившемся окне включите переключатели нужных справочников расписаний. Нажмите **Сохранить**.

Управление сетевыми фильтрами

Вы можете создавать сетевые фильтры следующими способами:

- Вручную с помощью справочников (см. ниже).
- Из журнала активных соединений путем блокировки приложений, которые в настоящий момент работают с сетью (см. Отслеживание и блокировка активных соединений на стр. 58).
- Из журнала регистрации трафика путем разрешения или блокировки зарегистрированного трафика (см. Просмотр журнала регистрации трафика и создание сетевых фильтров на основе событий журнала на стр. 60).

Чтобы создать сетевой фильтр, выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора или аудитора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. Выполните одно из действий:
   - Для создания разрешающего сетевого фильтра на панели навигации перейдите в раздел **Панель управления** и в группе **Задачи** щелкните **Разрешить соединение**.
   - Для создания запрещающего сетевого фильтра на панели навигации перейдите в раздел **Панель управления** и в группе **Задачи** щелкните **Запретить соединение**.
   - На панели навигации перейдите в раздел **Сетевые фильтры** в подраздел с названием режима работы, для которого вы хотите настроить сетевой фильтр, и на панели инструментов нажмите **Создать фильтр**.

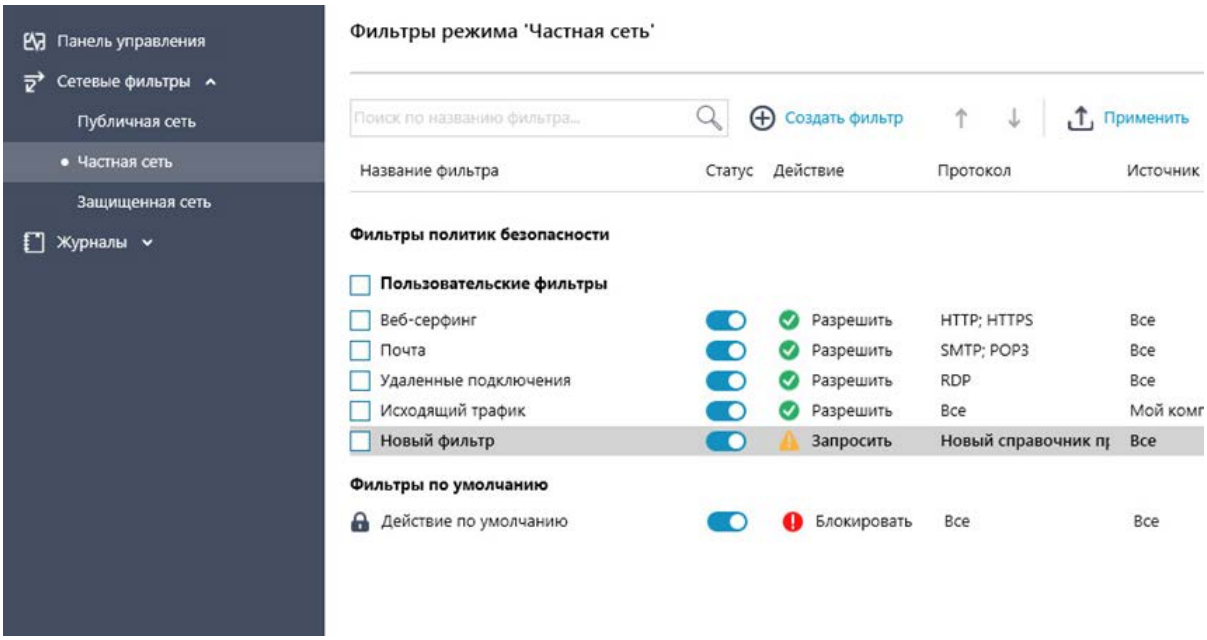

Рисунок 25. Создание сетевого фильтра

4 В появившемся мастере создания фильтра на странице **Основные настройки** выполните следующие действия:

4.1 Определите действие, которое будет выполнять фильтр при срабатывании, установив переключатель в положение **Разрешить**, **Запросить** или **Блокировать** IP-трафик. В текущей версии программы сетевой фильтр с действием **Запросить** работает аналогично блокирующему фильтру (с действием **Блокировать**).

4.2 Установите флажки тех режимов, для которых вы хотите создать сетевой фильтр. Вы можете создать фильтр, как для одного режима, так и сразу для двух режимов работы **Частная сеть** и **Защищенная сеть**.

Примечание. В ViPNet Personal Firewall Linux на первой странице мастера создания фильтра следует указать также название фильтра.

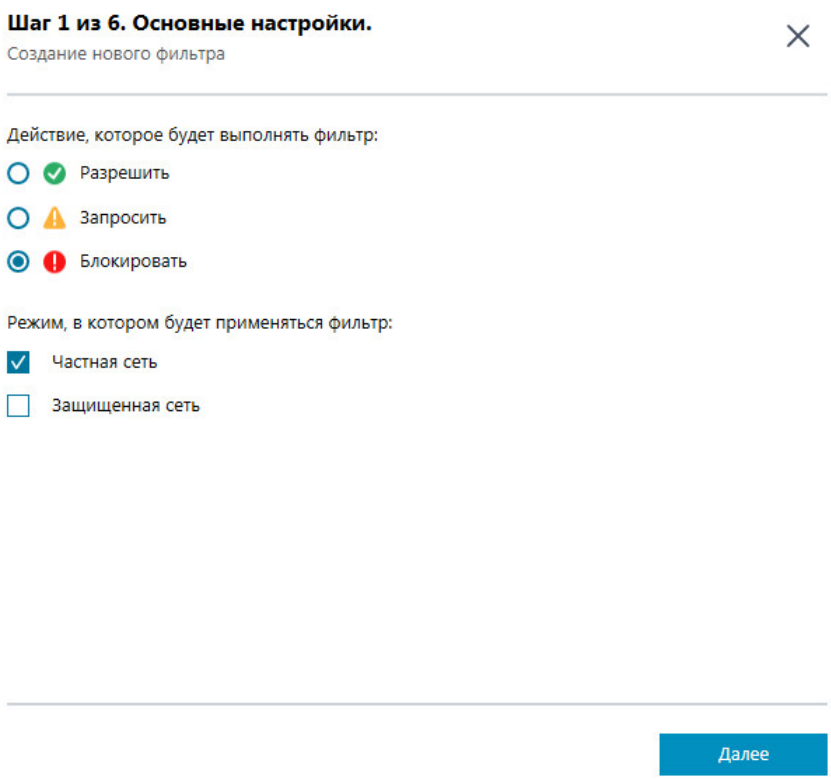

Рисунок 26. Настройка действия фильтра и режима применения

5 На странице **Выберите протоколы** укажите протоколы передачи IP-пакетов. По умолчанию фильтр применяется к IP-пакетам, передаваемым по всем протоколам. Для выбора определенных протоколов включите переключатели тех справочников протоколов, на основании которых будет срабатывать фильтр.

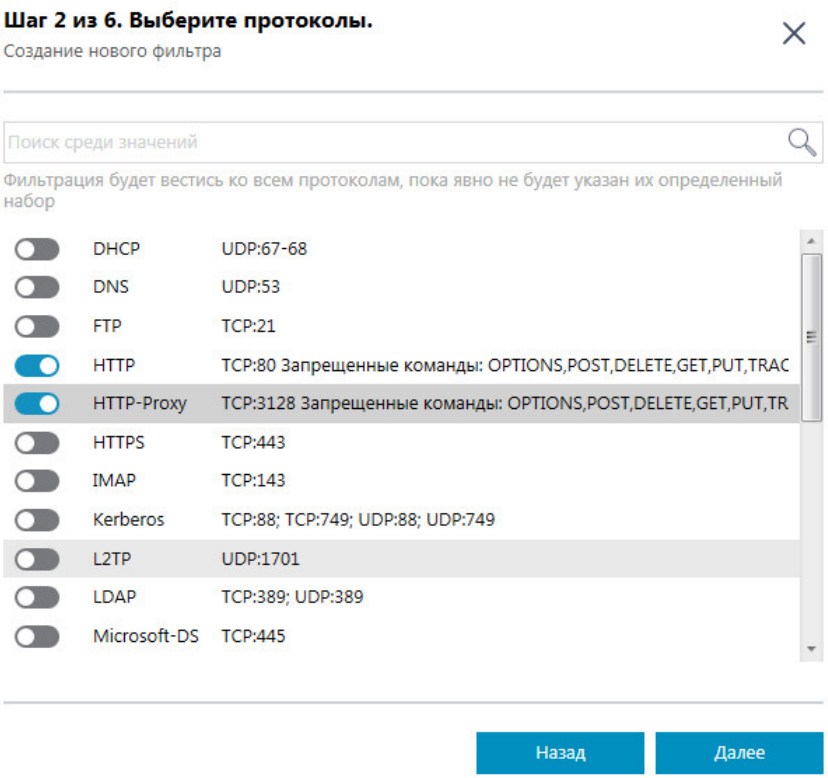

Рисунок 27. Выбор протоколов для фильтрации

6 На странице **Укажите адреса источников** укажите отправителей IP-пакетов. По умолчанию фильтр применяется к IP-пакетам с любыми адресами отправителя. Для выбора определенных IP-адресов отправителей введите нужные IP-адреса или включите переключатели тех справочников адресов, на основании которых будет срабатывать фильтр.

Примечание. При указании диапазона IP-адресов разделяйте начальное и конечное значение диапазона дефисом. Например, 192.168.0.0-192.168.0.100. При указании нескольких IP-адресов или диапазонов IP-адресов разделяйте их запятыми. Например, 192.168.0.0-192.168.0.100,192.168.0.111,192.168.0.120.

---

7 На странице **Укажите адреса назначений** укажите получателей IP-пакетов. По умолчанию фильтр применяется к IP-пакетам с любыми адресами получателя. Для выбора определенных IP-адресов получателей введите нужные IP-адреса или включите переключатели тех справочников адресов, на основании которых будет срабатывать фильтр.

8 На странице **Установите расписание** укажите время применения фильтра. По умолчанию фильтр применяется постоянно. Для выбора определенного времени применения фильтра включите переключатели тех справочников расписаний, на основании которых будет срабатывать фильтр.

9 На странице **Подтверждение** введите название фильтра и проверьте заданные настройки. При необходимости внесения изменений нажмите кнопку напротив того параметра фильтра, который нужно изменить, и внесите изменения.

Примечание. В ViPNet Personal Firewall Linux нет страницы подтверждения. Для внесения изменений перейдите на нужную страницу мастера создания фильтра.

10 Нажмите кнопку **Готово**.

В результате для указанных режимов будет создан фильтр, который отобразится на страницах с названием соответствующего режима работы **Частная сеть** или **Защищенная сеть** в группе **Пользовательские фильтры**.

11 Задайте порядок действия фильтров, переместив созданный фильтр в группе **Пользовательские фильтры** на нужное место. Для этого установите флажок перед названием фильтра и переместите его с помощью кнопок ↑ и ↓ на панели инструментов.

Примечание. В ViPNet Personal Firewall Linux для перемещения фильтра два раза щелкните его и на появившейся панели воспользуйтесь кнопками перемещения ↑ и ↓.

12 Чтобы изменения вступили в силу, на странице с названием каждого режима работы, для которого создан фильтр, на панели инструментов нажмите кнопку **Применить**.

Чтобы изменить настройки сетевого фильтра или выключить его, в списке фильтров два раза щелкните строку с нужным фильтром и на появившейся панели на вкладках **Основные**, **Протоколы**, **Источники**, **Назначения** и **Расписания** внесите необходимые изменения в соответствии с приведенным выше описанием. Чтобы отключить фильтр, на вкладке **Основные** выключите переключатель **Фильтрация активна**.

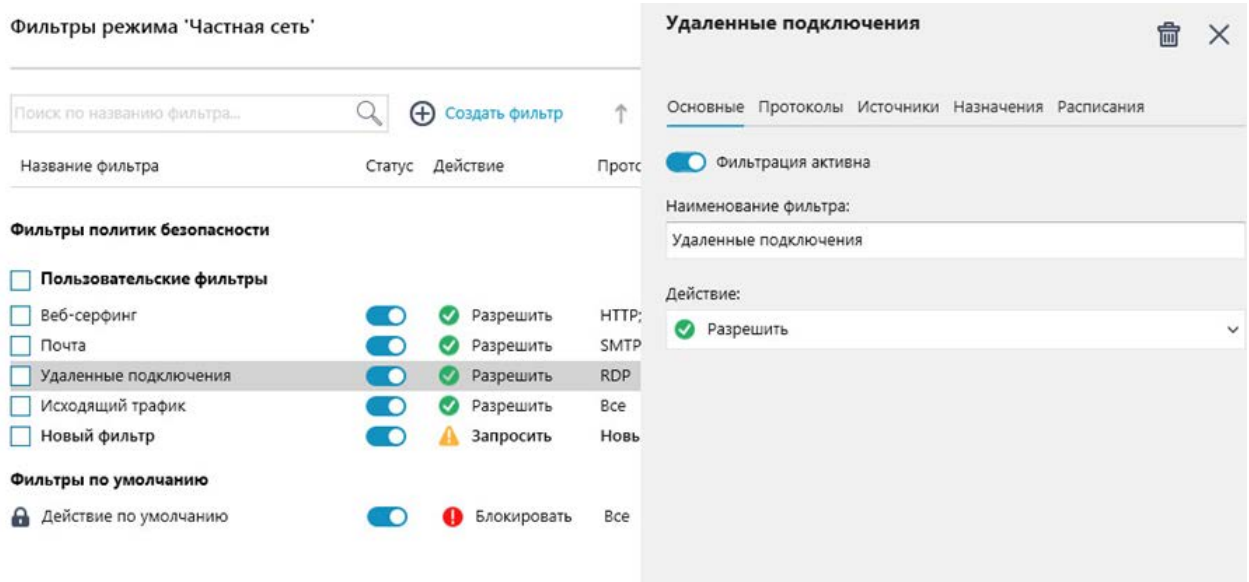

Рисунок 28. Изменение параметров сетевого фильтра

Чтобы удалить сетевой фильтр, нажмите кнопку **Удалить**.

Примечание. Вы можете удалить сразу несколько сетевых фильтров, для этого установите флажки напротив нужных фильтров и на появившейся панели нажмите кнопку **Удалить**. Данная возможность недоступна в ViPNet Personal Firewall Linux.

Запрет входящих соединений на указанные порты

Если требуется ограничить доступ к вашему компьютеру через определенные порты, создайте сетевой фильтр по портам. Для этого выполните следующие действия:

1 Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора или аудитора (см. Запуск и завершение работы с программой на стр. 20).

2 В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.

3 На панели навигации перейдите в раздел **Панель управления** и в группе **Задачи** щелкните **Скрыть порты**.

4 В появившемся мастере скрытия портов на странице **Выберите порт** выполните следующие действия:

Примечание. В ViPNet Personal Firewall Linux на первой странице мастера создания фильтра следует указать также название фильтра.

4.1 Укажите один или несколько портов, на которые вы хотите запретить входящие соединения.

Примечание. При указании диапазона портов разделяйте начальное и конечное значение диапазона дефисом. Например, 20-27. При указании нескольких портов или диапазонов портов разделяйте их запятыми. Например, 40-45,80,81,593. В ViPNet Personal Firewall Linux можно указать только один порт или диапазон портов.

4.2 Установите флажки тех режимов, для которых вы хотите создать сетевые фильтры.

5 На странице **Установите расписание** укажите время применения фильтра. По умолчанию фильтр применяется постоянно. Для выбора определенного времени применения фильтра включите переключатели тех справочников расписаний, на основании которых будет срабатывать фильтр.

6 На странице **Подтверждение** введите название фильтра и проверьте заданные настройки. При необходимости внесения изменений нажмите кнопку напротив того параметра фильтра, который нужно изменить, и внесите изменения.

Примечание. В ViPNet Personal Firewall Linux нет страницы подтверждения. Для внесения изменений перейдите на нужную страницу мастера создания фильтра.

7 Нажмите кнопку **Готово**.

В результате для указанных режимов будет создан фильтр, который отобразится на страницах с названием соответствующего режима работы **Частная сеть** или **Защищенная сеть** в группе **Пользовательские фильтры**.

8 Задайте порядок действия фильтров, переместив созданный фильтр в группе **Пользовательские фильтры** на нужное место. Для этого установите флажок перед названием фильтра и переместите его с помощью кнопок ↑ и ↓ на панели инструментов.

Примечание. В ViPNet Personal Firewall Linux для перемещения фильтра два раза щелкните его и на появившейся панели воспользуйтесь кнопками перемещения ↑ и ↓.

---

9 Чтобы изменения вступили в силу, на странице с названием каждого режима работы, для которого создан фильтр, на панели инструментов нажмите кнопку **Применить**.

Централизованное обновление настроек сетевых фильтров

В программе ViPNet Personal Firewall предоставляется возможность обновлять сетевые фильтры с помощью специального файла в формате `JSON`. Доступно обновление как вручную, так и автоматически из файла, сохраненного на сетевом диске. Для централизованного обновления настроек сетевых фильтров выполните следующие действия:

1. На одном из компьютеров с ViPNet Personal Firewall создайте необходимые сетевые фильтры (см. Управление сетевыми фильтрами на стр. 47).
2. Выгрузите настройки сетевых фильтров в файл (см. Выгрузка настроек в файл на стр. 54).
3. Распространите файл с настройками среди других компьютеров с ViPNet Personal Firewall одним из следующих способов:
   - Передайте файл с настройками администраторам других ViPNet Personal Firewall для их загрузки в программу (см. Загрузка настроек из файла на стр. 55).
   - Сохраните файл на сетевой диск, а на остальных компьютерах с ViPNet Personal Firewall настройте автоматическое обновление из этого файла и укажите период обновления (см. Автоматическое обновление настроек из файла на стр. 55).

   При изменении сетевых фильтров сохраняйте на сетевом диске обновленный файл с настройками.

Выгрузка настроек в файл

Вы можете сохранить пользовательские сетевые фильтры в файл. Для этого выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **Панель управления** и в группе **Задачи** щелкните **Выгрузить настройки**.
4. Укажите папку для сохранения файла с настройками и подтвердите сохранение. По умолчанию настройки сохраняются в файл `pfsettings.json`.

Примечание. В ViPNet Personal Firewall Linux необходимо задать имя файла.

В результате все пользовательские сетевые фильтры будут сохранены в указанный файл по выбранному пути.

Загрузка настроек из файла

Вы можете загрузить в программу ViPNet Personal Firewall пользовательские сетевые фильтры из файла в формате `JSON`. Для этого выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **Панель управления** и в группе **Задачи** щелкните **Загрузить настройки**.
4. Выберите нужный файл с сетевыми фильтрами.

В результате пользовательские сетевые фильтры из файла будут загружены в ViPNet Personal Firewall и отобразятся в окне консоли управления ViPNet Personal Firewall на панели просмотра в разделах **Сетевые фильтры** > **Частная сеть** или **Защищенная сеть** в зависимости от фильтров, заданных в файле.

Автоматическое обновление настроек из файла

Вы можете настроить автоматическое обновление настроек сетевых фильтров из файла (`*.json`), сохраненного на сетевом диске. Для этого выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **Настройки**.
4. На странице **Настройки** установите флажок **Автоматически обновлять настройки**.
5. Справа от поля **Сетевой путь к файлу с настройками** нажмите кнопку **Изменить** и укажите путь к файлу.

Примечание. В ViPNet Personal Firewall Linux путь к файлу введите в поле **Сетевой путь к файлу с правилами**.

---

6. В списке **Период опроса** выберите период проверки изменений в файле для загрузки новых данных.
7. Нажмите **Сохранить**.

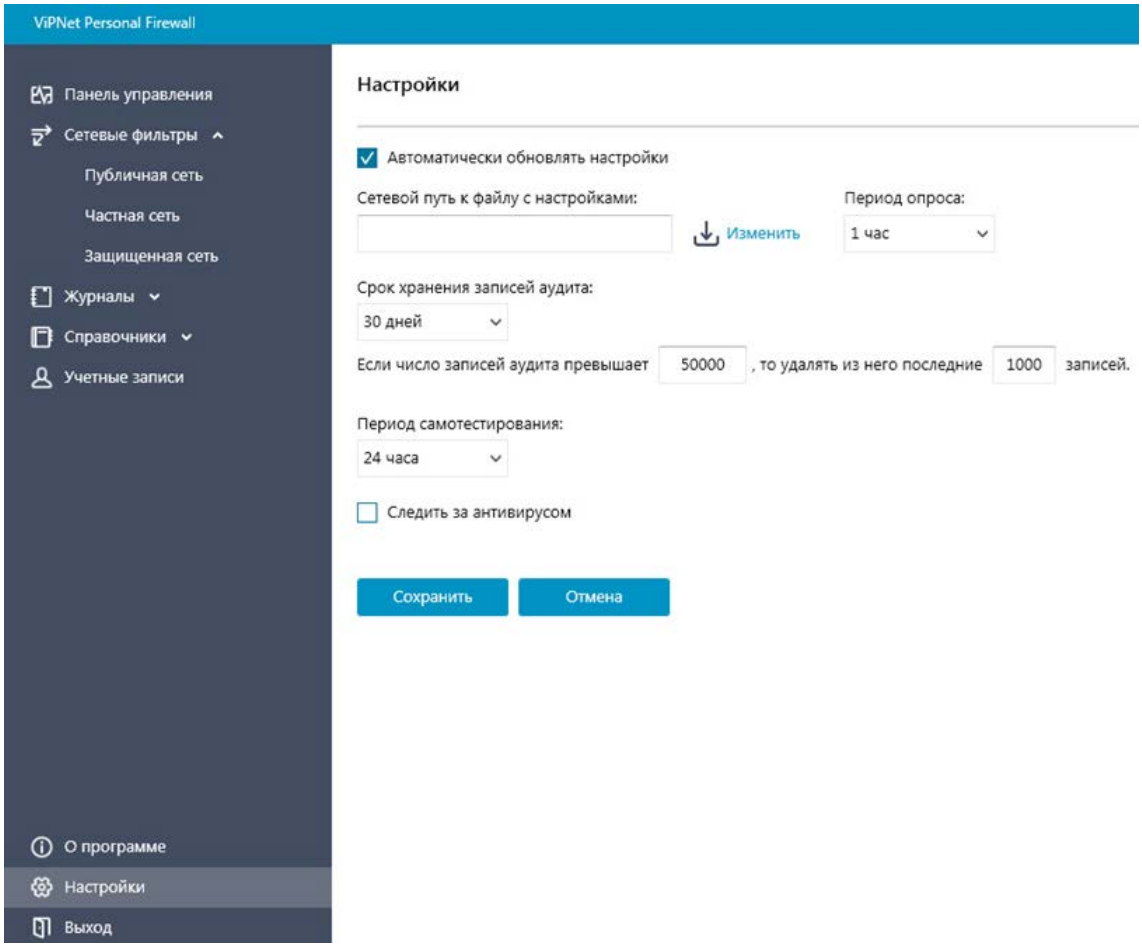

Рисунок 29. Настройка автоматического обновления настроек из файла на сетевом диске

В результате будет включено и настроено автоматическое обновление настроек сетевых фильтров из указанного файла с заданной периодичностью.

4

Мониторинг событий

Отслеживание и блокировка активных соединений 58

Просмотр журнала регистрации трафика и создание сетевых фильтров на основе событий журнала 60

Самотестирование 63

Аудит 65

Отслеживание и блокировка активных соединений

ViPNet Personal Firewall отслеживает сетевую активность приложений, работающих на компьютере. Вы можете просмотреть приложения, которые в настоящий момент работают с сетью (имеют активные соединения), а также посмотреть параметры соединений. При обнаружении подозрительной сетевой активности приложения, вы можете заблокировать его.

Для просмотра информации о приложениях, работающих с сетью, выполните следующие действия:

1 Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора или аудитора (см. Запуск и завершение работы с программой на стр. 20).

2 В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.

3 На панели навигации перейдите в раздел **Журналы** > **Активные соединения.**

4 На странице **Активные соединения** просмотрите список всех приложений, имеющих в настоящий момент активные соединения с сетью. Для просмотра параметров соединений (протокола, локальных и удаленных адресов передачи данных) щелкните значок > перед названием приложения. Параметры соединений отобразятся ниже.

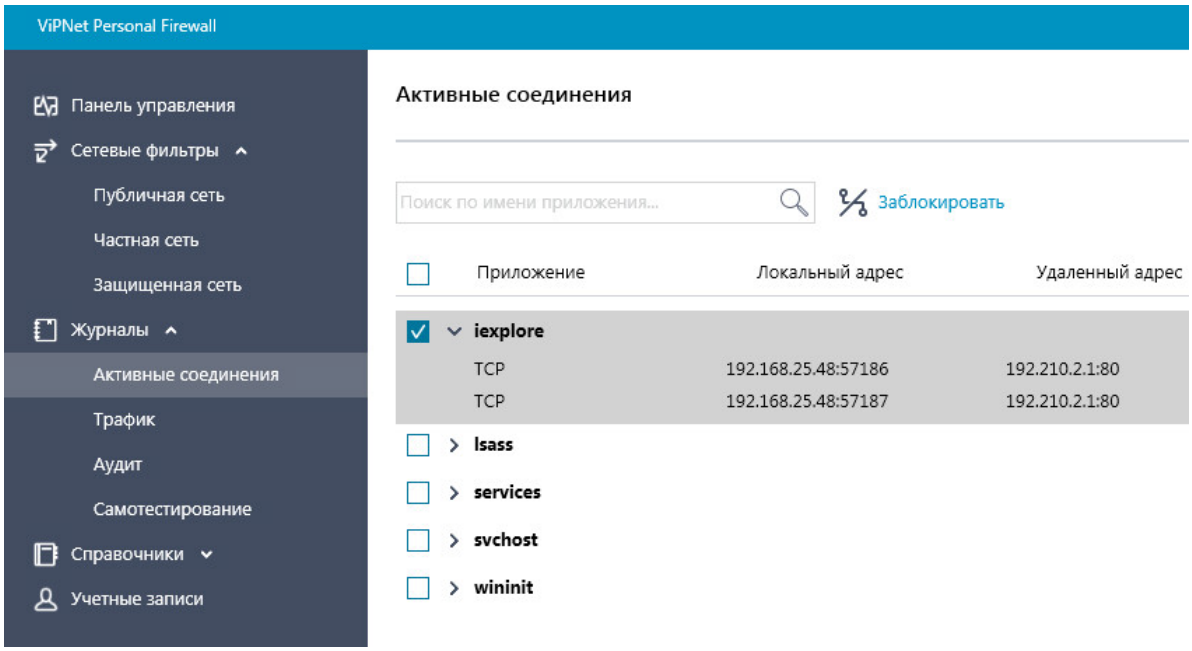

Рисунок 30. Просмотр активных соединений

Чтобы разорвать соединение и заблокировать приложение, установите флажок перед названием нужного приложения, на панели инструментов нажмите **Заблокировать** и подтвердите блокировку.

В результате для выбранного приложения будет разорвано соединение с сетью, а также для режимов **Частная сеть** и **Защищенная сеть** создан сетевой фильтр, полностью блокирующий любые соединения выбранного приложения с сетью. Созданные сетевые фильтры появятся в разделе **Сетевые фильтры** > **Частная сеть** и **Защищенная сеть** в группе **Пользовательские фильтры**.

Внимание! В ViPNet Personal Firewall Linux будет создан сетевой фильтр, блокирующий только текущие сетевые соединения приложения.

Просмотр журнала регистрации трафика и создание сетевых фильтров на основе событий журнала

В ViPNet Personal Firewall ведутся журналы регистрации трафика, проходящего через компьютер и разрешенного либо запрещенного правилами фильтрации. Вы можете на основе различных параметров поиска сформировать отчет о заблокированных и разрешенных IP-пакетах, а также просмотреть время регистрации каждого IP-пакета. Такие отчеты позволяют контролировать трафик компьютера и при необходимости на основе событий журнала создавать дополнительные блокирующие либо разрешающие сетевые фильтры. Это упрощает процесс создания сетевых фильтров.

Для просмотра журнала регистрации трафика выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора или аудитора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **Журналы** > **Трафик**. По умолчанию отобразится информация обо всем зарегистрированном трафике за последние сутки.
4. Для поиска определенных событий в поле поиска введите часть адреса источника или назначения IP-пакета и/или воспользуйтесь фильтром поиска  по наименованию, действию сетевого фильтра, периоду времени.

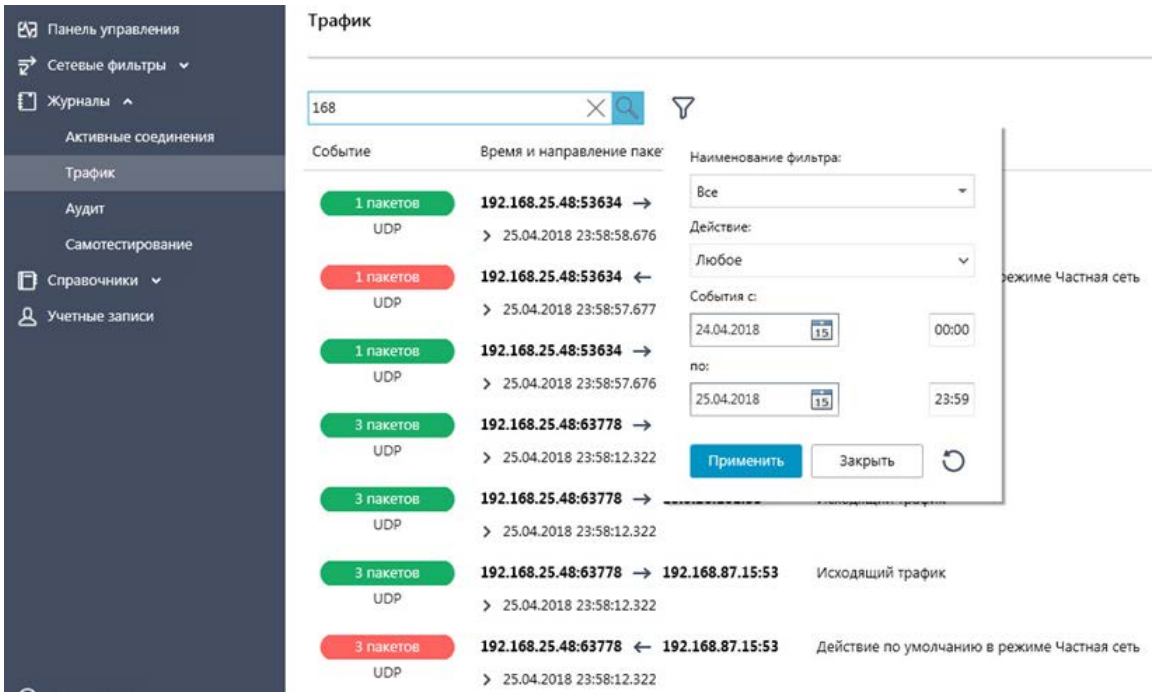

Рисунок 31. Поиск событий в журнале регистрации трафика

В результате будет отображен список событий в соответствии с параметрами поиска.

Каждое событие журнала содержит следующую информацию:

- В столбце **Событие** содержится информация о протоколе передачи и количестве зарегистрированных однотипных IP-пакетов за указанный период времени, а также пропущены (отмечены зеленым цветом) или заблокированы (отмечены красным цветом) данные IP-пакеты.
- В столбце **Время и направление пакетов** содержится информация о направлении (← — входящие IP-пакеты, → — исходящие IP-пакеты), адресах источника и назначения, а также дате и времени регистрации последнего IP-пакета данного типа.
- В столбце **Наименование фильтра** указано название сетевого фильтра, в соответствии с которым было создано событие. В ViPNet Personal Firewall Linux этот столбец называется **Фильтр**.

Чтобы просмотреть информацию о дате и времени регистрации каждого IP-пакета из события, выберите нужное событие и щелкните поле даты и времени регистрации последнего IP-пакета события. В результате событие будет развернуто и вы увидите список дат и времени регистрации нескольких последних IP-пакетов события.

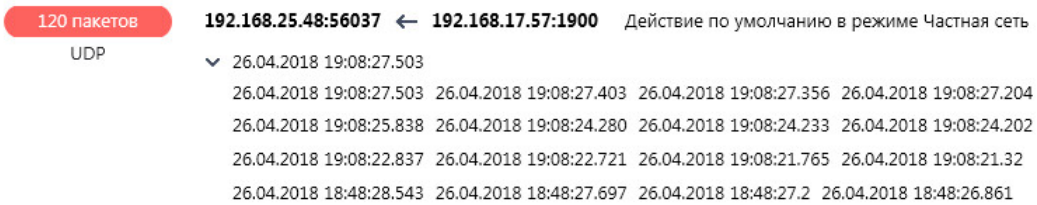

Рисунок 32. Просмотр информации о дате и времени регистрации каждого IP-пакета в событии

Для создания блокирующего или разрешающего сетевого фильтра на основе события выполните следующие действия:

1 Выполните одно из действий:

- Чтобы заблокировать ранее разрешенный сетевыми фильтрами трафик, наведите указатель мыши на строку с нужным событием (с параметрами разрешенного трафика, который вы хотите заблокировать) и нажмите на появившуюся справа кнопку **Заблокировать**.
- Чтобы разрешить ранее заблокированный сетевыми фильтрами трафик, наведите указатель мыши на строку с нужным событием (с параметрами заблокированного трафика, который вы хотите разрешить) и нажмите на появившуюся справа кнопку **Разблокировать**.

Примечание. В ViPNet Personal Firewall Linux для создания фильтра на основе события разверните это событие и нажмите появившуюся кнопку **Разрешить** или **Блокировать**.

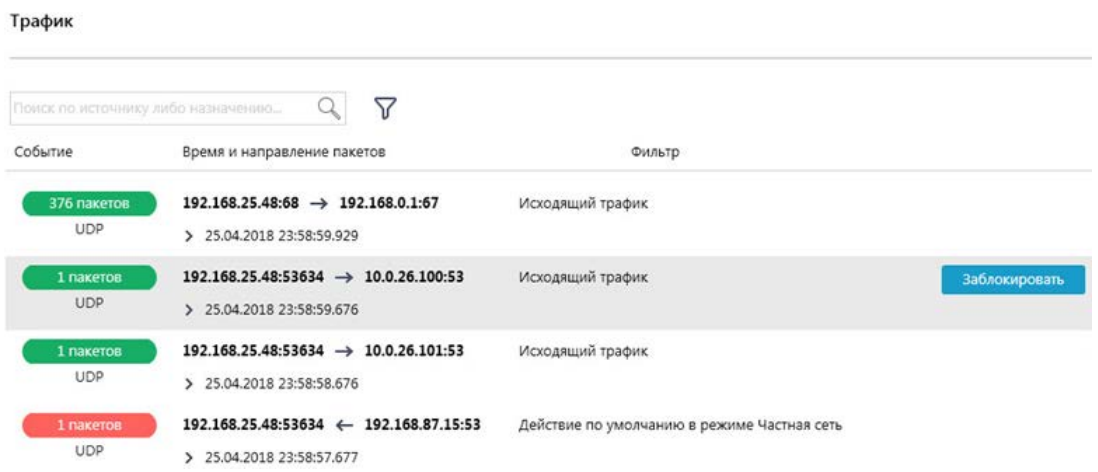

Рисунок 33. Создание блокирующего сетевого фильтра на основе события журнала

2 В окне создания фильтра введите имя фильтра, установите флажки режимов, для которых необходимо создать сетевой фильтр, и нажмите кнопку **Создать**.

В результате будет создан блокирующий или разрешающий фильтр с параметрами из события. Созданные сетевые фильтры появятся в разделе **Сетевые фильтры** > **Частная сеть** и **Защищенная сеть** (в зависимости от выбранных режимов) в группе **Пользовательские фильтры**.

Примечание. В ViPNet Personal Firewall Linux записи журнала по умолчанию хранятся 1 сутки. Записи со сроком хранения более установленного срока автоматически удаляются. Также выполняется автоматическая ротация записей журнала событий при превышении максимального количества записей. По умолчанию при превышении количества записей журнала значения 100000 будут удаляться 1000 самых старых записей. Вы можете изменить срок хранения журнала и параметры автоматической ротации записей журнала (см. Настройка срока хранения и параметров ротации записей журнала аудита на стр. 67) аналогично настройкам ротации журнала аудита.

Самотестирование

В программе ViPNet Personal Firewall реализована процедура самотестирования, которая заключается в контроле корректности работы программы, включая проверку доступности базы данных и целостности журнала. Процедура самотестирования запускается автоматически при запуске ViPNet Personal Firewall и по расписанию один раз в 24 часа. Администратор может изменить период запуска процедуры самотестирования, а также запустить самотестирование вручную, например, для регламентной проверки.

Чтобы провести проверку работоспособности ViPNet Personal Firewall, выполните следующие действия:

1 Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).

2 В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.

3 На панели навигации перейдите в раздел **Журналы** > **Самотестирование**.

4 На странице **Самотестирование** нажмите **Запустить самотестирование**.

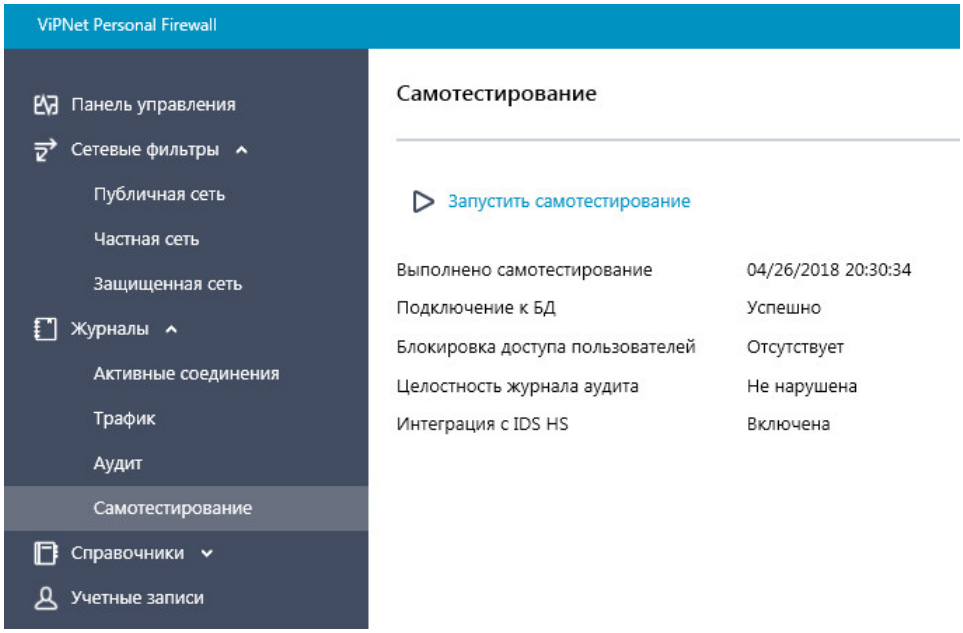

Рисунок 34. Запуск самотестирования

По окончании проверки отобразится информация о текущем состоянии ViPNet Personal Firewall.

Чтобы изменить период автоматического запуска самотестирования, выполните следующие действия:

1 Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора.

2 В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.

3 На панели навигации перейдите в раздел **Настройки**.

4 На странице **Настройки** в списке **Период самотестирования** выберите необходимый период (от 5 минут до 24 часов). В ViPNet Personal Firewall Linux период самотестирования задается в днях.

5 Нажмите **Сохранить**.

В результате самотестирование будет автоматически запускаться через заданный период времени.

Аудит

В программе ViPNet Personal Firewall обеспечивается аудит всех событий, которые могут повлиять на безопасность и работоспособность программы. Все действия, производимые пользователями в ViPNet Personal Firewall, а также системные события ViPNet Personal Firewall фиксируются в журнале событий аудита. В журнале событий аудита содержится вся необходимая информация для анализа нарушений, связанных с безопасностью системы. Эта информация позволяет определить, каким пользователем было инициировано то или иное действие.

Просмотр журнала аудита (на стр. 65) доступен только пользователям с ролями администратора и аудитора.

В журнале регистрируются следующие категории событий:

- События аутентификации пользователя и выхода из системы.
- Действия с учетными записями — создание, изменение параметров учетной записи, удаление.
- Запуск и завершение самотестирования.
- События журнала аудита — переполнение журнала аудита и удаление записей.
- Изменение настроек ViPNet Personal Firewall.
- Запуск и останов службы ViPNet Personal Firewall.
- Изменение режима работы ViPNet Personal Firewall.
- Включение и отключение блокировки трафика при слежении за антивирусом.
- Действия с сетевыми фильтрами — добавление, изменение, удаление сетевого фильтра.
- Действия со справочниками — добавление, изменение, удаление адресов, протоколов или расписаний в справочнике.
- Экспорт и импорт конфигурации — выгрузка настроек в файл и загрузка из файла.

По умолчанию записи журнала аудита хранятся 30 дней (в ViPNet Personal Firewall Linux — 1 сутки). Записи со сроком хранения более установленного срока автоматически удаляются. Также выполняется автоматическая ротация записей журнала событий при превышении максимального количества записей. По умолчанию при превышении количества записей журнала значения 50000 (в ViPNet Personal Firewall Linux — 10000) будут удаляться 1000 (в ViPNet Personal Firewall Linux — 2000) самых старых записей. Вы можете изменить срок хранения журнала и параметры автоматической ротации записей журнала (см. Настройка срока хранения и параметров ротации записей журнала аудита на стр. 67).

Просмотр журнала аудита

Для просмотра журнала аудита выполните следующие действия:

1 Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора или аудитора (см. Запуск и завершение работы с программой на стр. 20).

2 В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.

3 На панели навигации перейдите в раздел **Журналы** > **Аудит**. По умолчанию отобразится информация обо всех событиях за последние сутки.

Каждое событие журнала содержит следующую информацию:

- Дату и время регистрации события.
- Наименование события.
- Имя учетной записи пользователя, инициировавшего событие.
- Объект, на который направлено действие.

4 Для поиска определенных событий в поле поиска введите часть наименования события, имени инициатора или объекта действия и/или воспользуйтесь фильтром поиска по инициализатору, наименованию события, периоду времени.

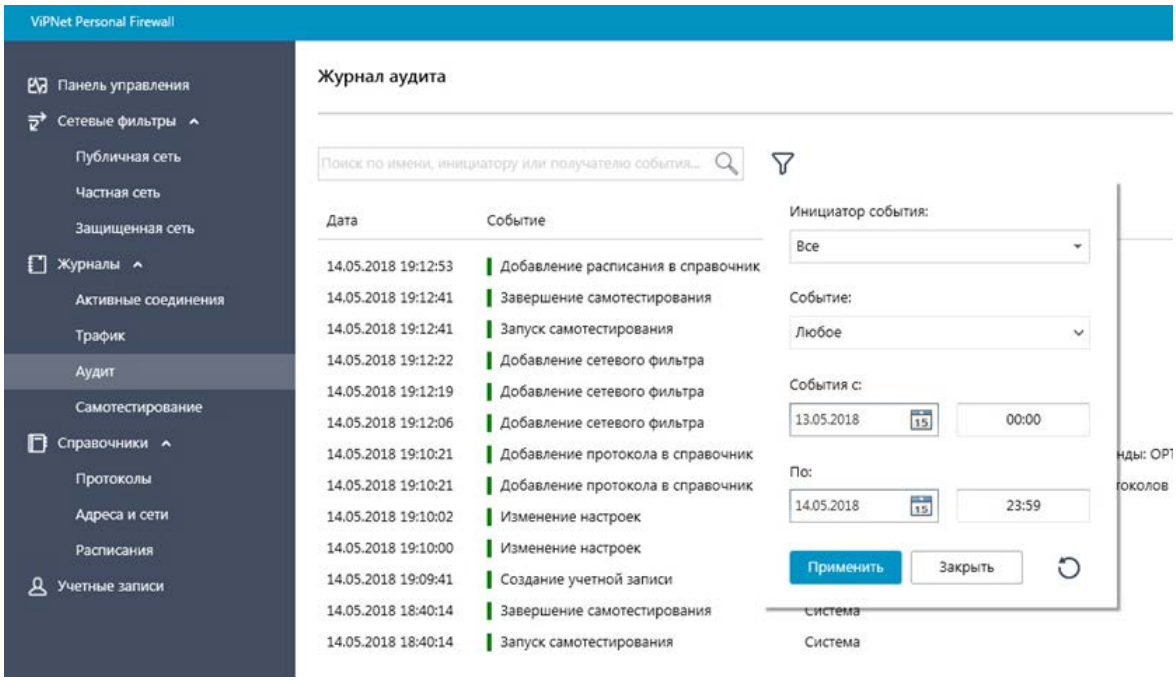

Рисунок 35. Поиск событий в журнале аудита

В результате будет отображен список событий в соответствии с параметрами поиска.

Для удобства просмотра информации доступны следующие возможности:

- Изменение порядка расположения столбцов путем их перетаскивания.
- Сортировка по любому из отображаемых столбцов (по возрастанию или убыванию). Для этого нужно щелкнуть заголовок нужного столбца.

Примечание. В ViPNet Personal Firewall Linux возможность изменения порядка столбцов и сортировки столбцов отсутствует.

Настройка срока хранения и параметров ротации записей журнала аудита

Чтобы изменить срок хранения записей журнала и/или параметры автоматической ротации записей журнала, выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора или аудитора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **Настройки**.
4. На странице **Настройки** в списке **Срок хранения записей аудита** выберите необходимый срок хранения (30, 60 или 90 дней). В ViPNet Personal Firewall Linux срок хранения записей аудите задается в минутах.
5. В следующей строке при необходимости измените параметры ротации (см. Аудит на стр. 65): количество записей, при достижении которого начнут удаляться старые записи журнала, а также количество удаляемых старых записей.

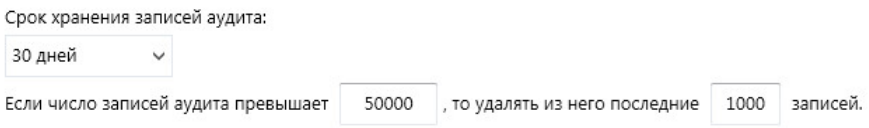

Рисунок 36. Настройка параметров журнала аудита

6. Нажмите **Сохранить**.

В результате к записям журнала аудита будут применяться новые настройки срока хранения и параметров ротации.

5

Управление и настройка ViPNet Personal Firewall

Настройка блокировки трафика при отключении защитного функционала антивируса 69

Управление учетными записями пользователей 70

Обновление лицензии 73

Настройка блокировки трафика при отключении защитного функционала антивируса

Если на вашем компьютере установлен антивирус Kaspersky Endpoint Security 10, то для обеспечения более надежной защиты вашего компьютера вы можете настроить программу ViPNet Personal Firewall таким образом, чтобы она контролировала наличие работающего антивируса. В этом случае при отключении защитного функционала антивируса будет заблокирован весь входящий и исходящий трафик компьютера. По умолчанию настройка блокировки трафика отключена.

Перед настройкой ViPNet Personal Firewall произведите настройку Kaspersky Endpoint Security 10 таким образом, чтобы следующие события антивируса сохранялись в журнале событий операционной системы (см. документацию к Kaspersky Endpoint Security 10):

- Автозапуск программы выключен.
- Черный список ключей поврежден или не найден.
- Не удалось выполнить задачу.
- Самозащита программы выключена.
- Компоненты защиты выключены.
- Задача остановлена.
- Продукт остановлен.

Чтобы настроить блокировку трафика при отключении защитного функционала антивируса, выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **Настройки**.
4. На странице **Настройки** установите флажок **Следить за антивирусом**.
5. Нажмите **Сохранить**.

В результате в ViPNet Personal Firewall будут отслеживаться перечисленные выше события антивируса и при их обнаружении осуществляться блокировка трафика компьютера (ViPNet Personal Firewall будет переведен в режим работы **Полная блокировка трафика**).

Управление учетными записями пользователей

Первая учетная запись для входа в ViPNet Personal Firewall с ролью администратора была создана при установке ViPNet Personal Firewall. В процессе работы вы можете создать нужное количество учетных записей и назначить им необходимые роли (см. Разграничение полномочий на основе ролей на стр. 13). Также вы можете изменять параметры ранее созданных учетных записей (например, изменить роль или пароль) и удалять ненужные учетные записи.

Для создания учетной записи выполните следующие действия:

1 Войдите в программу ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).

2 В окне **Панель управления** щелкните ссылку **Показать экспертные настройки**.

3 На панели навигации перейдите в раздел **Учетные записи**.

4 На панели инструментов страницы **Учетные записи** нажмите кнопку **Создать запись**.

5 В окне **Новая учетная запись** выполните следующие действия:

5.1 В поле **Наименование** введите имя пользователя (например, имя и фамилию).

5.2 В поле **Учетная запись** введите имя учетной записи.

5.3 Задайте роль пользователя, установив переключатель **Полномочия** в нужное положение.

5.4 В поле **Пароль** введите пароль пользователя.

Внимание! Пароль должен соответствовать следующим требованиям:

- Минимальная длина — 8 символов.
- Любые идущие подряд три символа пароля не должны совпадать с частью имени учетной записи.
- Один и тот же символ не должен встречаться более двух раз.

В пароле должны одновременно присутствовать символы четырех категорий:

- прописные буквы английского алфавита от A до Z,
- строчные буквы английского алфавита от a до z,
- десятичные цифры от 0 до 9,
- символы, не принадлежащие алфавитно-цифровому набору (например, @,#, $ и другие).

5.5 Снимите флажок **Использовать простой пароль**.

Внимание! Вы можете установить флажок **Использовать простой пароль** и в поле **Пароль** указать любой пароль, но из соображений безопасности мы не рекомендуем вам использовать простые пароли.

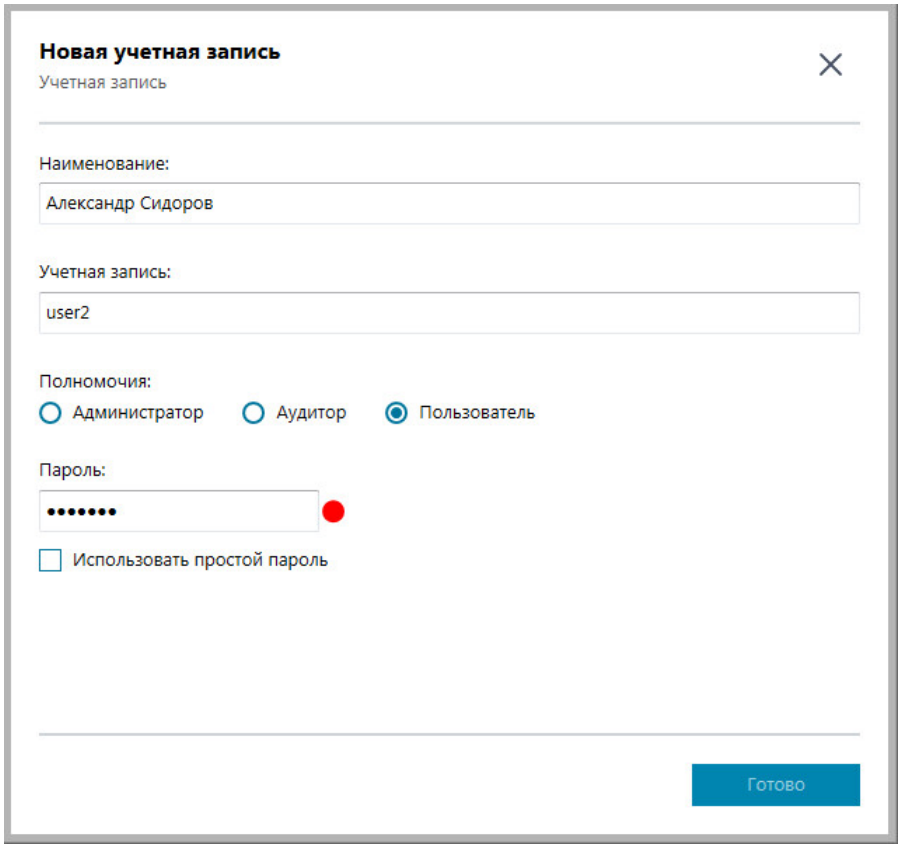

Рисунок 37. Создание учетной записи

5.6 Нажмите кнопку **Готово**.

В результате будет создана новая учетная запись. Учетная запись отобразится в списке на странице **Учетные записи**.

Чтобы изменить параметры или удалить учетную запись, два раза щелкните нужную учетную запись и на появившейся панели выполните одно из следующих действий:

- Для изменения параметров учетной записи задайте новые параметры аналогично описанию выше и нажмите **OK**. Для изменения пароля предварительно нажмите кнопку **Изменить**.

Примечание. В ViPNet Personal Firewall Linux для изменения пароля сразу введите новый пароль в поле **Пароль**.

- Для удаления учетной записи нажмите кнопку **Удалить**.

Примечание. Вы можете удалить сразу несколько учетных записей, для этого установите флажки перед строками нужных учетных записей и на появившейся панели нажмите кнопку **Удалить**.

Обновление лицензии

Если у лицензии закончился срок действия, вам необходимо ее обновить. Для получения лицензии обратитесь в отдел продаж ОАО "ИнфоТеКС".

Чтобы обновить лицензию, выполните следующие действия:

1. Войдите в консоль управления программой ViPNet Personal Firewall под учетной записью администратора (см. Запуск и завершение работы с программой на стр. 20).
2. В нижней части окна **Режимы работы** щелкните ссылку **Показать экспертные настройки**.
3. На панели навигации перейдите в раздел **О программе**.
4. На вкладке **Данные** нажмите кнопку **Загрузить другую лицензию** и выберите файл лицензии (`*.itcslic`).

В результате после проверки лицензия будет установлена и на странице **О программе** отобразится информация о лицензии.

A

Глоссарий

IP-адрес

Адрес узла в сети, построенной на основе протокола IP.

MAC-адрес

В большинстве технологий локальных сетей для однозначной адресации интерфейсов используются MAC-адреса (Media Access Control — управление доступом к среде). MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне, которую используют протоколы сетевого уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, протокол разрешения адресов — Address Resolution Protocol, ARP).

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Доверенная зона

Доверенная зона содержит сетевые узлы, которые считаются безопасными друг для друга. Понятие доверенной зоны определяется политикой безопасности организации, эксплуатирующей ViPNet

Personal Firewall. Например, доверенной зоной может считаться периметр помещения, в котором установлен ViPNet Personal Firewall.

Журнал событий

Файл или группа файлов, предназначенных для хранения сведений о событиях программы.

Локальная сеть (LAN)

Группа компьютеров и других устройств, размещенных на относительно небольшом пространстве и соединенных линиями связи, которые позволяют любому устройству взаимодействовать с любым другим устройством в этой сети.

Персональный сетевой экран

Программное обеспечение, осуществляющее контроль сетевой активности компьютера, а также фильтрацию трафика в соответствии с заданными сетевыми фильтрами. В отличие от межсетевого экрана, персональный сетевой экран устанавливается непосредственно на защищаемом компьютере и позволяет пользователям индивидуально настраивать необходимые сетевые фильтры.

Сетевая атака

Компьютерная атака с использованием протоколов межсетевого взаимодействия.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN.

Сетевой порт

Системный ресурс, выделяемый приложению для соединения и обмена данными с другими приложениями, выполняемыми на этом же или других узлах, доступных через сеть. Позволяет различным программам, выполняемым на одном узле, получать данные независимо друг от друга (предоставлять сетевые сервисы). Каждая программа обрабатывает данные, поступающие на определенный сетевой порт.

Сетевой протокол

Набор правил, позволяющий осуществлять соединение и обмен данными между двумя и более включенными в сеть устройствами.

Сетевой фильтр

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