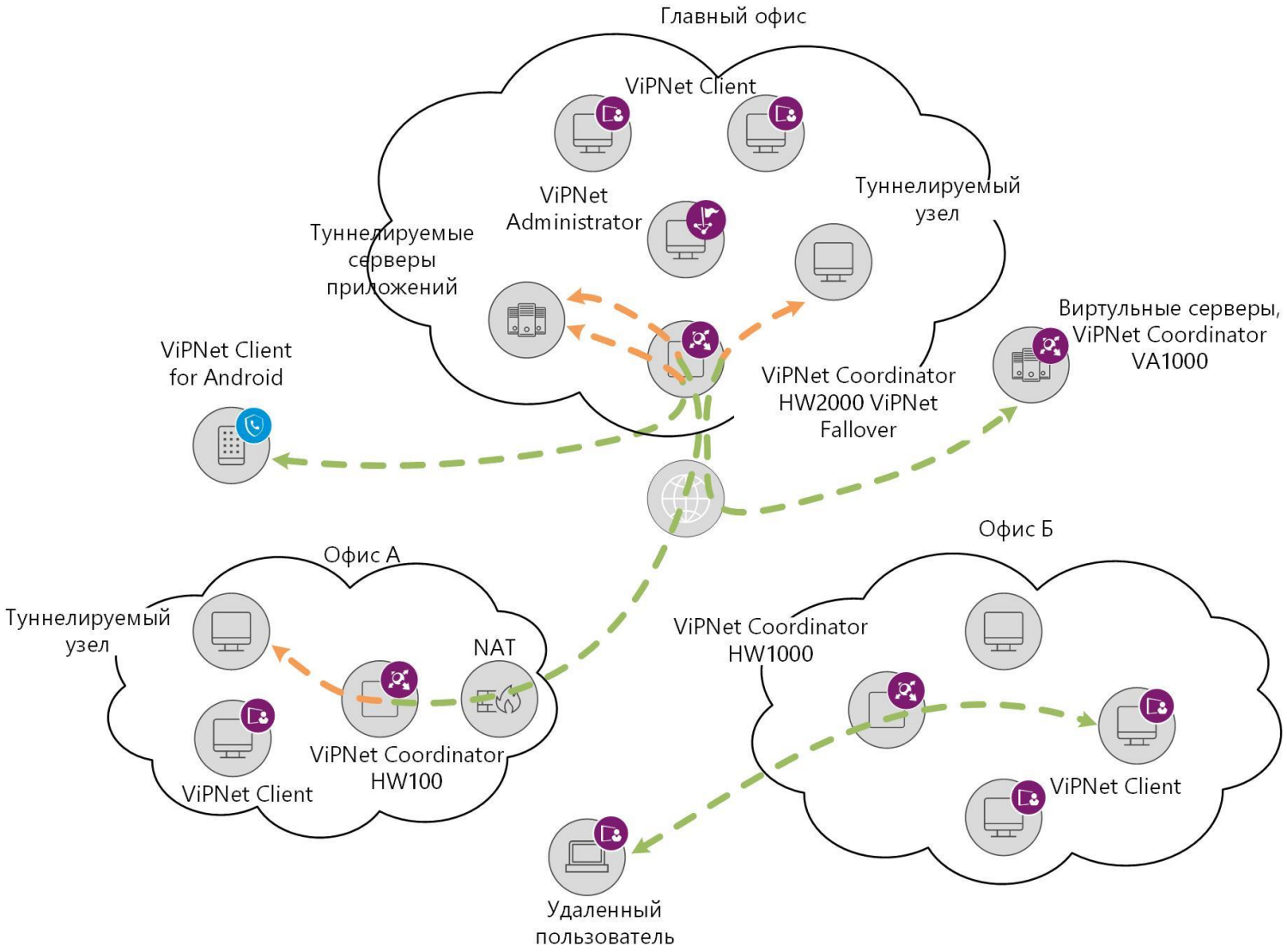
ViPNet Coordinator 4.x

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru

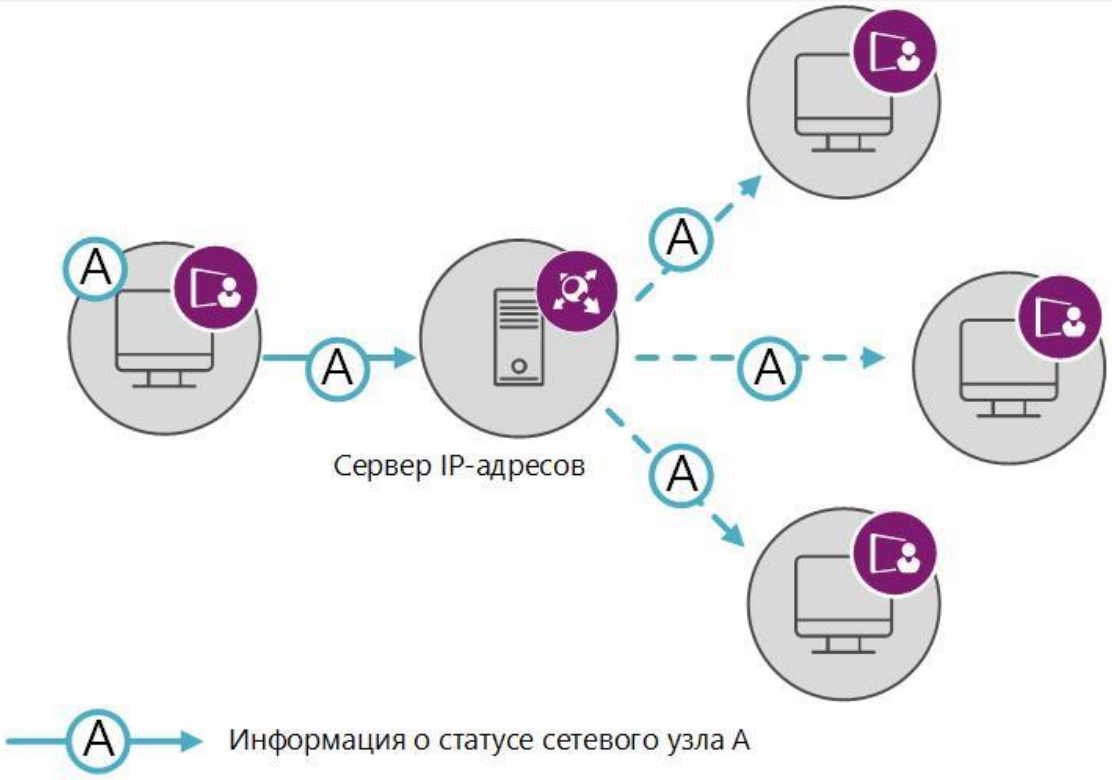
Пример использования компонентов сети ViPNet в крупной компании



Функции ViPNet Coordinator 4.x

Сервер IP-адресов

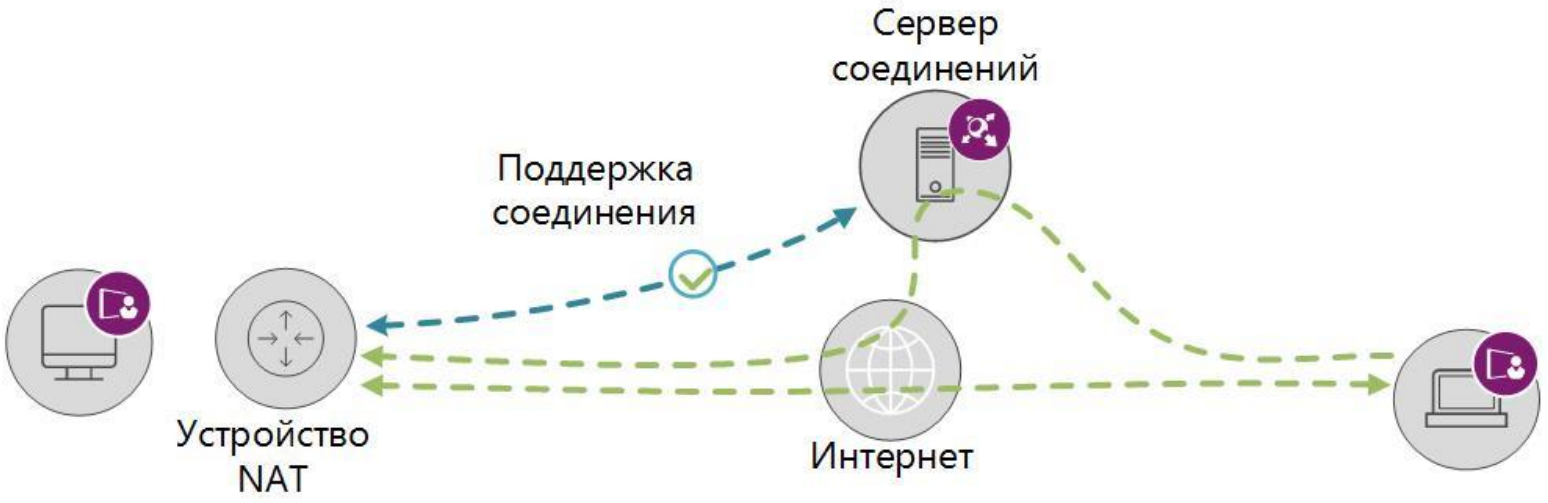
- отправляет на сетевые узлы информацию о параметрах подключения и о состоянии всех узлов, с которыми у данного узла имеется связь;



Функции ViPNet Coordinator 4.x

Сервер соединений

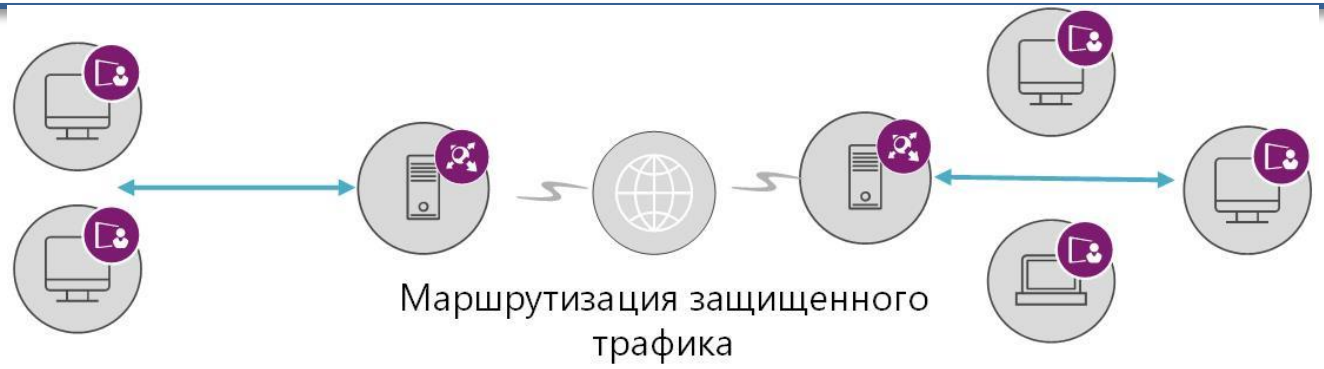
- устанавливать соединения между клиентами и координаторами по кратчайшему пути, если они находятся в разных подсетях и не могут соединиться друг с другом напрямую;
- для каждого клиента может быть назначен свой сервер соединений;
- по умолчанию сервер соединений для клиента служит также сервером IP-адресов. Для координаторов также при необходимости может быть выбран сервер соединений.



Функции ViPNet Coordinator 4.x

Маршрутизатор VPN-пакетов

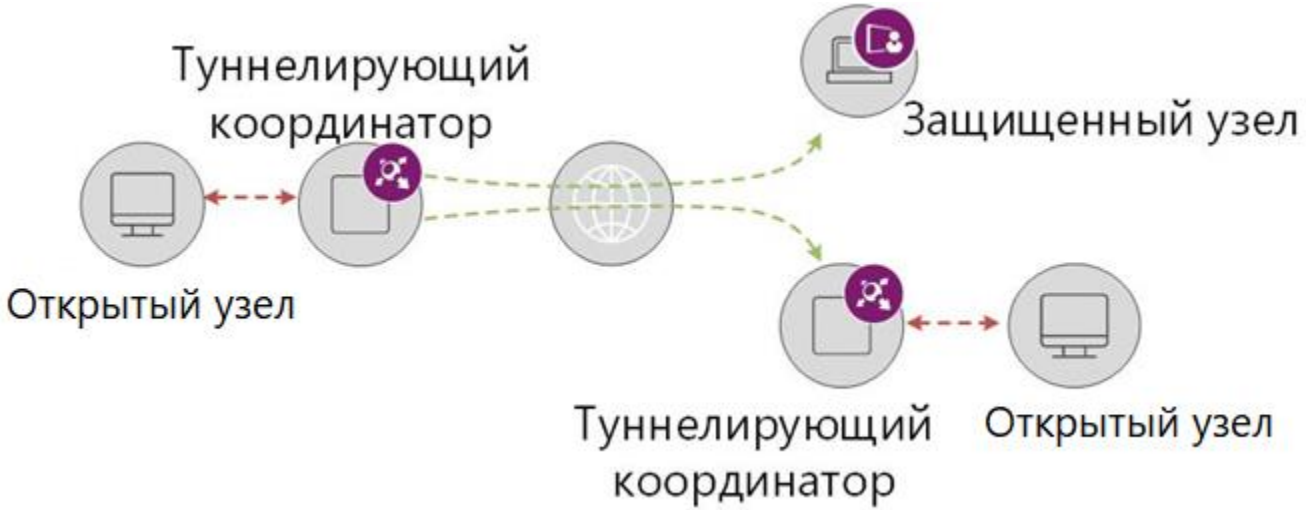
- обеспечивает маршрутизацию транзитного защищенного трафика, проходящего через координатор, на другие защищенные узлы;
- маршрутизация осуществляется на основании :
  - идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов;
  - защищенного протокола динамической маршрутизации трафика;
- для защищенного трафика выполняется трансляция адресов (NAT). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора.



Функции ViPNet Coordinator 4.x

VPN-шлюз

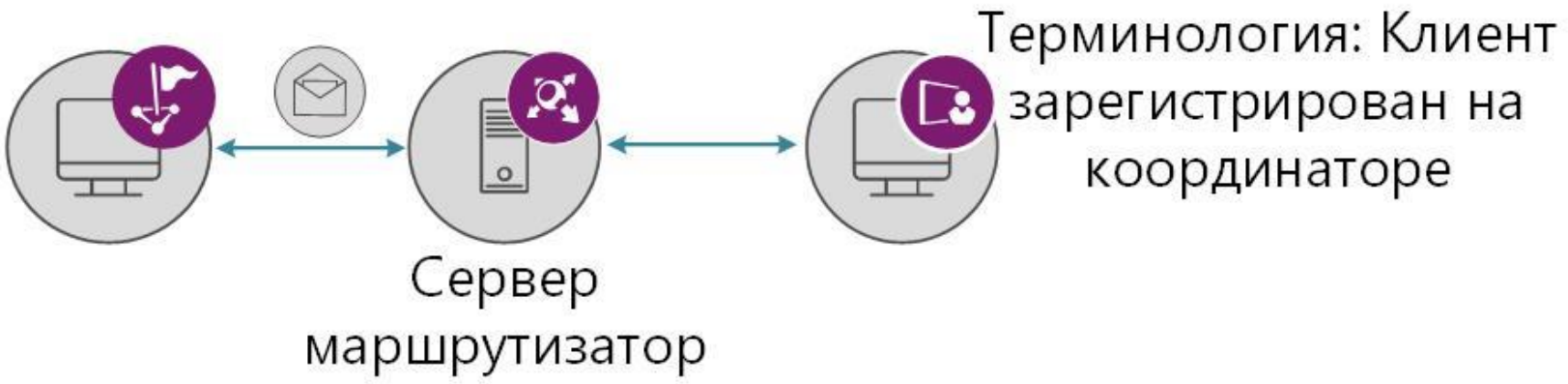
- позволяет создавать защищенные каналы (туннели) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты;
- VPN-шлюз интегрирован с межсетевым экраном для защищенных и открытых соединений, осуществляющим фильтрацию незашифрованного трафика, а также трафика внутри защищенного соединения.



Функции ViPNet Coordinator 4.x

Сервер-маршрутизатор

- позволяет доставить на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью, а также обмен прикладными транспортными конвертами между узлами;
- маршрутизация прикладных и управляющих конвертов осуществляется с помощью транспортного модуля ViPNet MFTP, работающего на прикладном уровне.



Функции ViPNet Coordinator 4.x

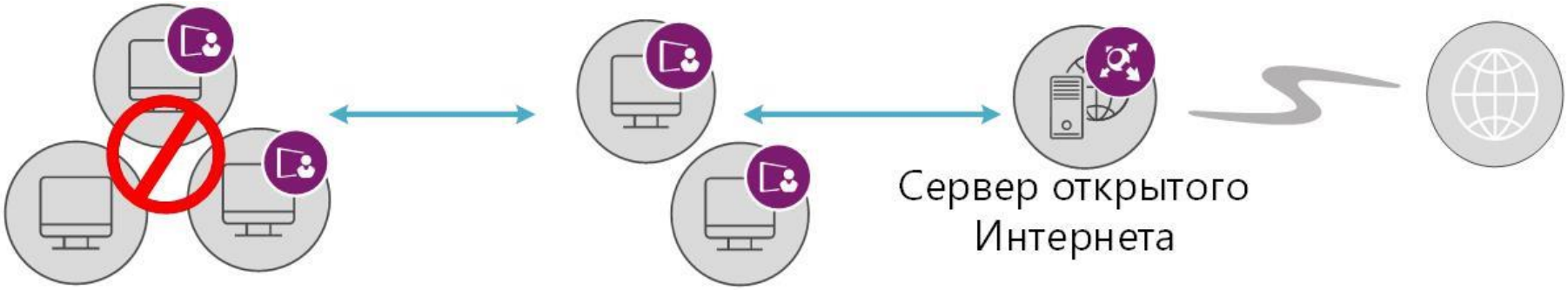
Межсетевой экран

- выполняет фильтрацию открытых, транзитных и локальных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил;
- осуществляет трансляцию адресов (NAT) для проходящего через координатор открытого трафика. Позволяет задать правила трансляции адресов для решения двух основных задач:
  - подключение локальной сети к открытым ресурсам Интернета, когда количество узлов локальной сети превышает количество публичных IP-адресов, выданных поставщиком услуг Интернета;
  - организация доступа к открытым серверам локальной сети из Интернета.

Функции ViPNet Coordinator 4.x

Сервер открытого Интернета

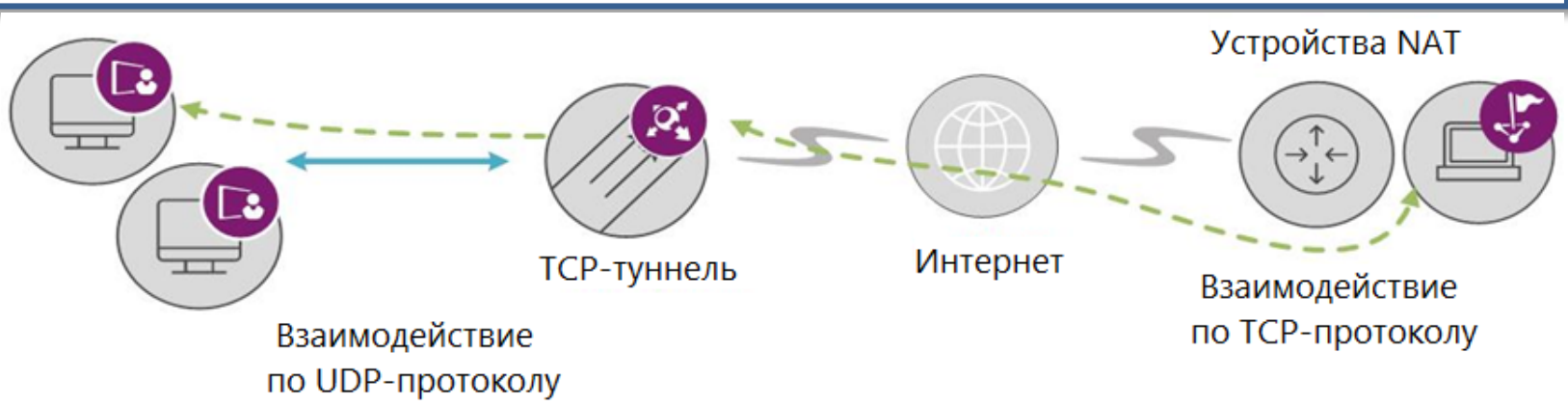
- позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации. Защищенные узлы, которые имеют связь с сервером открытого Интернета, могут работать в одном из двух режимов:
  - доступ к защищенной сети ViPNet при отсутствии подключения к Интернету;
  - доступ в Интернет при отсутствии соединения с защищенными узлами ViPNet.



Функции ViPNet Coordinator 4.x

TCP-туннель

- осуществляет соединение клиентов, находящихся во внешних сетях, с другими узлами сети ViPNet, в том случае, если при подключении клиентов к внешним сетям интернет-провайдером блокируется UDP-протокол;
- если удаленный клиент не может связаться с другими узлами по протоколу UDP, и на его сервере соединений при этом настроен TCP-туннель, он автоматически начинает устанавливать с узлами соединение через TCP-туннель сервера соединений. На сервере соединений полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.



Новые возможности ViPNet Coordinator 4.x

реализована установка ViPNet Coordinator с помощью установочного пакета MSI и сценария входа в систему logon script;

функции криптопровайдера выполняет отдельная программа ViPNet CSP;

мастер первичной инициализации больше не используется. Все сценарии, связанные с установкой или заменой ключей выполняет Мастер установки ключей;

все обновления происходят через систему обновления ViPNet;

реализована возможность централизованного управления политиками безопасности через программу ViPNet Policy Manager;

Новые возможности ViPNet Coordinator 4.x

реализована возможность создания групп объектов;

реализована возможность автоматической смены конфигураций;

изменился порядок применения сетевых фильтров и правил трансляции IP-адресов;

режимы безопасности больше не используются;

обеспечена интеграция с программой ViPNet SafeDisk-V;

Новые возможности ViPNet Coordinator 4.x

разработан новый формат сетевых фильтров в программе ViPNet Монитор;

реализована возможность создавать в журнале IP-пакетов как разрешающие, так и блокирующие фильтры;

настройка антиспуфинга больше не требуется. Фильтры формируются автоматически на основе таблицы маршрутизации сетевого узла;

при создании правила трансляции IP-адресов в одном правиле можно задать трансляцию как источника, так и назначения IP-пакетов;

при передаче конвертов по каналу SMTP/POP3 появилась возможность разбивать конверты на фрагменты.

Состав ViPNet Coordinator 4.x

Драйвер сетевой защиты ViPNet-драйвер:

- осуществляет шифрование и фильтрацию IP-трафика;
- перехватывает и контролирует весь IP-трафик, поступающий и исходящий из компьютера;
- взаимодействует непосредственно с драйверами сетевых интерфейсов компьютера, что обеспечивает независимость программы от операционной системы и ее недокументированных возможностей;
- обеспечивает эффективный контроль IP-трафика во время загрузки операционной системы и первым получает контроль над стеком протоколов TCP/IP.

Состав ViPNet Coordinator 4.x

ViPNet Монитор:

- является интерфейсом для управления ViPNet-драйвером;
- позволяет настраивать параметры встроенного сетевого экрана;
- позволяет управлять параметрами обработки прикладных протоколов;
- предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена.

Сервис управления драйвером защиты ViPNet:

- обеспечивает загрузку в ViPNet-драйвер справочной информации о структуре сети, правил фильтрации и ключей шифрования;
- обеспечивает прием и передачу на другие сетевые узлы информации о состоянии узла и параметрах доступа;
- обеспечивает ведение журнала IP-пакетов.

Состав ViPNet Coordinator 4.x

Транспортный модуль ViPNet MFTP:

- обеспечивает обмен управляющей, адресной и ключевой информацией с программой ViPNet Центр управления сетью или ViPNet Network Manager;
- реализует в координаторе функцию сервера-маршрутизатора почтовых конвертов.

Криптопровайдер ViPNet CSP:

- обеспечивает формирование и проверку электронной подписи;
- обеспечивает шифрование данных, в том числе сообщений электронной почты;
- обеспечивает аутентификацию и защиту соединений по протоколу TLS/SSL.

Состав ViPNet Coordinator 4.x

ViPNet Контроль приложений:

- отслеживает сетевую активностью приложений, установленных на компьютере, а именно:
  - попытки создания исходящих соединений;
  - попытки открытия портов для входящих соединений;
  - отправку пакетов без предварительного создания соединения
- ограничивает (разрешает или запрещает) доступ приложений к сети;
- ведет журнал событий по сетевой активности приложений.

Система обновления ViPNet:

- обеспечивает получение и установку программных обновлений, справочников и ключей из программы ViPNet Administrator, а также обновлений политик безопасности ViPNet Policy Manager.

Установка ViPNet Coordinator

Режимы установки ViPNet Coordinator

- **Установка с использованием Microsoft System Center**
  - позволяет формировать пакеты, содержащие в себе установочные файлы MSI, и публиковать их на сервере обновлений для рассылки на компьютеры домена
- **Установка с использованием сценария входа в систему (logon script)**
  - позволяет установить ПО ViPNet одновременно на любое количество компьютеров в домене Windows
- **Неинтерактивный режим установки**
  - позволяет выполнять удаленную установку и создавать программы, обращающиеся к командной строке Windows и запускающие автоматическую установку ПО ViPNet Client или ViPNet Coordinator с заданными параметрами
- **Интерактивный режим установки**

Установка ViPNet Coordinator

Для установки ViPNet Coordinator требуется:

установочный EXE-файл ПО ViPNet Coordinator;

дистрибутив ключей для сетевого узла (файл *.dst);

******* пароль пользователя сетевого узла;

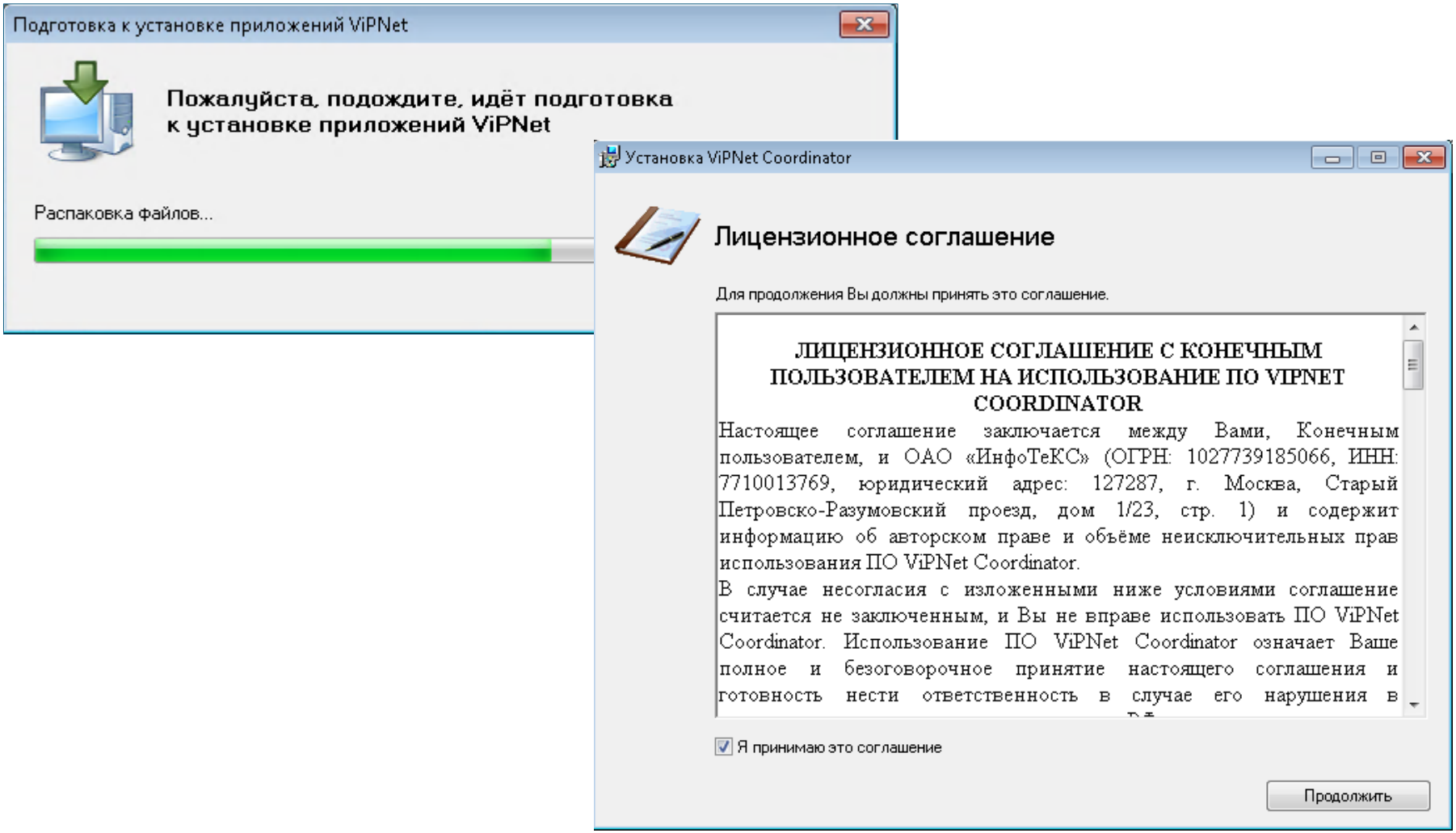
права администратора в операционной системе;

отключить сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT);

убедиться, что на компьютере правильно заданы часовой пояс, дата и время.

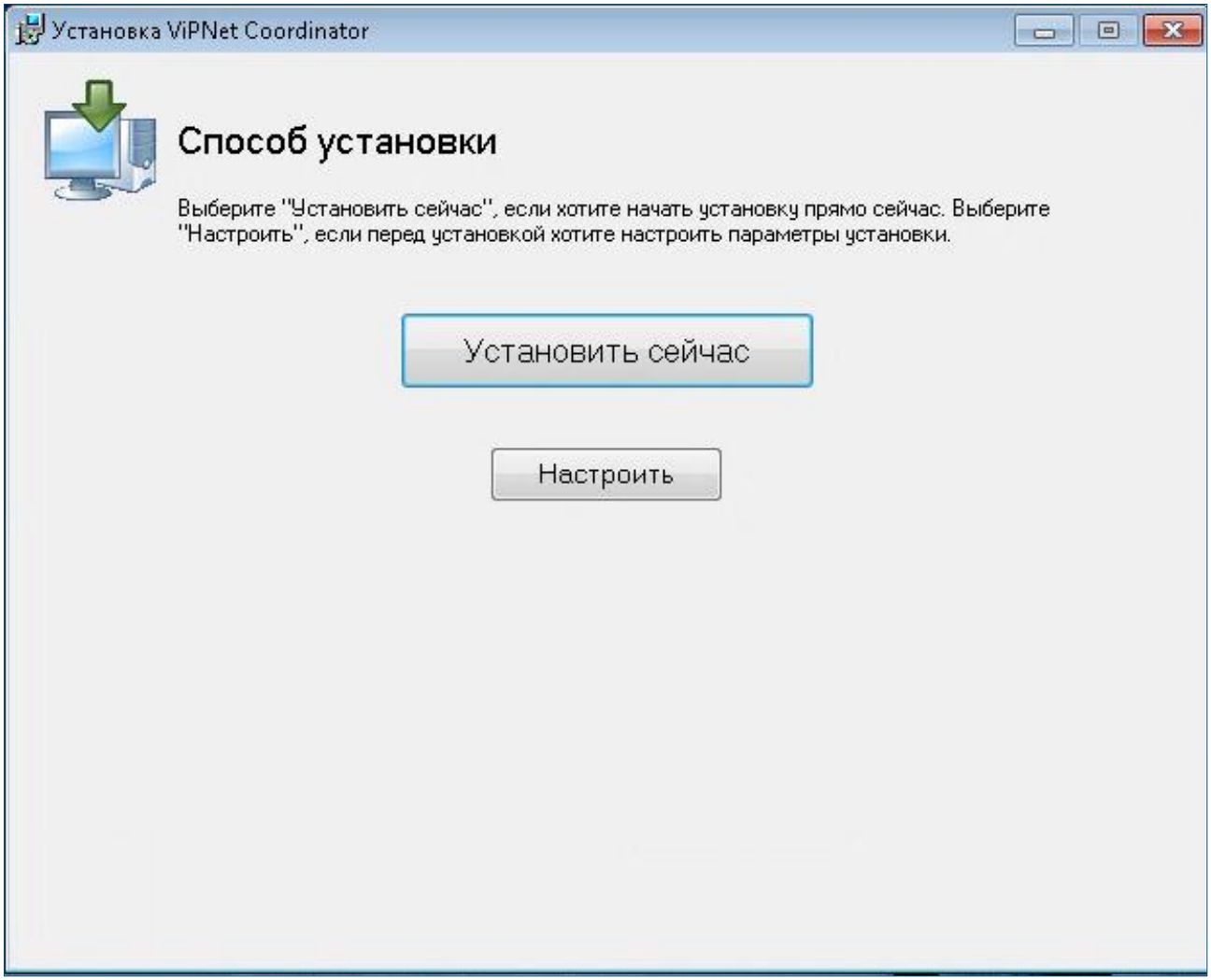
Установка ViPNet Coordinator

Установка в интерактивном режиме



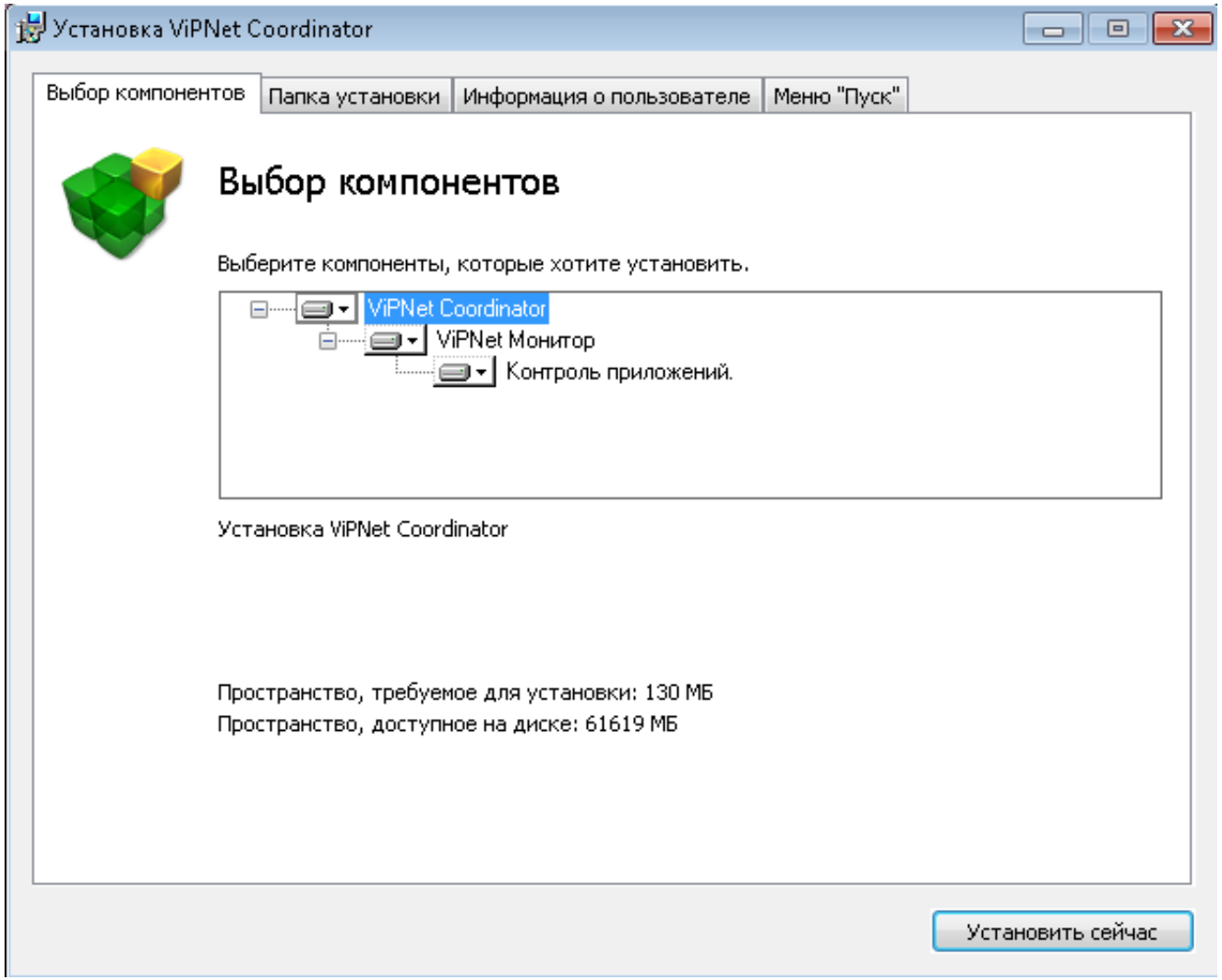
Установка ViPNet Coordinator

Установка в интерактивном режиме



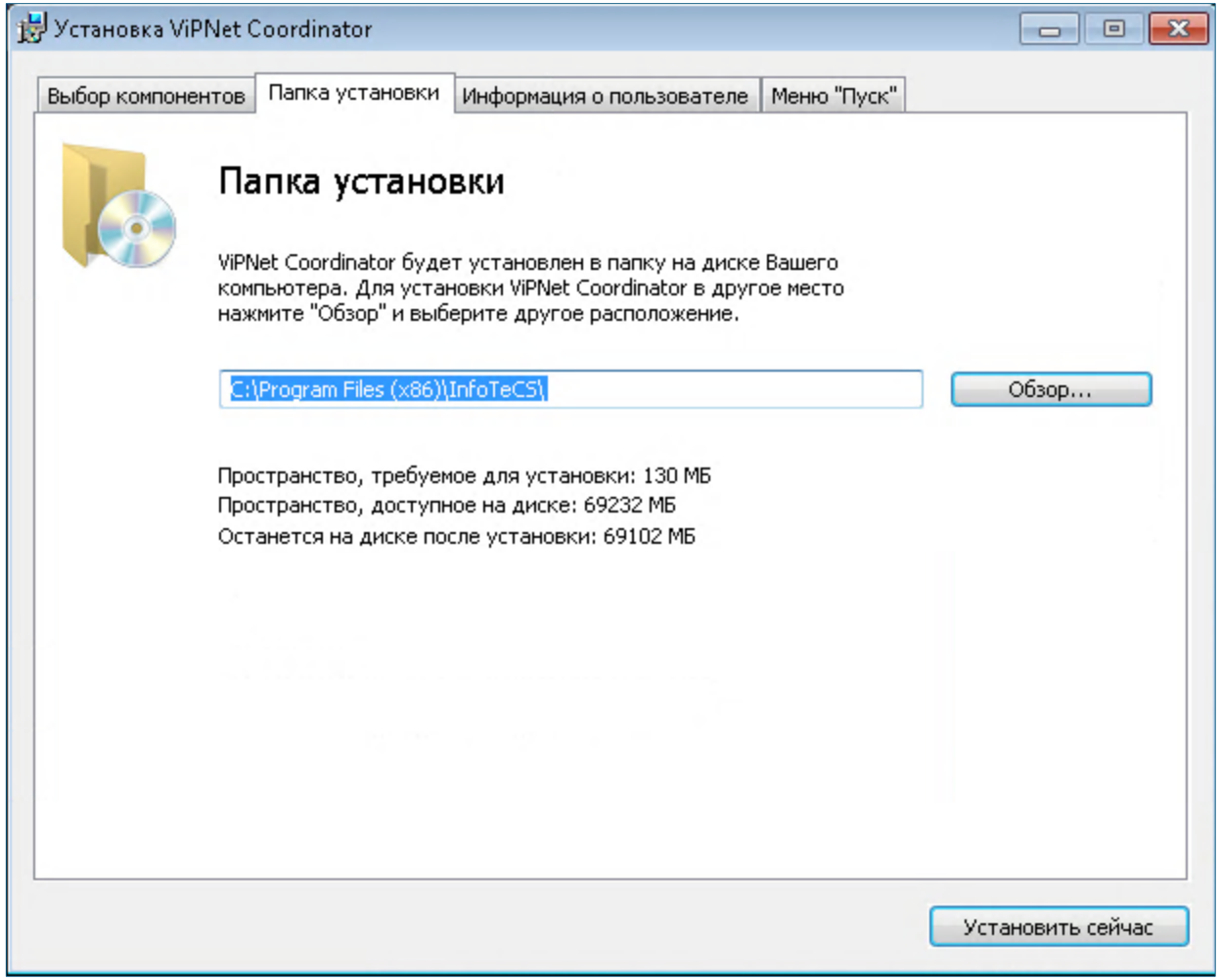
Установка ViPNet Coordinator

Дополнительные параметры установки



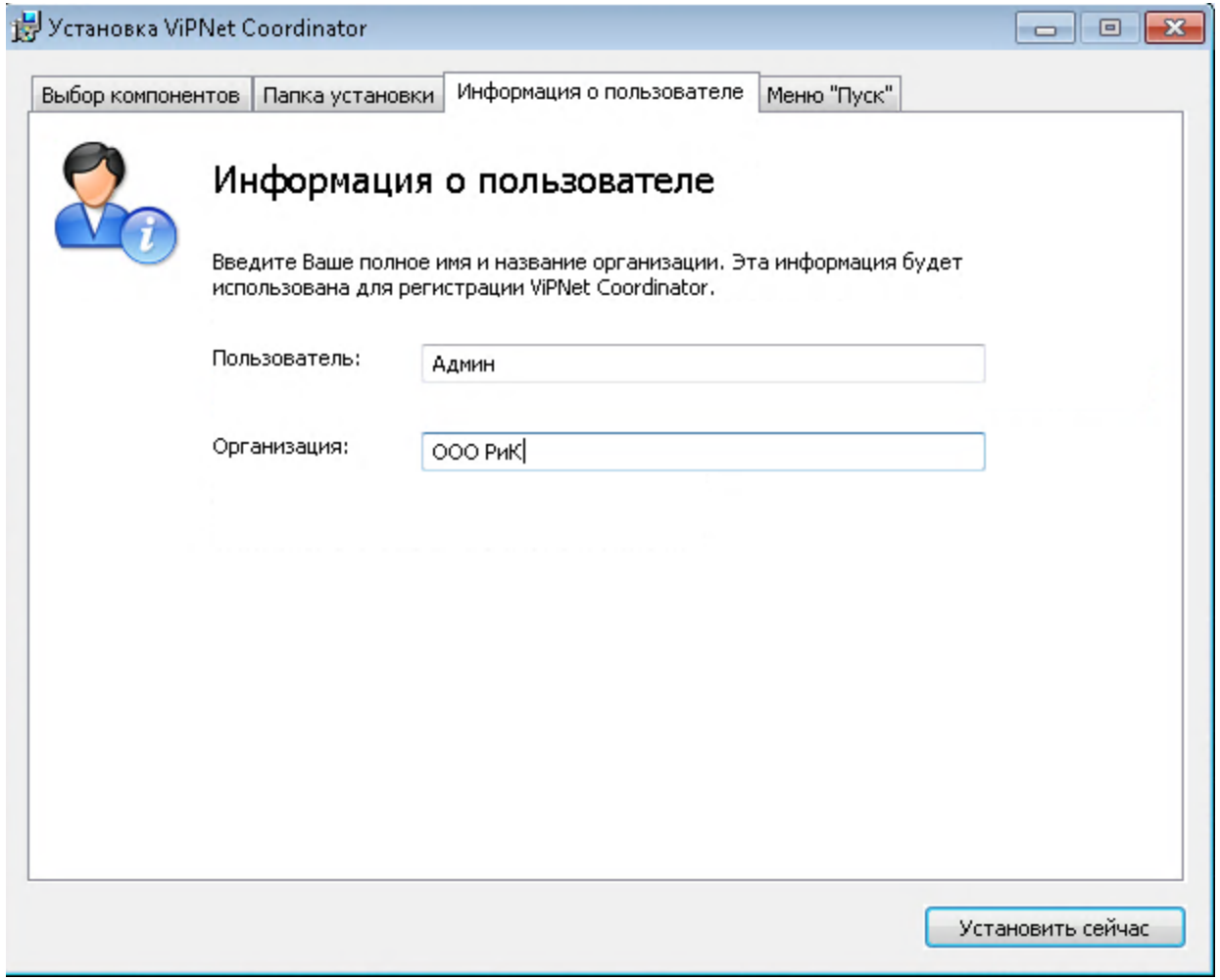
Установка ViPNet Coordinator

Дополнительные параметры установки



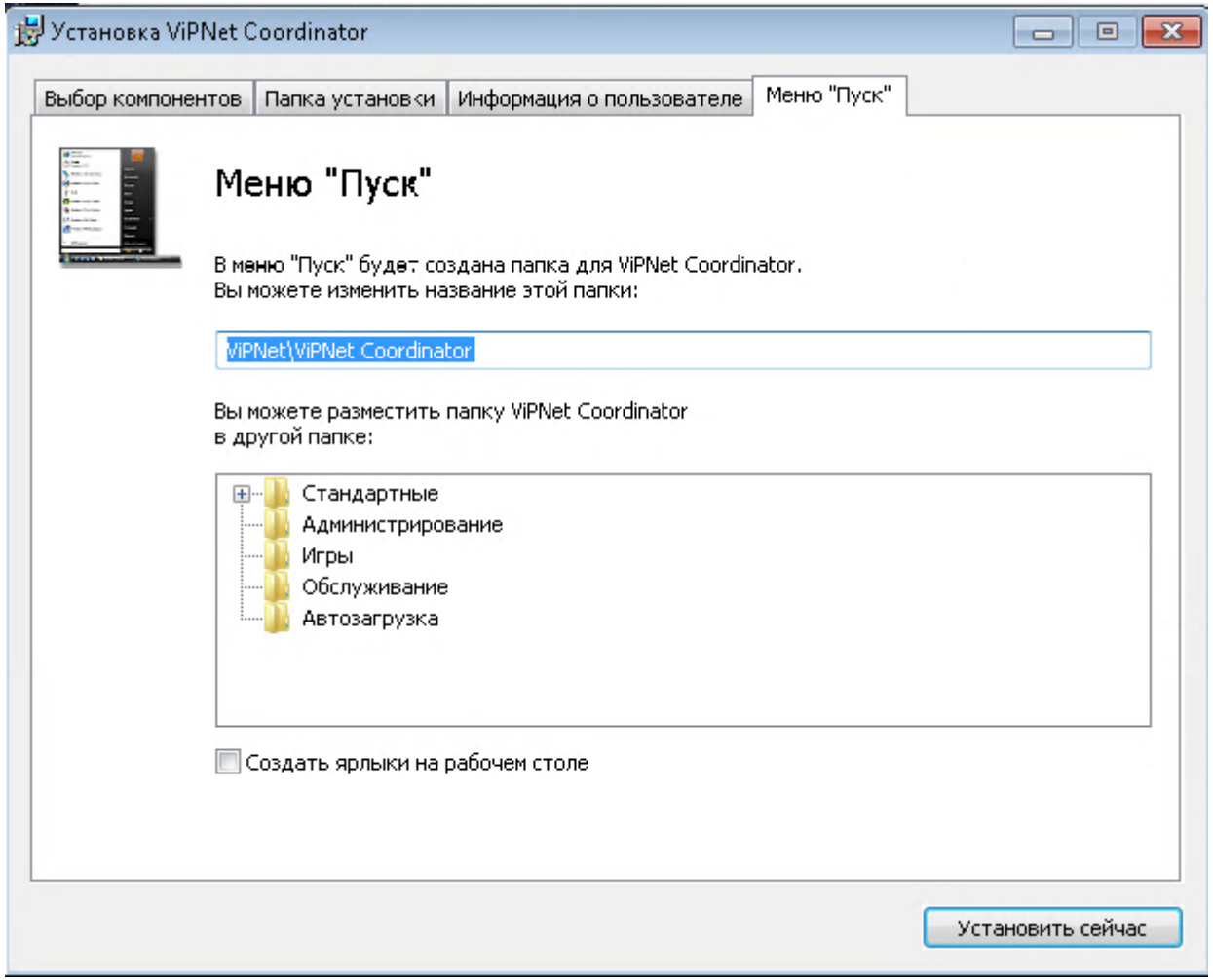
Установка ViPNet Coordinator

Дополнительные параметры установки



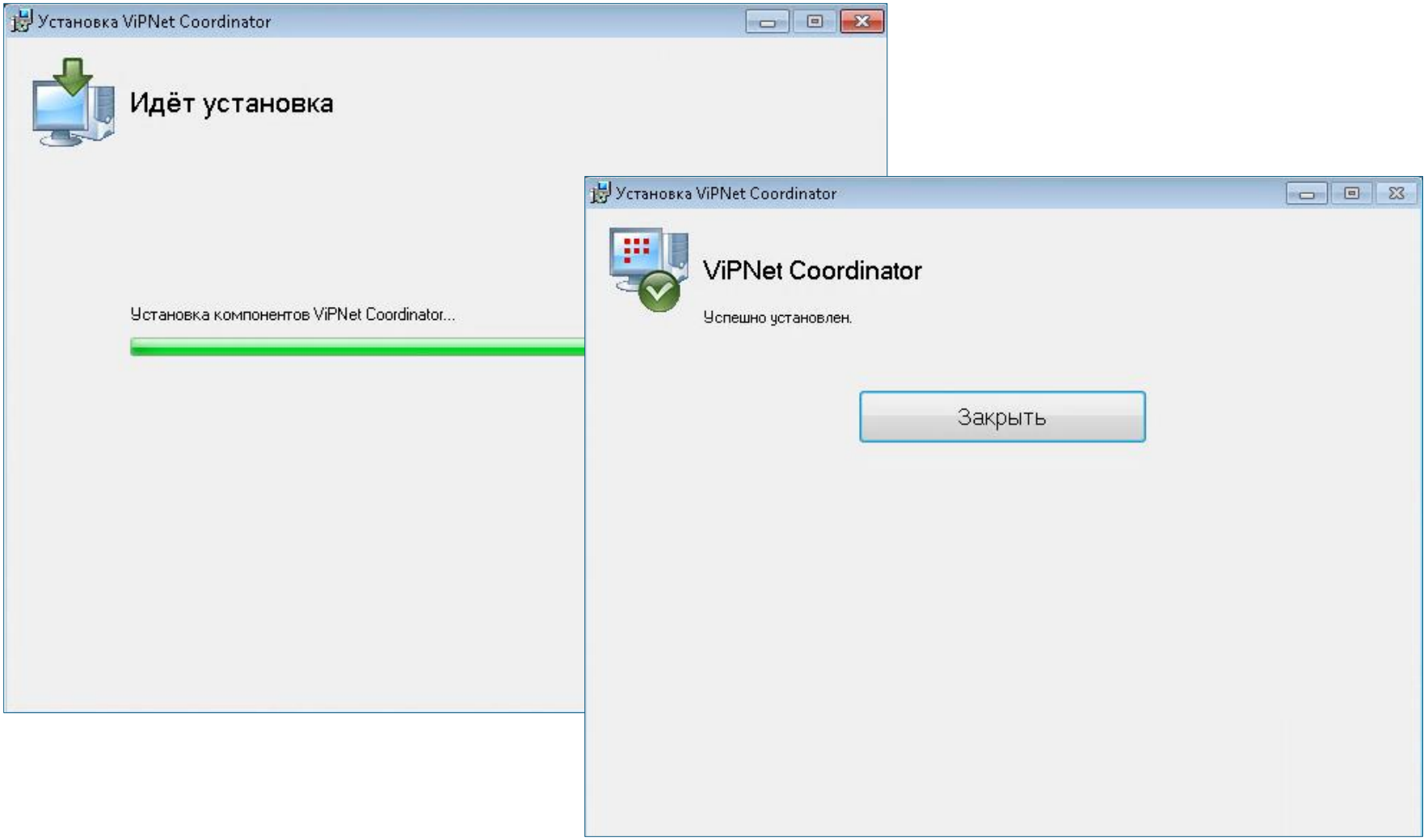
Установка ViPNet Coordinator

Дополнительные параметры установки



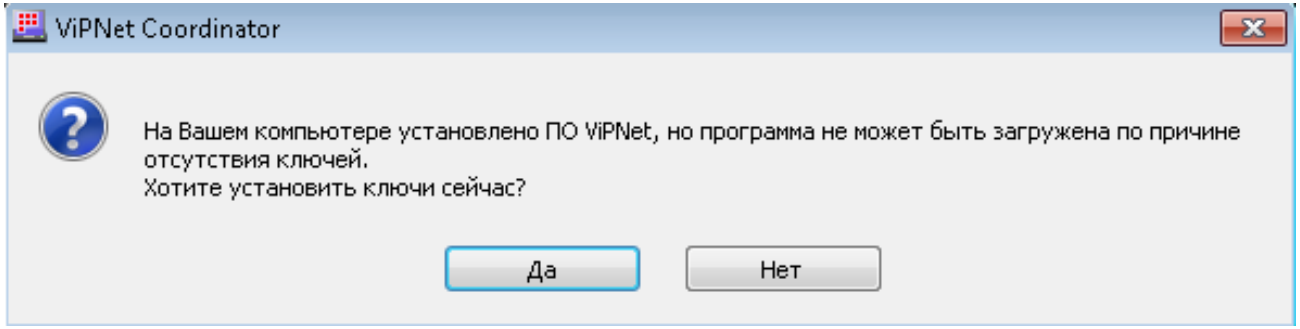
Установка ViPNet Coordinator

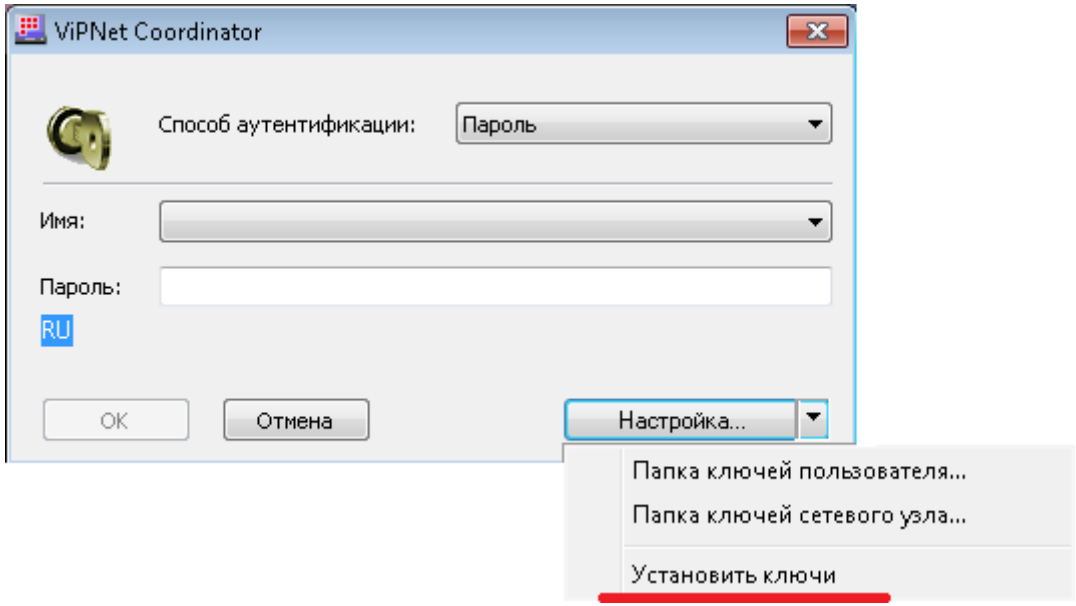
Установка в интерактивном режиме



Установка ViPNet Coordinator

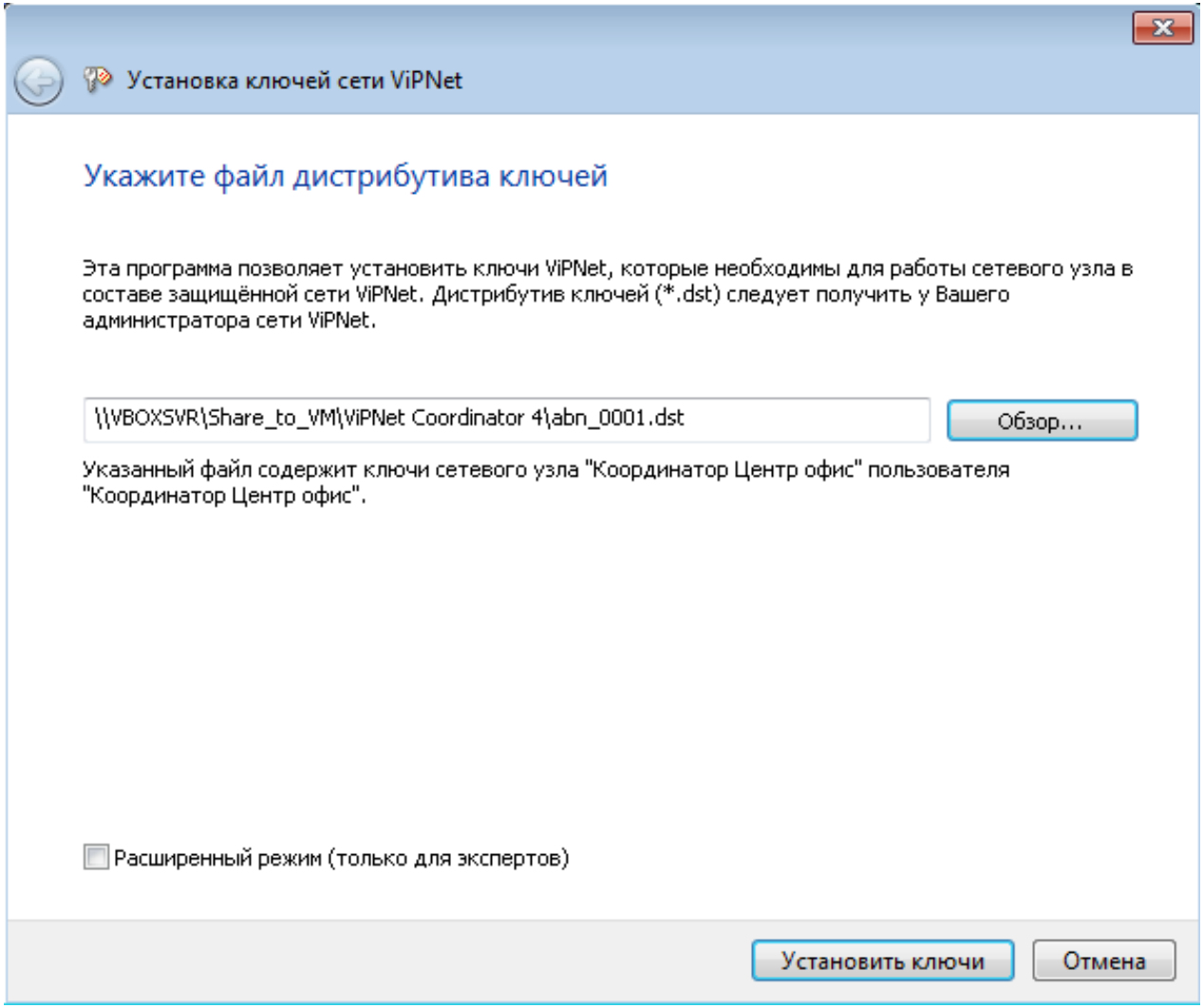
Установка справочников и ключей





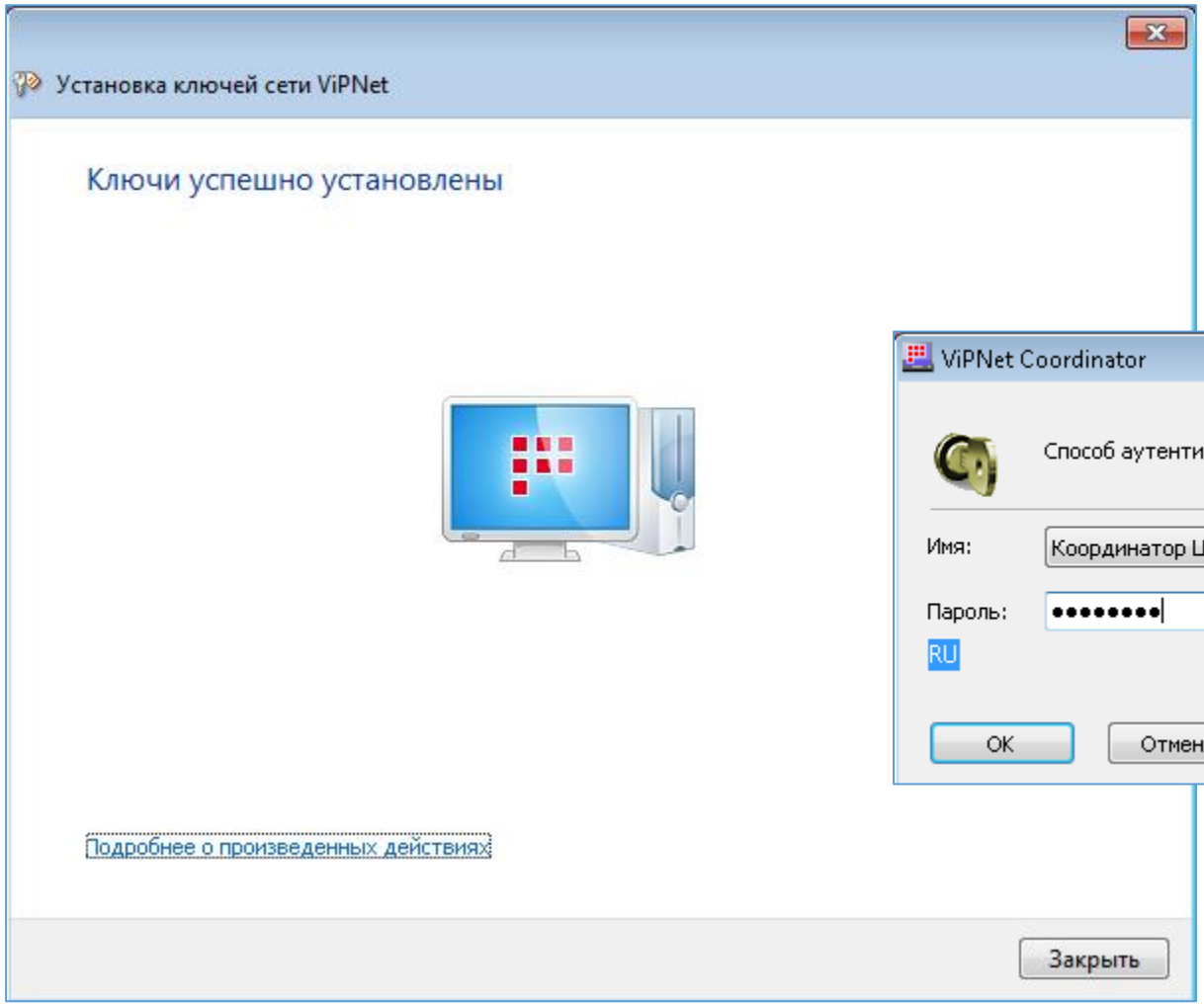
Установка ViPNet Coordinator

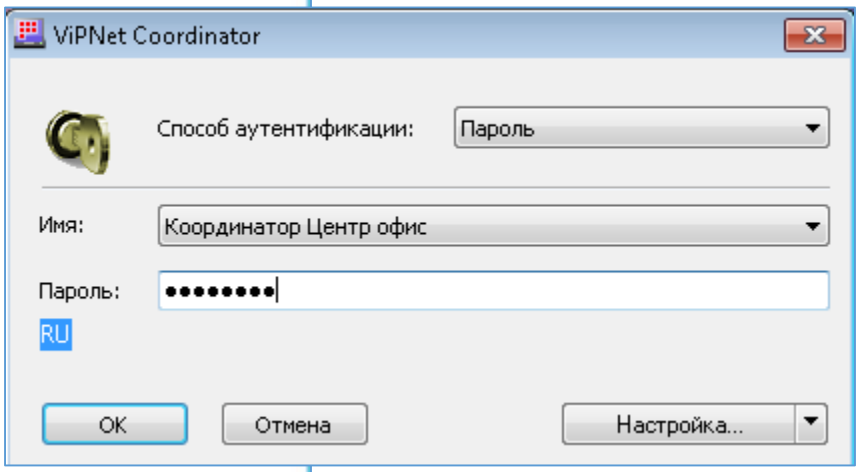
Установка справочников и ключей



Установка ViPNet Coordinator

Установка справочников и ключей





Способы аутентификации в ViPNet Coordinator

Пароль

- Для входа в программу нужно ввести свой пароль.
- Этот способ аутентификации установлен по умолчанию.

Устройство

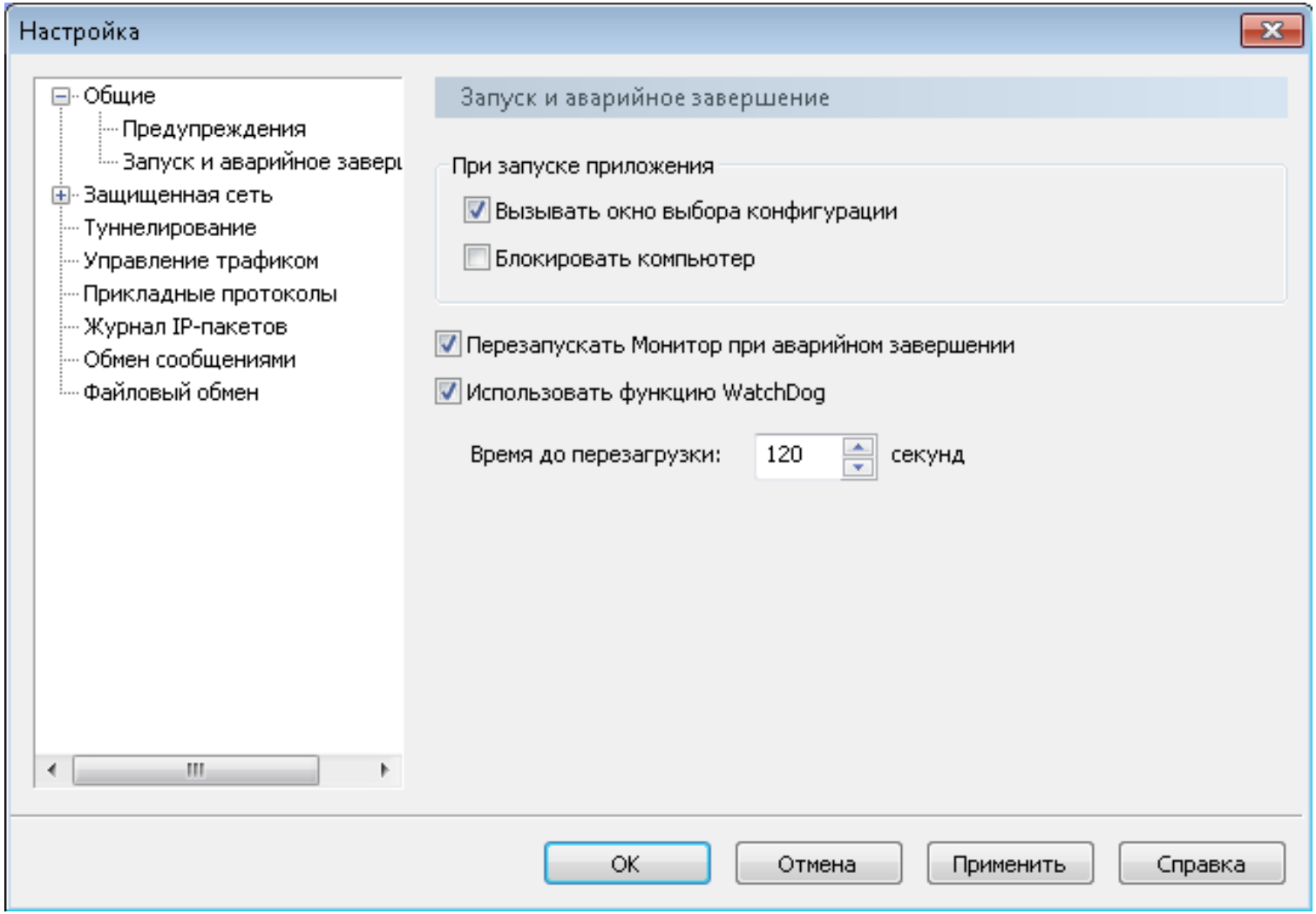
- Для входа в программу нужно подключить устройство и ввести PIN-код

Пароль на устройстве

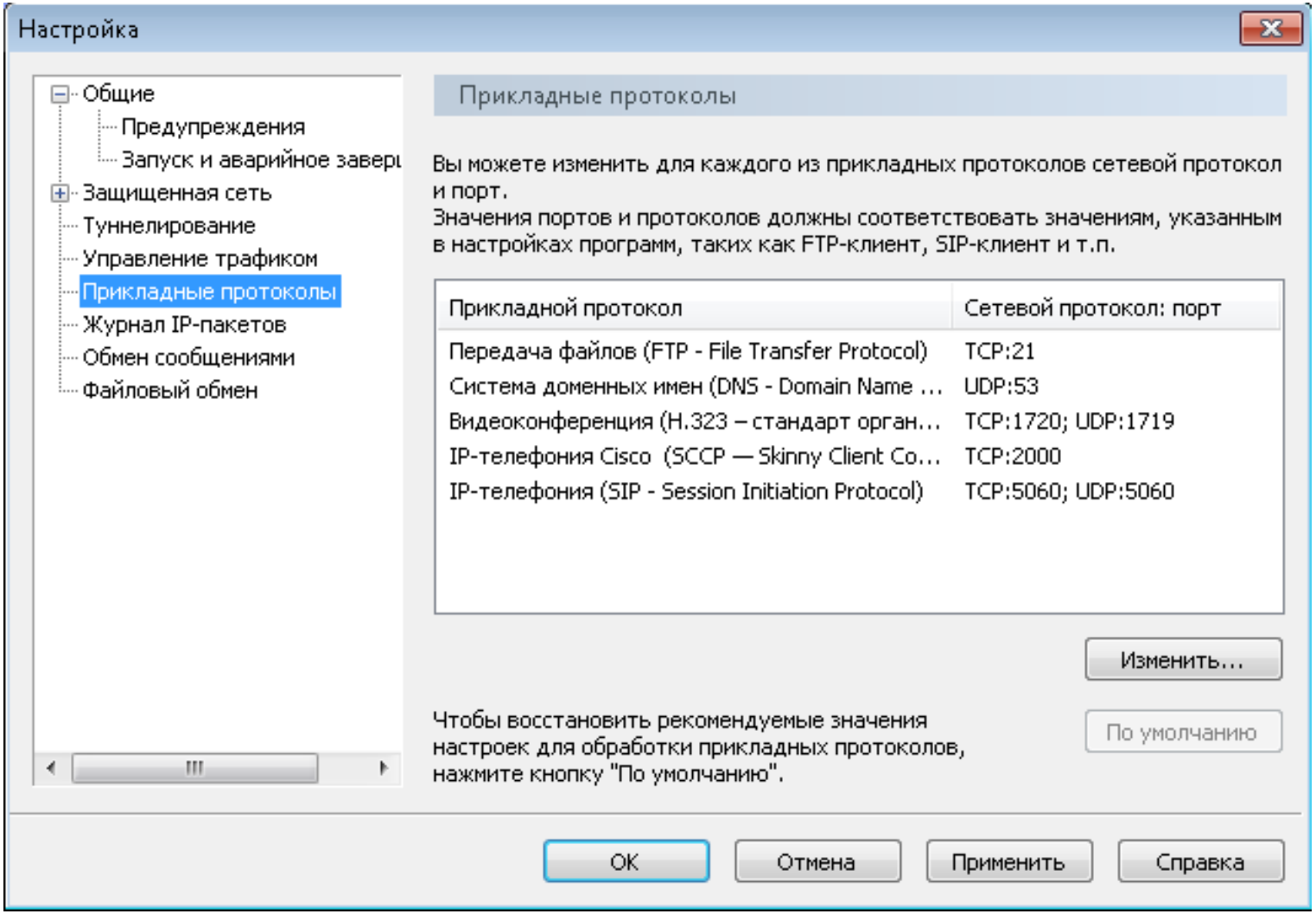
- Для входа в программу нужно подключить устройство и ввести ПИН-код
- Пароль хранится на устройстве
- Внимание! Способ аутентификации **Пароль на устройстве** не отвечает требованиям безопасности. Возможность его использования оставлена для совместимости с ПО ViPNet более ранних версий

Настройка ViPNet Coordinator

Общие настройки

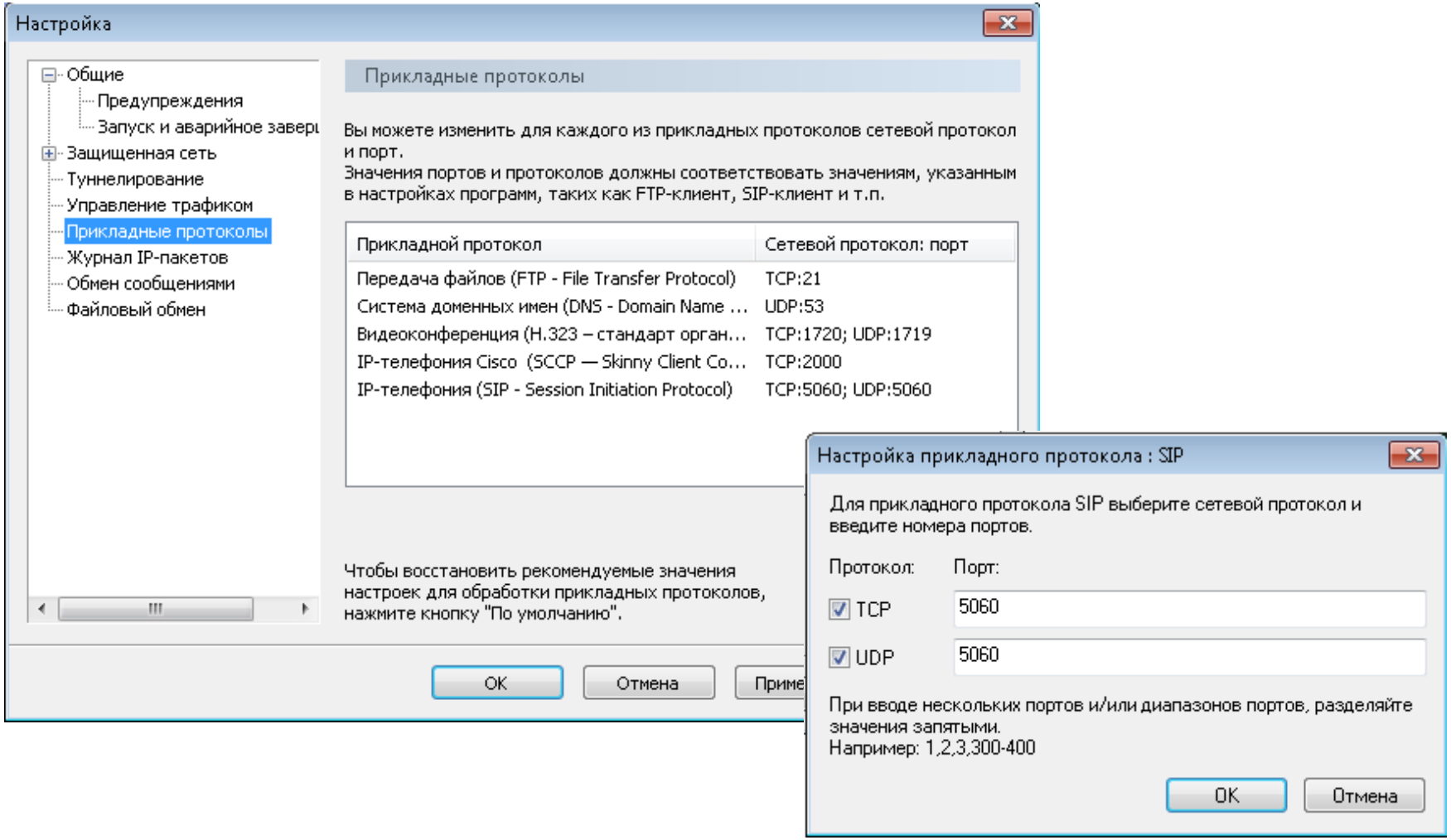


Настройка обработки прикладных протоколов



Настройка ViPNet Coordinator

Настройка обработки прикладных протоколов

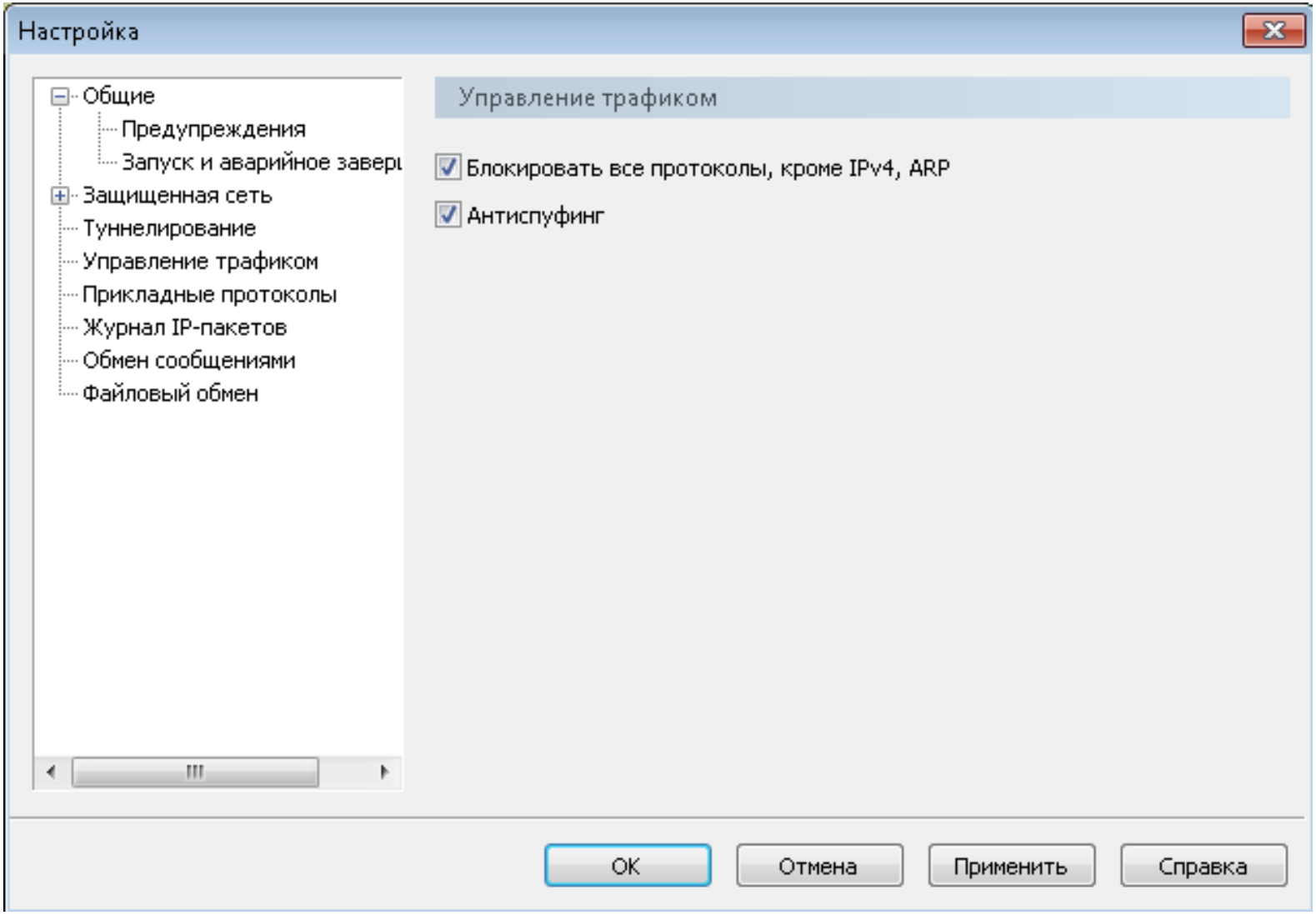


Настройка ViPNet Coordinator

Антиспуфинг:

- предназначен для защиты от сетевых атак (спуфинга), при которых злоумышленник подменяет адрес отправителя;
- блокирует входящие IP-пакеты от отправителей, IP-адреса которых недопустимы на данном сетевом интерфейсе;
- работает только для открытого трафика. Открытые пакеты сначала проверяются системой антиспуфинга, а потом обрабатываются сетевыми фильтрами;
- правила антиспуфинга задают для каждого сетевого интерфейса диапазоны IP-адресов, пакеты от которых недопустимы на данном интерфейсе. Пакеты, попадающие в такой диапазон, будут блокироваться;
- правила антиспуфинга создаются автоматически на основе таблицы маршрутизации сетевого узла.

Настройка антиспуфинга



Принципы организации соединений в сети ViPNet

- Защищенные узлы ViPNet могут располагаться в сетях любого типа, поддерживающих IP-протокол
- Для создания защищенных VPN-туннелей между сетевыми узлами используются IP-протоколы двух типов (IP/241 и IP/UDP), в которые упаковываются пакеты любых других IP-протоколов.

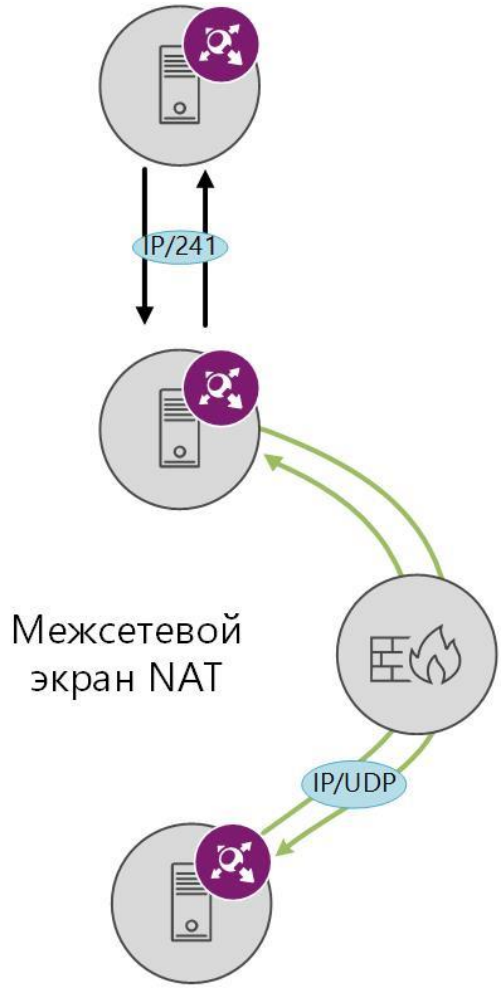
используется протокол IP/241

- если по пути следования пакета нет преобразования IP-адресов (узлы доступны по реальным IP-адресам)
- если узлы расположены в одном маршрутизируемом сегменте

используется протокол IP/UDP (порт 55777)

- если по пути пакета выполняется преобразование IP-адресов (на пути следования IP-пакета расположено устройство NAT)

Настройка параметров подключения к сети

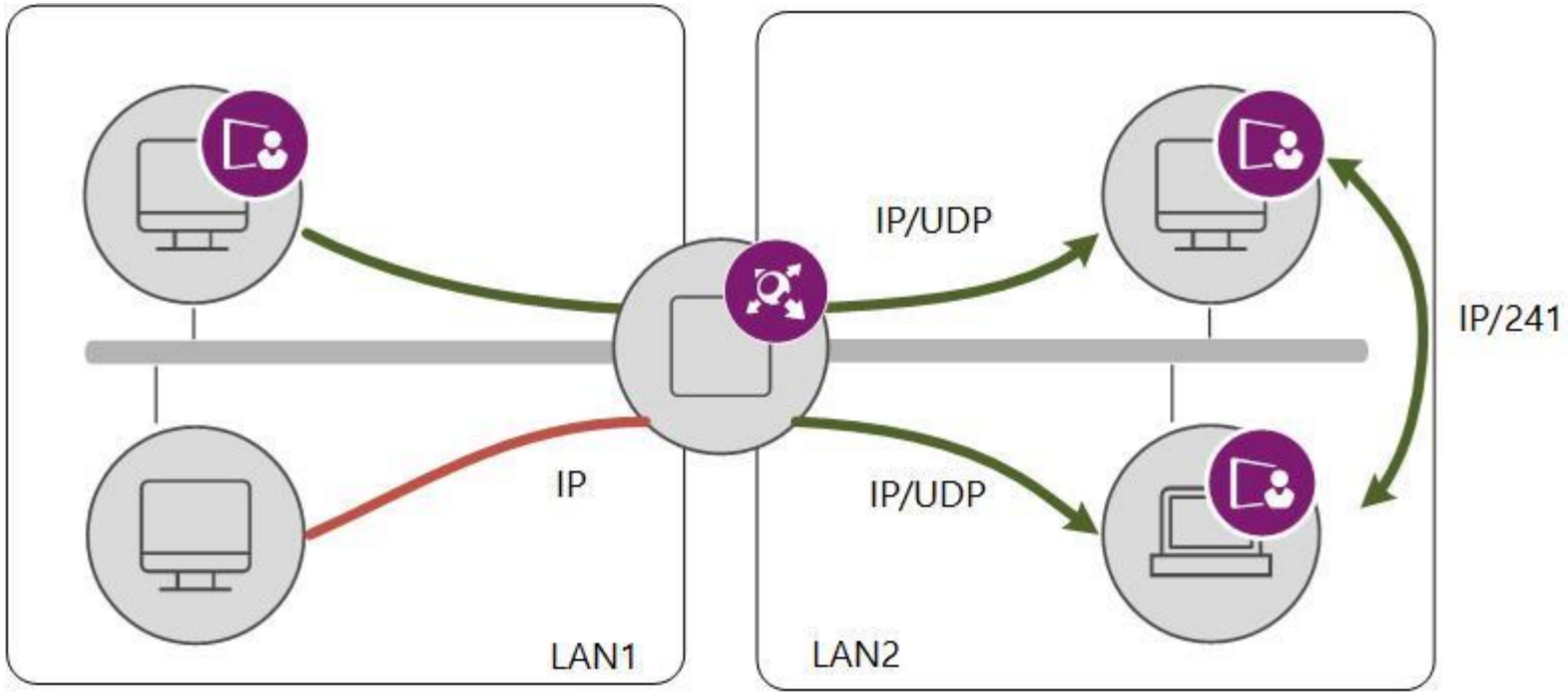


- подключение без использования межсетевого экрана
- подключение через координатор
- подключение через межсетевой экран с динамической трансляцией адресов
- подключение через межсетевой экран со статической трансляцией адресов

Настройка ViPNet Coordinator

- **без использования межсетевого экрана:**

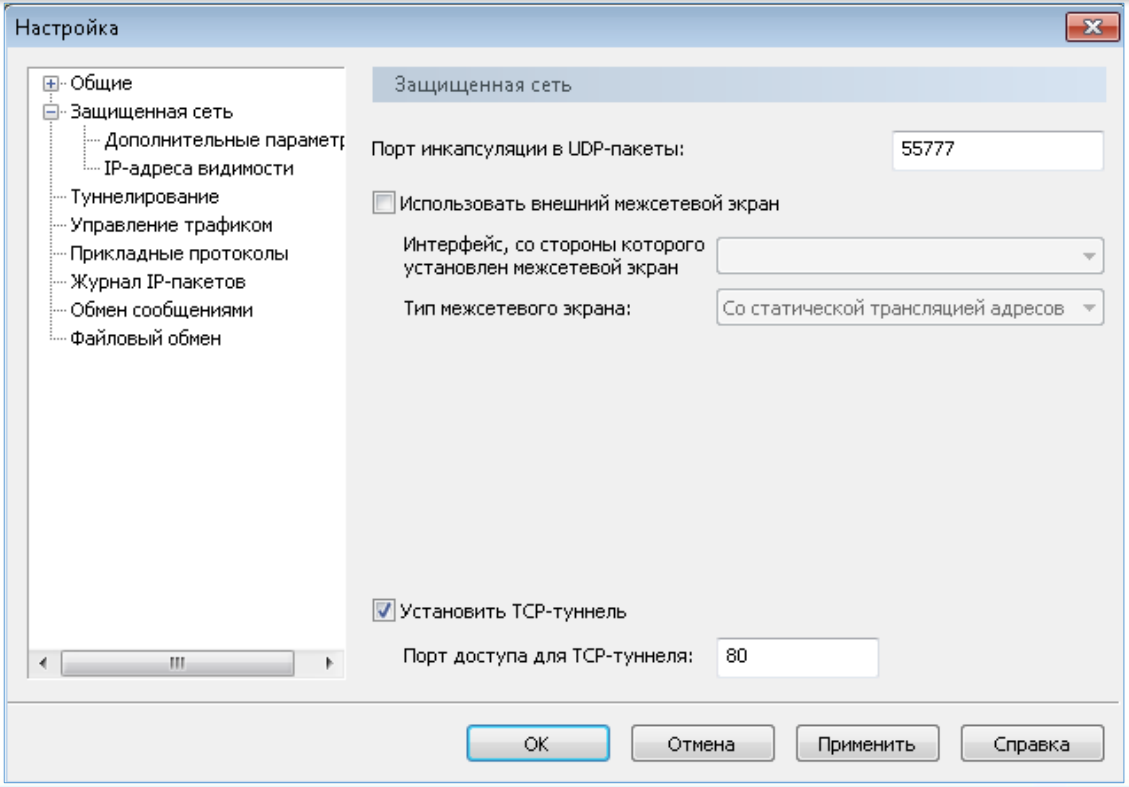
  - используется, если защищенный узел имеет IP-адрес, доступный по общим правилам маршрутизации другим узлам, с которыми нужно установить соединение;
  - защищенные узлы соединяются друг с другом напрямую по протоколу IP/241;



Настройка ViPNet Coordinator

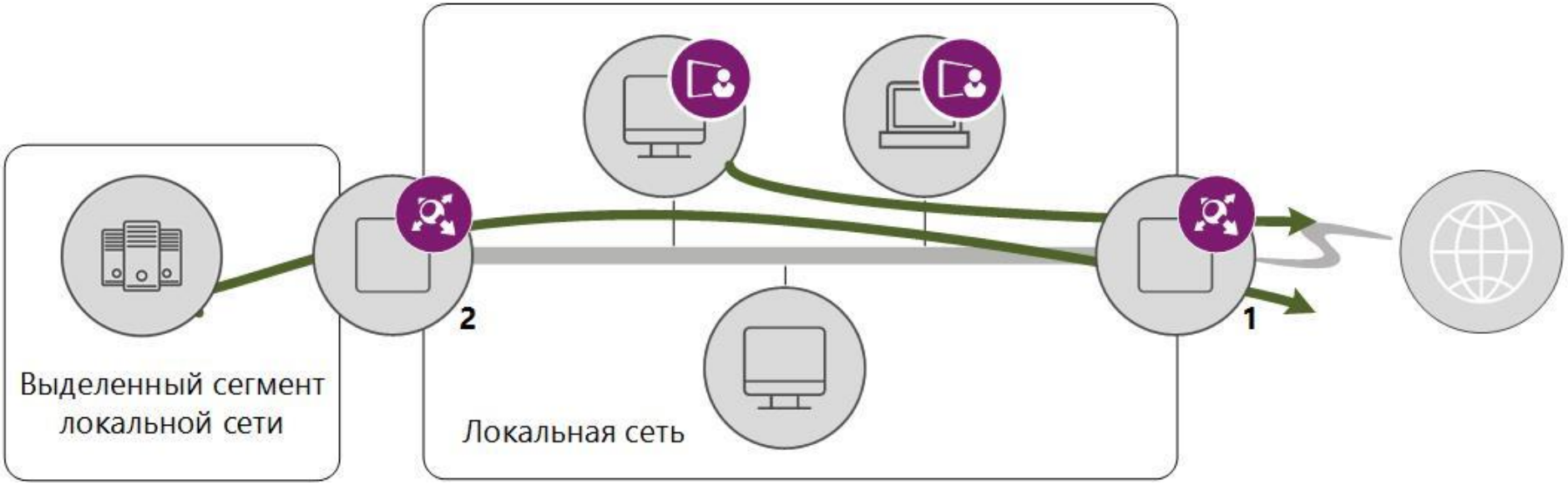
- **без использования межсетевого экрана:**

- используется, если защищенный узел имеет IP-адрес, доступный по общим правилам маршрутизации другим узлам, с которыми нужно установить соединение;
- защищенные узлы соединяются друг с другом напрямую по протоколу IP/241;



Настройка ViPNet Coordinator

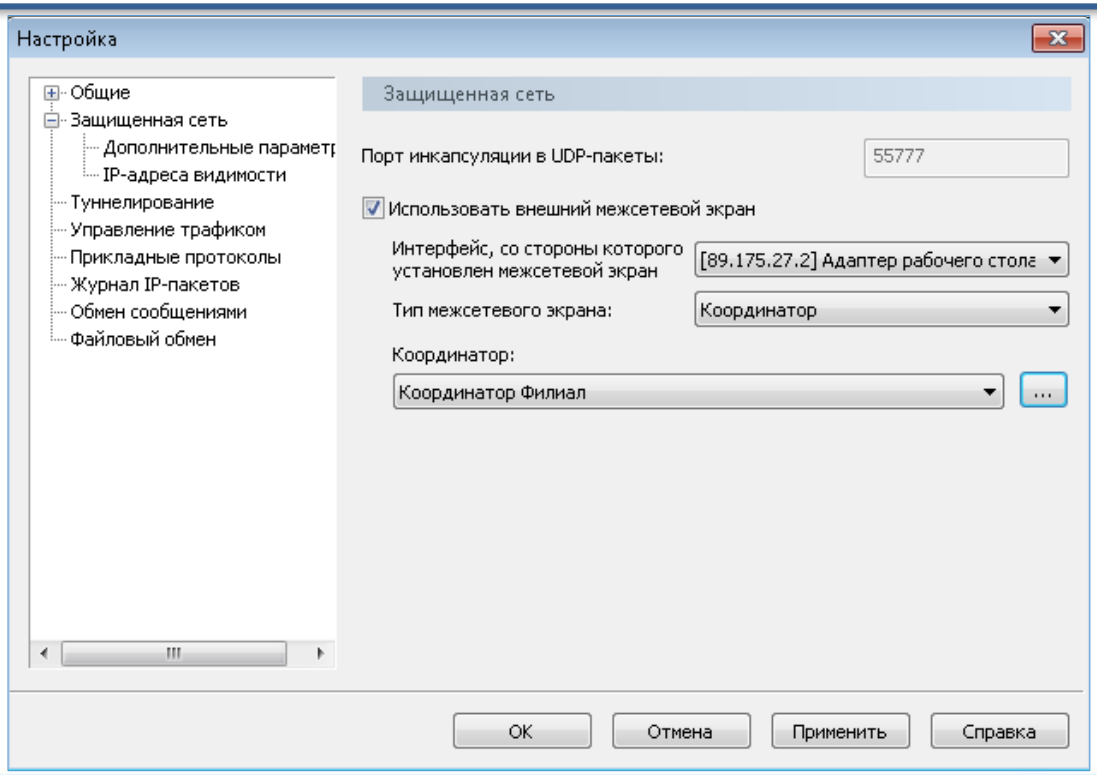
- **через координатор:**
  - используется, если на границе локальной сети в качестве шлюза установлен ViPNet-координатор;
  - зашифрованный трафик перенаправляется через ViPNet-координатор;
  - можно выбрать ViPNet-координатор, который не является сервером IP-адресов;



Настройка ViPNet Coordinator

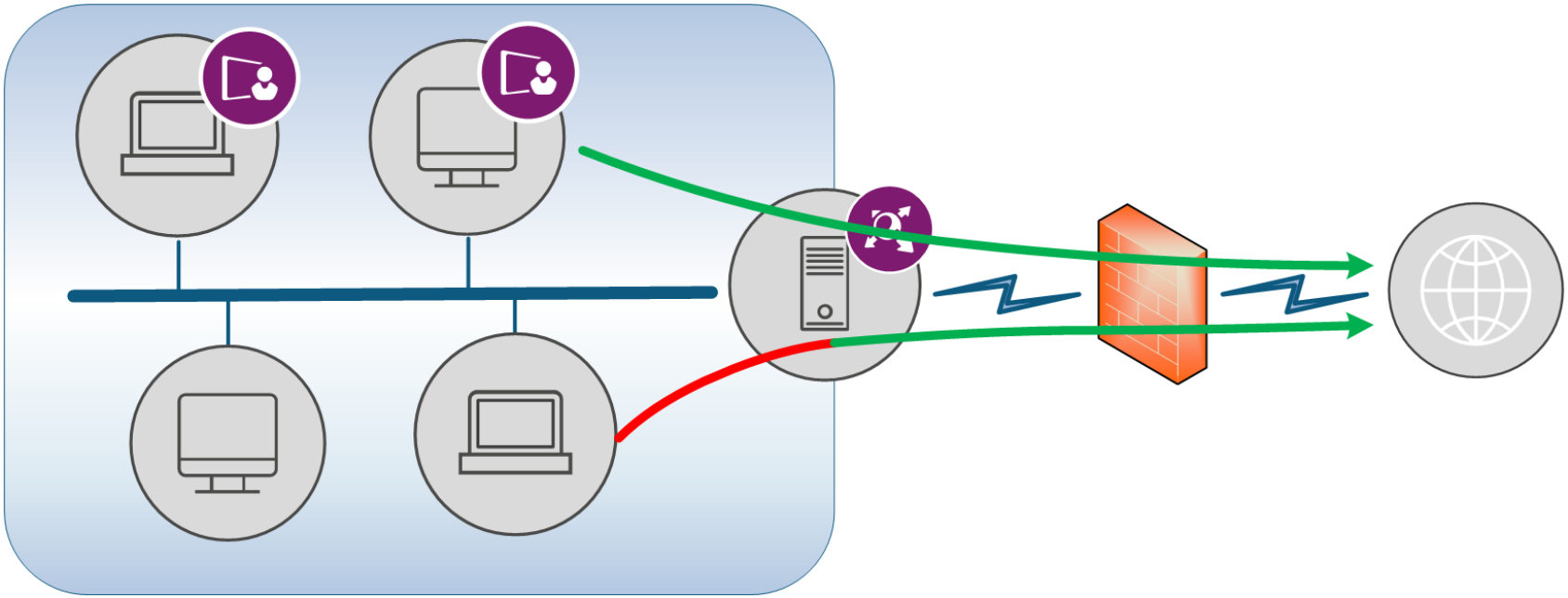
- **через координатор:**

- используется, если на границе локальной сети в качестве шлюза установлен ViPNet-координатор;
- зашифрованный трафик перенаправляется через ViPNet-координатор;
- можно выбрать ViPNet-координатор, который не является сервером IP-адресов;



Настройка ViPNet Coordinator

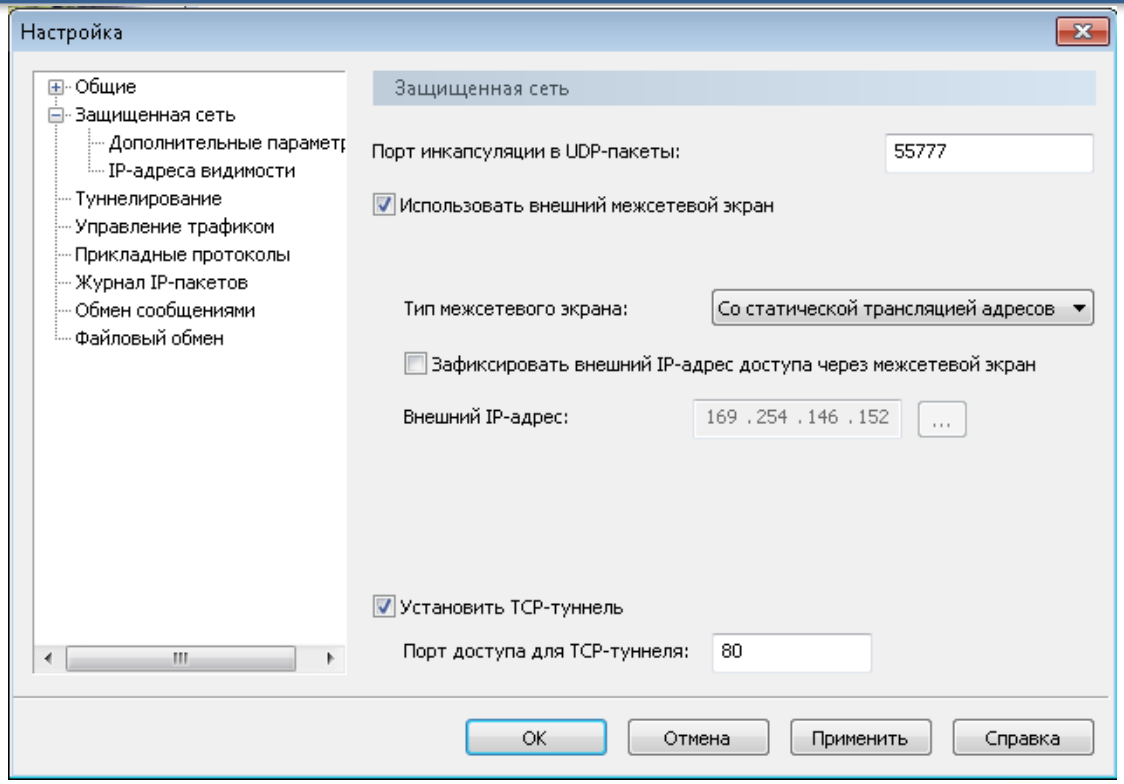
- **через межсетевой экран со статической трансляцией адресов:**
  - используется, если соединение с внешней сетью происходит через межсетевой экран, на котором можно настроить статические правила трансляции адресов;
  - для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию;



Настройка ViPNet Coordinator

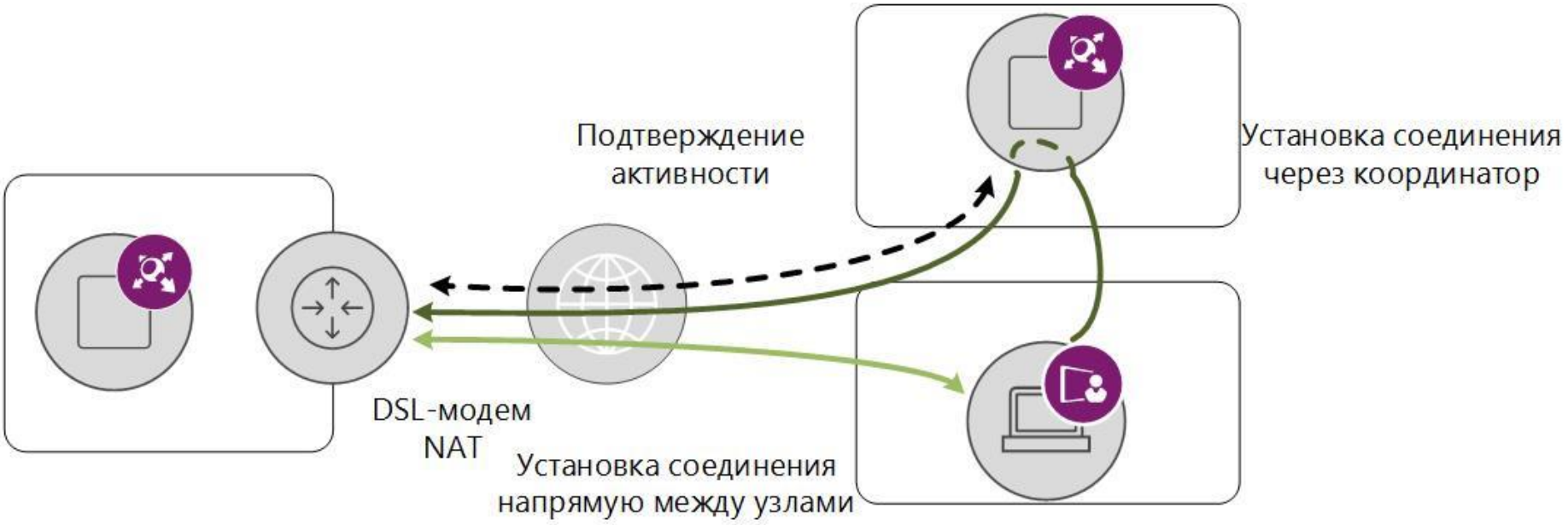
- **через межсетевой экран со статической трансляцией адресов:**

- используется, если соединение с внешней сетью происходит через межсетевой экран, на котором можно настроить статические правила трансляции адресов;
- для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию;



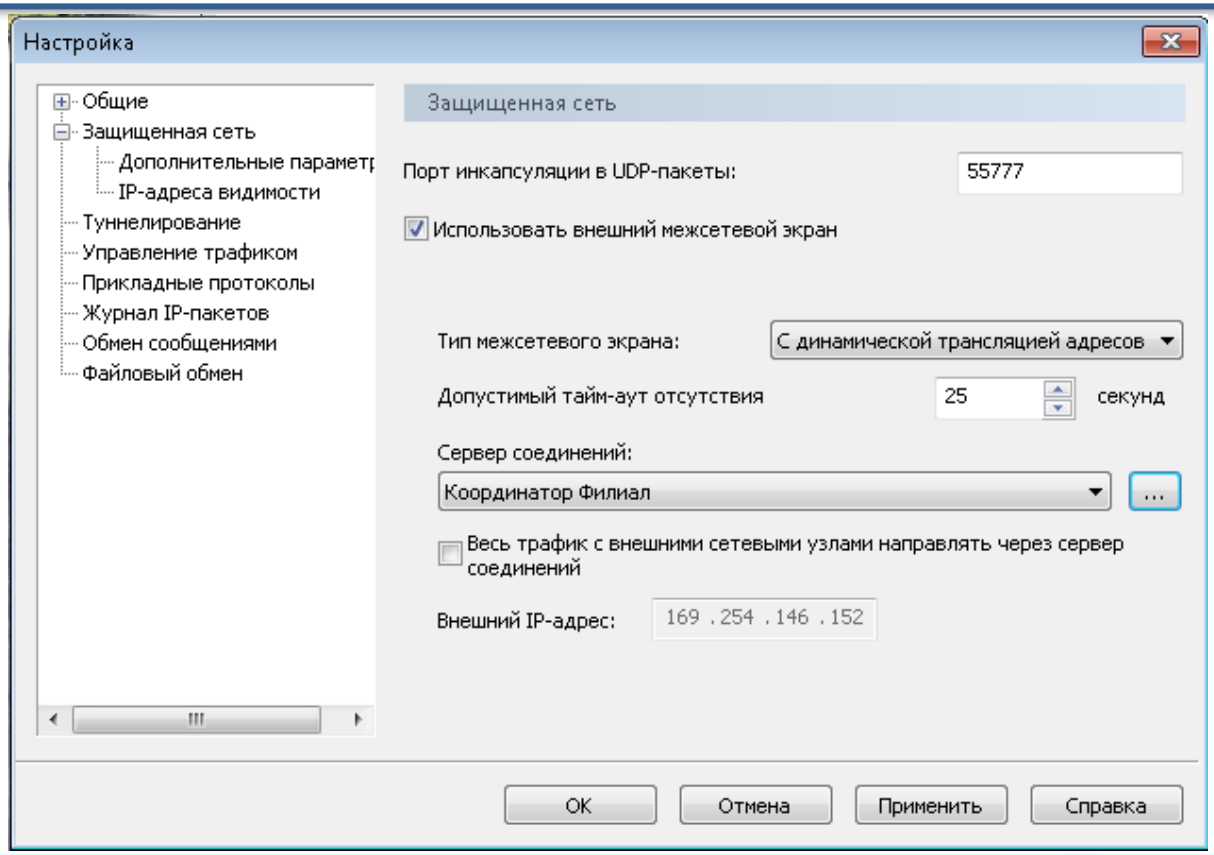
Настройка ViPNet Coordinator

- **через межсетевой экран с динамической трансляцией адресов:**
  - используется, если соединение с внешней сетью происходит через межсетевой экран, на котором нельзя настроить статические правила трансляции адресов;
  - для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию.



Настройка ViPNet Coordinator

- **через межсетевой экран с динамической трансляцией адресов:**
  - используется, если соединение с внешней сетью происходит через межсетевой экран, на котором нельзя настроить статические правила трансляции адресов;
  - для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию.



Виртуальные IP-адреса

Виртуальный IP-адрес - адрес, который приложения на сетевом узле ViPNet используют для обращения к ресурсам другого защищенного или туннелируемого узла вместо реального IP-адреса узла.

Виртуальные IP-адреса используются:

- при взаимодействии с компьютерами, которые установлены за межсетевым экраном;
- для обеспечения связи с защищенными узлами и туннелируемыми открытыми компьютерами в локальных сетях с пересекающейся внутренней адресацией;
- для разграничения доступа с защищенных узлов к ресурсам корпоративной сети;
- для защиты от подмены адреса отправителя.

Настройка ViPNet Coordinator

Виртуальные IP-адреса определяются на прикладном уровне стека протоколов TCP/IP, на сетевом уровне стека драйвер ViPNet заменяет виртуальные IP-адреса на реальные для передачи информации по сети.

Настройка ViPNet Coordinator

Принципы назначения виртуальных IP-адресов:

- виртуальные IP-адреса автоматически формируются на сетевом узле ViPNet для всех узлов, с которыми он связан;
- по умолчанию начальный адрес генератора виртуальных IP-адресов для узлов ViPNet и одиночных туннелируемых адресов — 11.0.0.1, маска подсети: 255.0.0.0;
- для диапазонов туннелируемых адресов начальным виртуальным адресом по умолчанию является 12.0.0.1;
- виртуальные IP-адреса формируются на основе уникального идентификатора сетевого узла и не привязаны к «реальному» IP-адресу сетевого интерфейса;

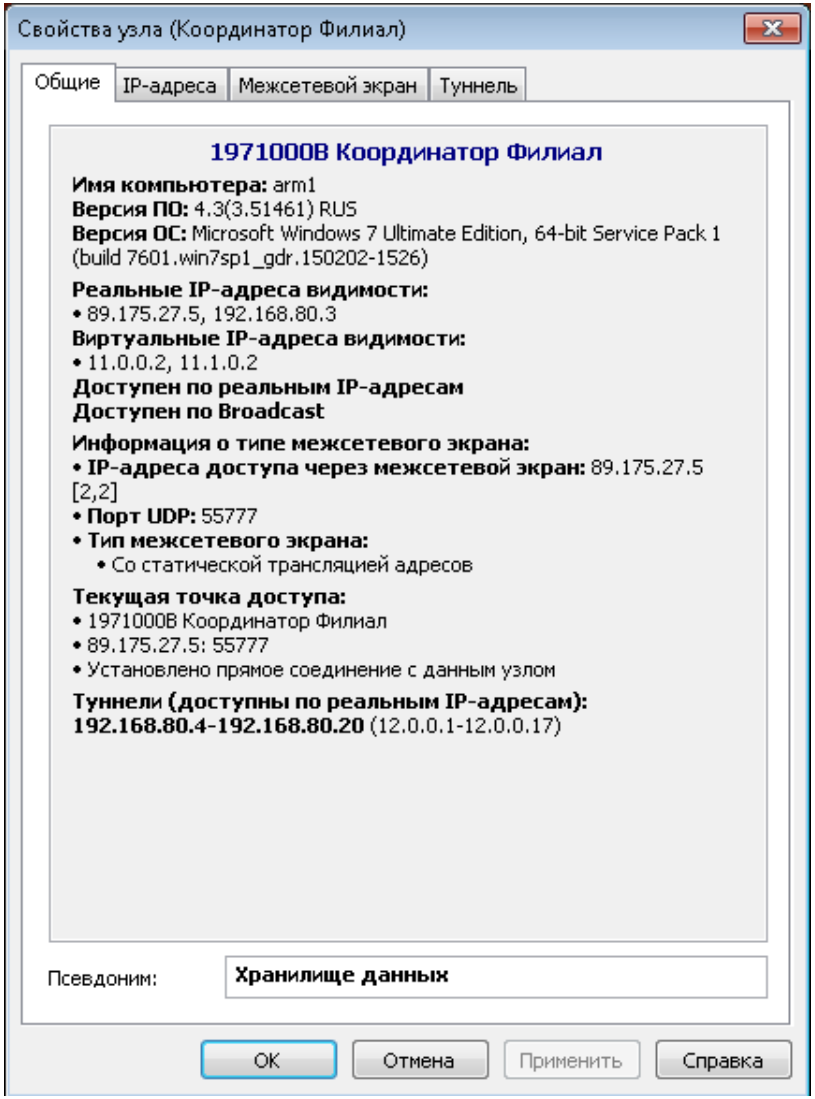
Настройка ViPNet Coordinator

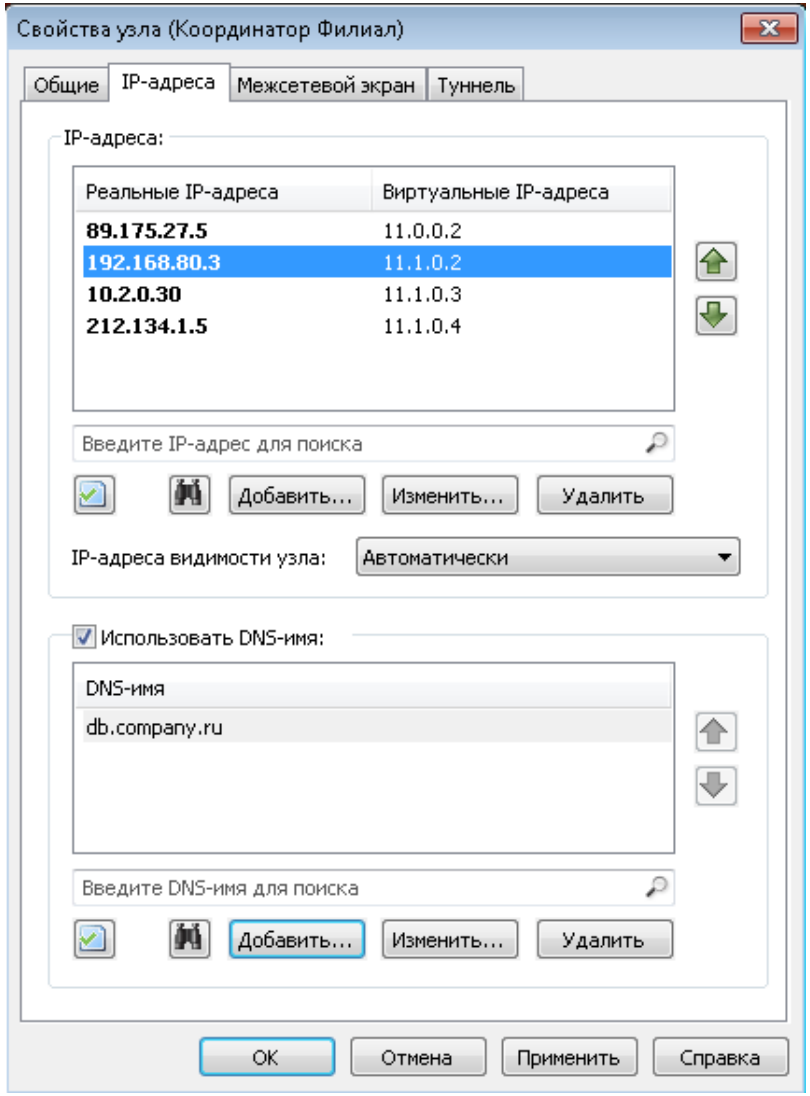
Принципы назначения виртуальных IP-адресов:

- виртуальные адреса для одиночных туннелируемых узлов закрепляются за каждым реальным туннелируемым IP-адресом;
- при обновлении адресных справочников, при изменении реальных адресов узла или при добавлении одиночного туннелируемого адреса **виртуальные адреса не изменяются;**
- виртуальные адреса, выделенные для туннелируемых диапазонов адресов, могут измениться при добавлении новых диапазонов туннелируемых адресов;
- при смене начального адреса для генератора виртуальных адресов все виртуальные адреса формируются заново;
- узлу ViPNet назначается столько виртуальных адресов, сколько «реальных» адресов имеет данный узел.

Настройка ViPNet Coordinator

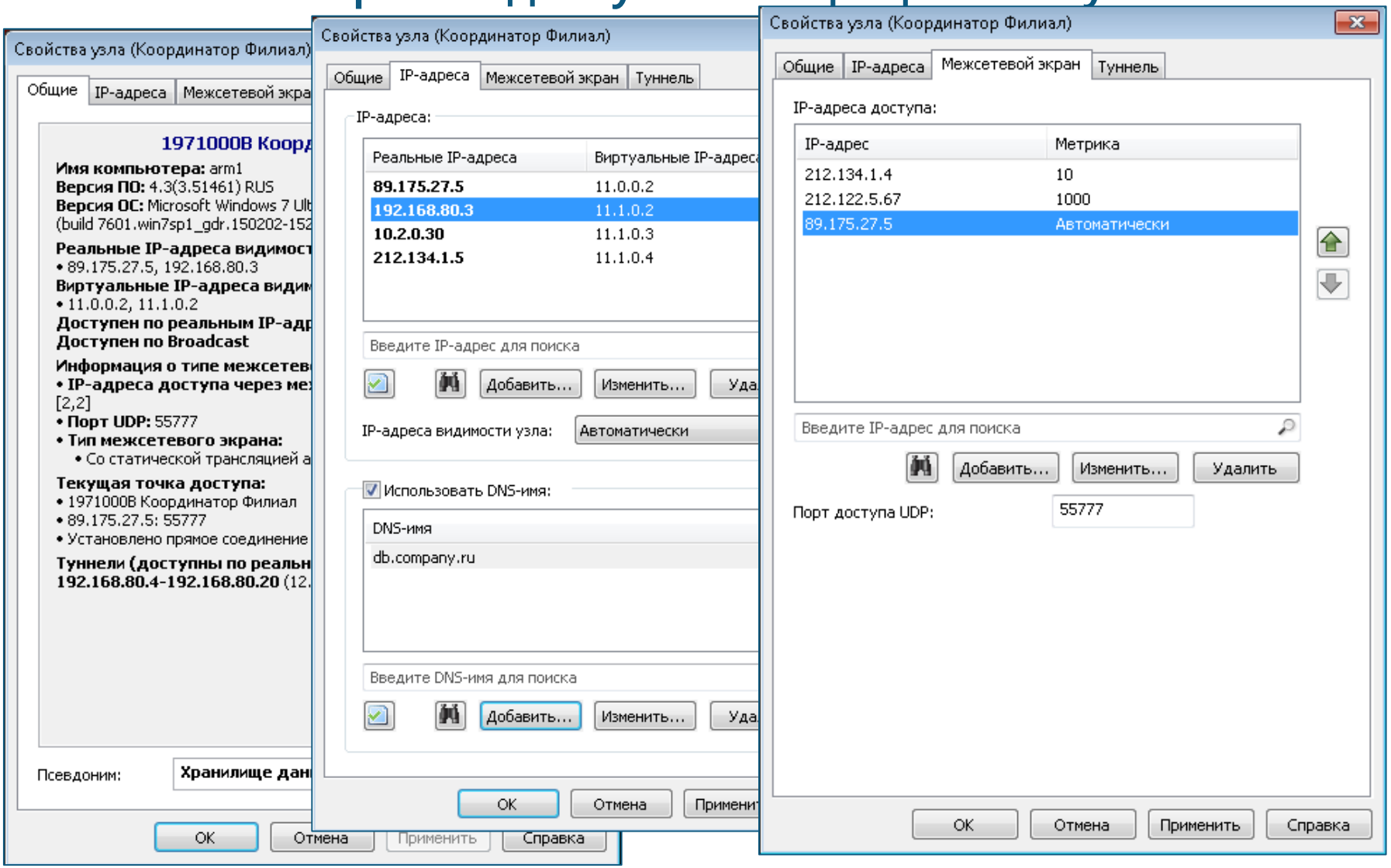
Настройка доступа к защищенным узлам



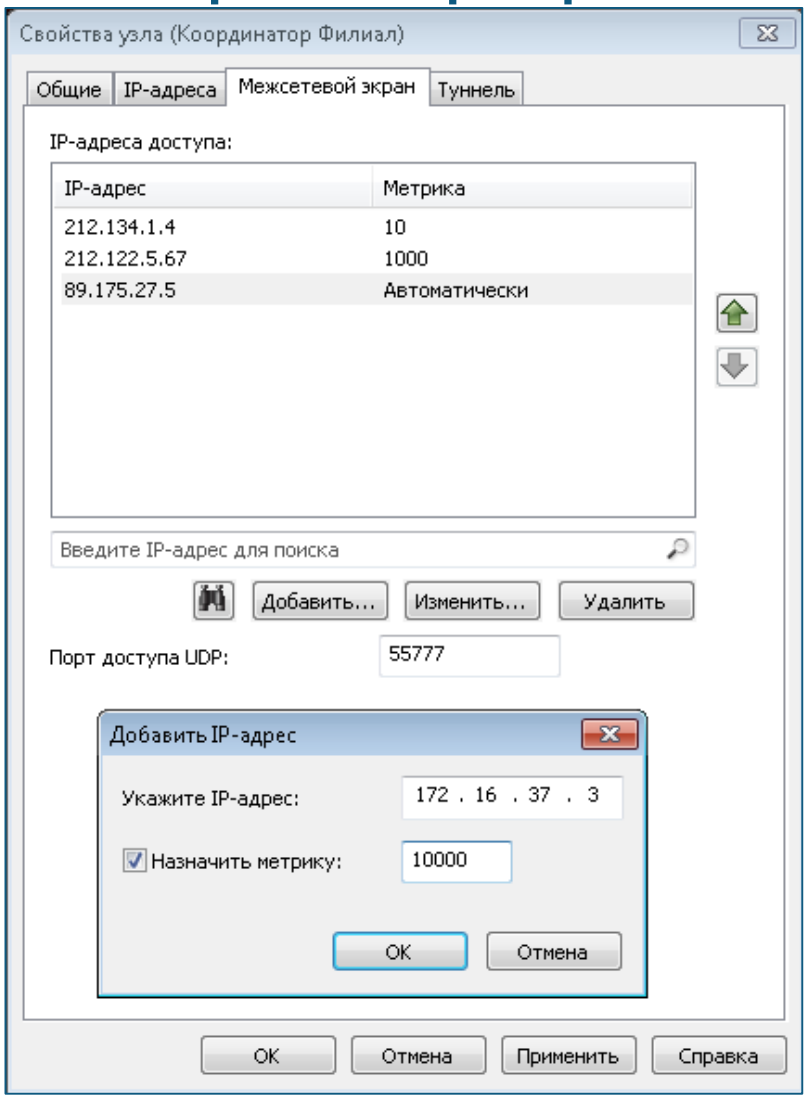


Настройка ViPNet Coordinator

Настройка доступа к защищенным узлам

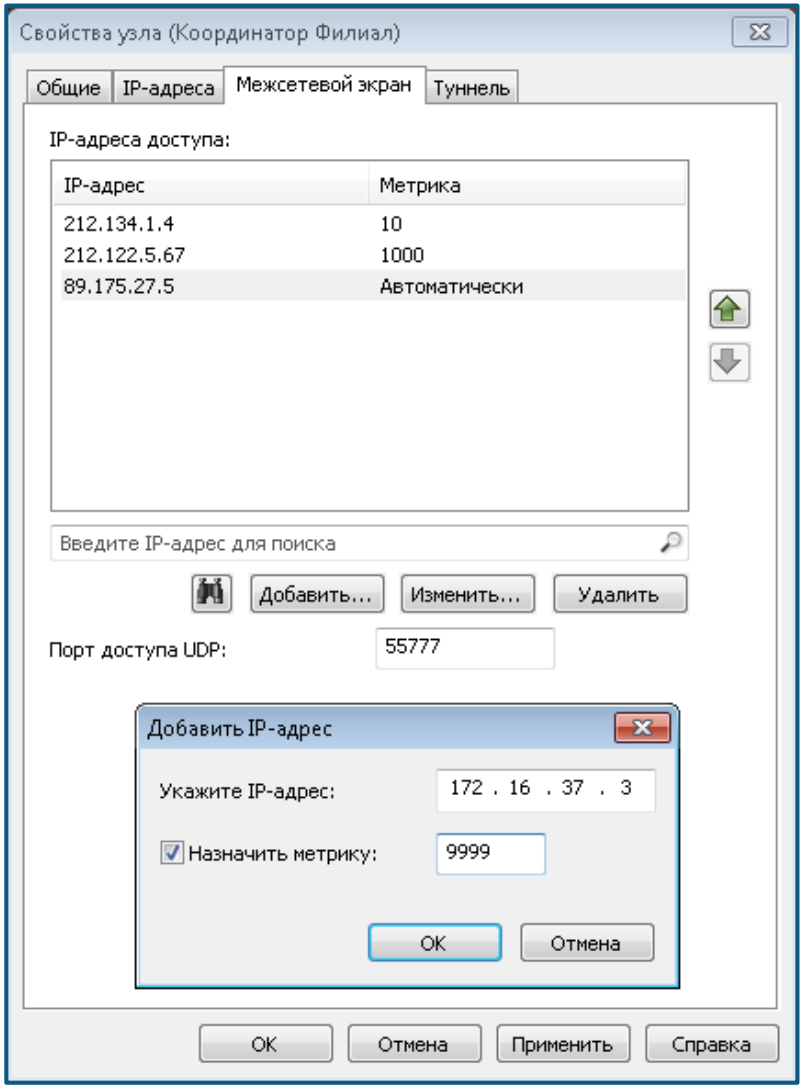


Настройка приоритета IP-адресов доступа (метрики):



- метрика задает приоритет использования для каждого IP-адреса доступа координатора;
- по умолчанию метрика назначается автоматически;
- метрика определяет задержку (в миллисекундах) отправки тестовых пакетов при проверки доступности адреса. Соединение устанавливается по тому адресу, доступность которого определится быстрее;

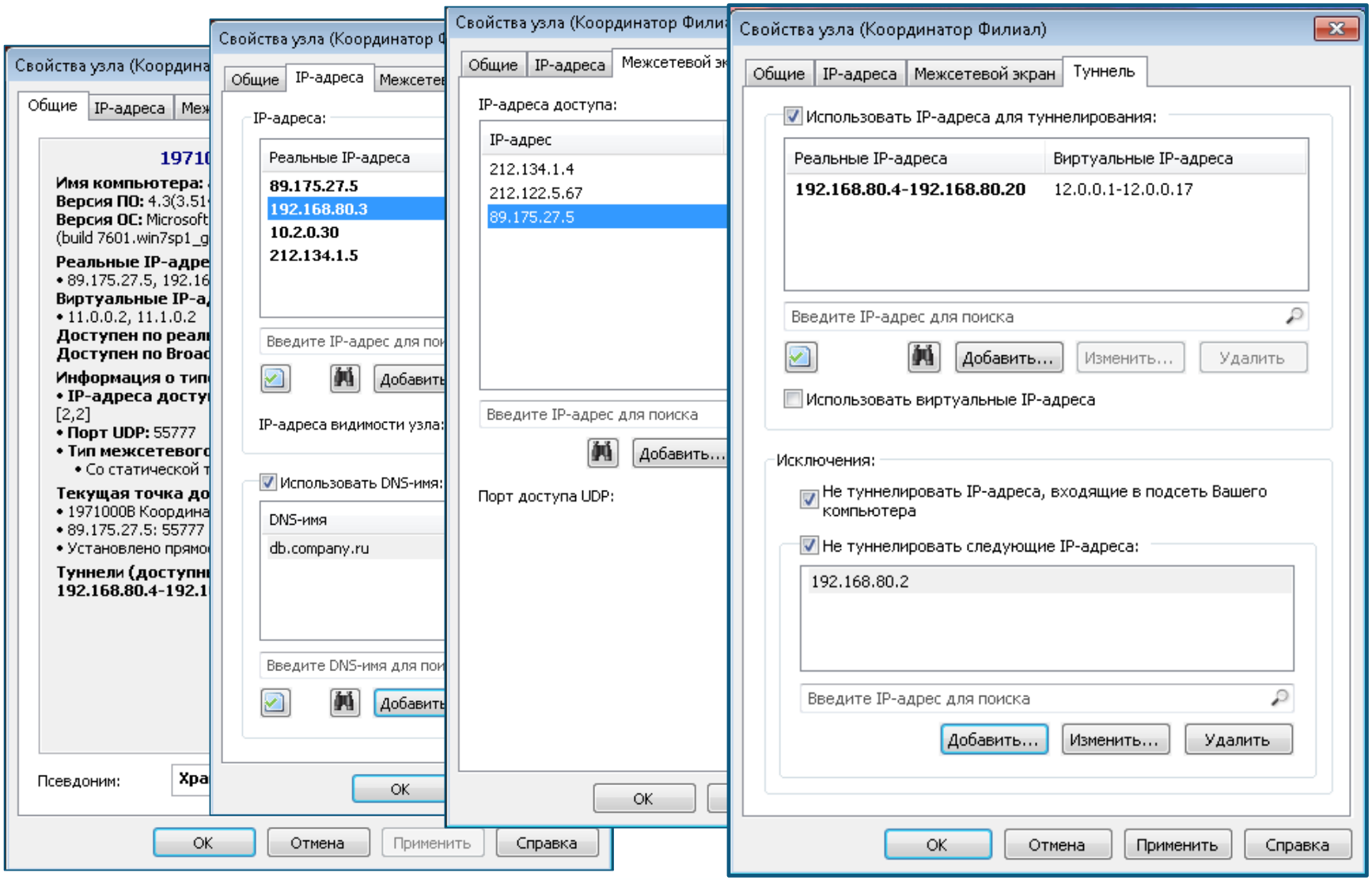
Настройка приоритета IP-адресов доступа (метрики):



- адрес с наименьшей метрикой считается самым приоритетным;
- если все метрики равны, то для работы будет выбран тот канал, через который соединение с координатором будет установлено быстрее.

Настройка ViPNet Coordinator

Настройка доступа к защищенным узлам



Защита трафика открытых узлов

Туннелирование IP-трафика

Технология туннелирования позволяет защитить трафик открытых узлов при его передаче на потенциально опасном участке сети.

Туннелирование предполагает защиту трафика по следующим правилам:

- туннелироваться может трафик любых устройств, находящихся со стороны любого сетевого интерфейса;
- трафик направляется не напрямую на другой узел, а через ViPNet Координатор, где он фильтруется и защищается криптографическими методами;

Защита трафика открытых узлов

Туннелирование IP-трафика

Туннелирование предполагает защиту трафика по следующим правилам:

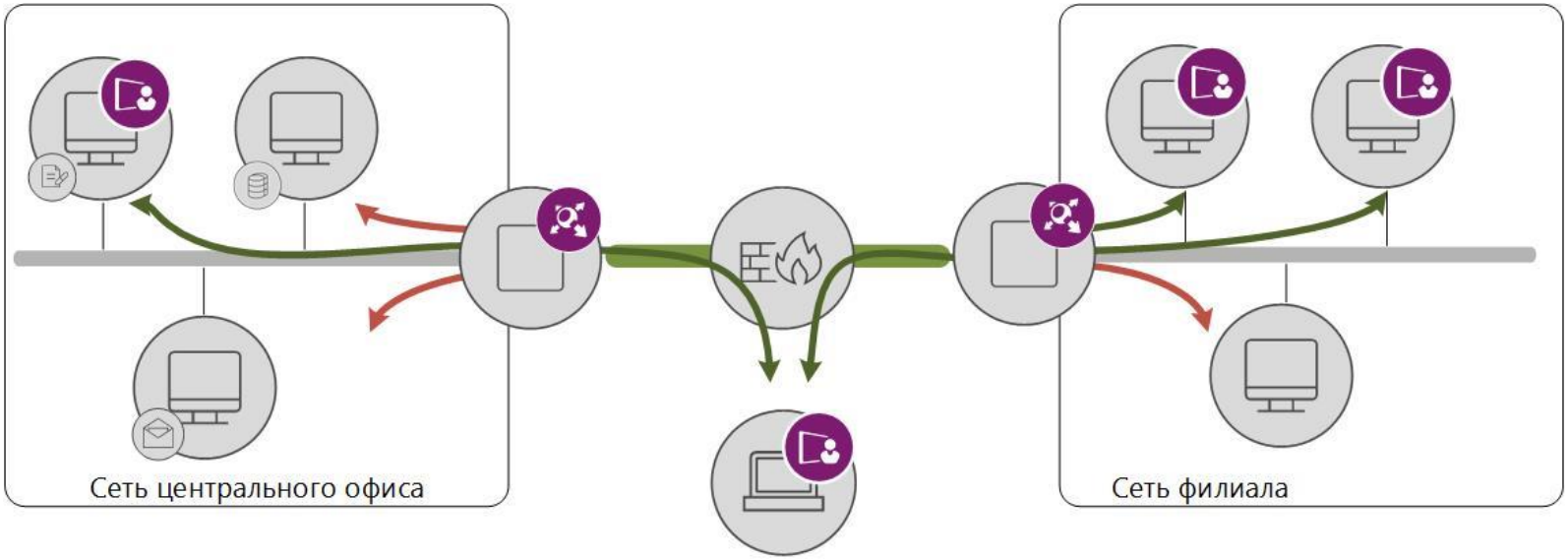
- от открытого узла до туннелирующего координатора трафик передается в открытом виде;
- на координаторе трафик подвергается фильтрации и шифрованию, после чего передается дальше в зашифрованном виде;
- на координаторе, туннелирующем узел получателя, трафик расшифровывается и передается на узел в открытом виде.

Защита трафика открытых узлов

Туннелирование IP-трафика

Туннелирующий координатор – координатор, за которым находится открытый узел и который с помощью туннелирования защищает трафик открытого узла.

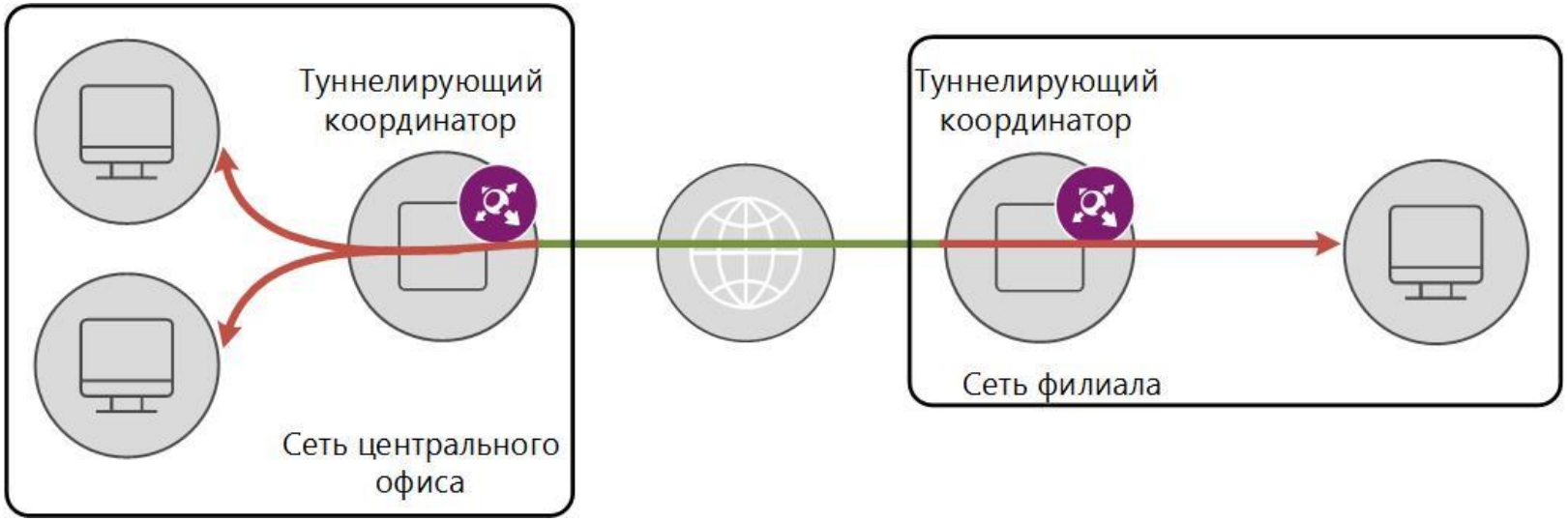
Туннелируемый ресурс – незащищенный компьютер, трафик которого защищается при передаче через открытые сети с помощью процедуры туннелирования.



Защита трафика открытых узлов

Туннелирование IP-трафика

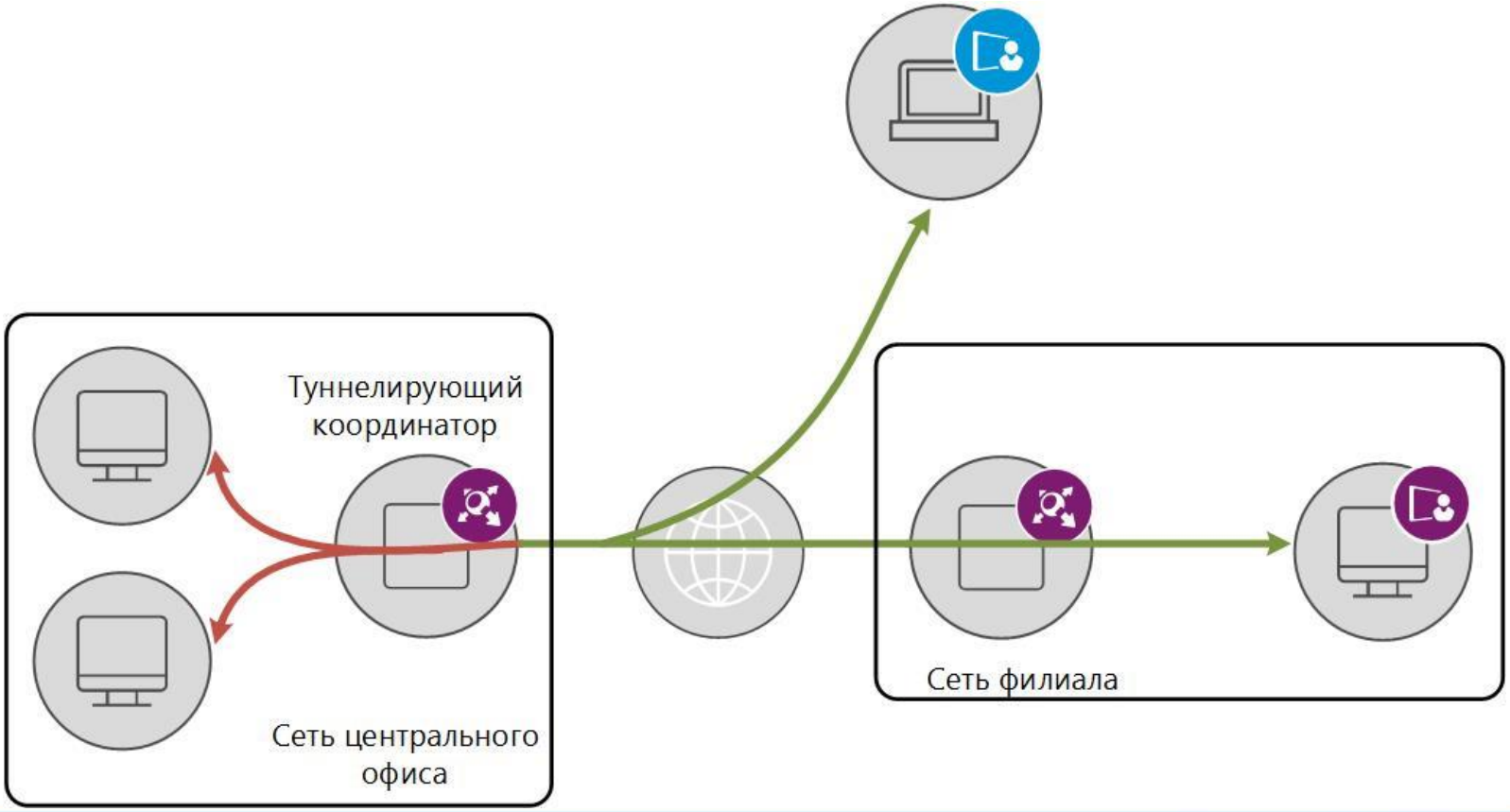
Туннель О-О – процедура туннелирования открытого трафика между двумя Открытыми узлами, входящими в состав разных защищенных сегментов ViPNet-сети.



Защита трафика открытых узлов

Туннелирование IP-трафика

Полутуннель О-З – процедура туннелирования открытого трафика между Открытым ресурсом и Защищенным узлом, которые входят в состав разных защищенных сегментов ViPNet-сети.



Защита трафика открытых узлов

Способы задания узлов для туннелирования

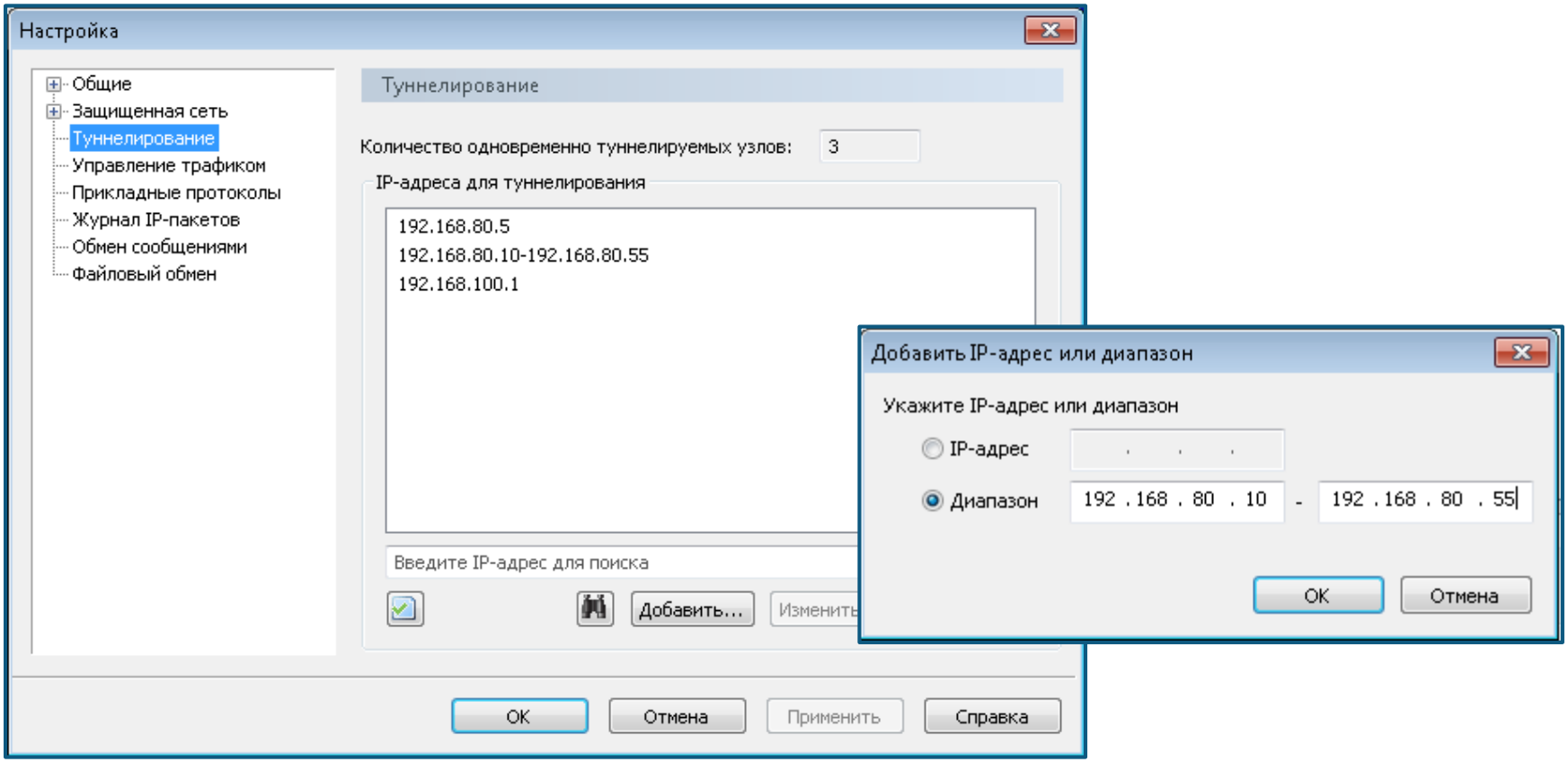
В программе ViPNet Administrator необходимо указать для этого координатора *максимально допустимое число одновременно туннелируемых соединений*.

Два способа задания узлов для туннелирования:

- В программе **ViPNet Центр управления сетью**. (централизованно): после рассылки новых справочников адреса туннелируемых узлов будут переданы и на туннелирующий координатор, и на все клиенты, связанные с этим координатором.
- В программе **ViPNet Монитор** (для небольшого количества узлов): адреса туннелируемых узлов необходимо задать на туннелирующем координаторе и на каждом сетевом узле, который должен иметь доступ к туннелируемым узлам.

Настройка ViPNet Coordinator

Задание узлов для туннелирования



Внимание! Задание туннелируемых IP-адресов в программе ViPNet ЦУС перекрывает все настройки, сделанные ранее на координаторах вручную.

Настройка сетевого экрана

Группы объектов:

- объединяют несколько значений одного типа;
- могут быть заданы при настройке параметров фильтра вместо отдельных объектов;
- позволяют упростить создание сетевых фильтров в программе ViPNet Монитор.

Настройка сетевого экрана

Виды групп объектов

Системные:

- встроены в ViPNet Coordinator;
- недоступны для редактирования;
- могут использоваться в сетевых фильтрах, а также в других; пользовательских группах объектов;
- не отображаются в списках групп.

Создаваемые в ViPNet Policy Manager:

- рассылаются вместе с политиками безопасности из ViPNet Policy Manager;
- недоступны для редактирования;
- нельзя использовать в сетевых фильтрах, правилах трансляции, других пользовательских группах объектов.

Настройка сетевого экрана

Виды групп объектов

Пользовательские:

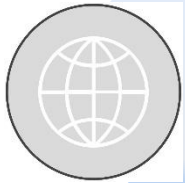
- создаются пользователем в программе ViPNet Монитор;
- работа с группами осуществляется в окне ViPNet Coordinator Монитор в разделе «Группы объектов».

Настройка сетевого экрана

Виды групп объектов

Узлы ViPNet

- группа узлов защищенной сети. Используется в фильтрах защищенной сети и туннелируемых узлов.



IP-адреса

- любая комбинация отдельных IP-адресов и диапазонов IP-адресов или DNS-имен. Используется в правилах трансляции IP-адресов и сетевых фильтрах, за исключением фильтров защищенной сети.

Протоколы

- любая комбинация протоколов и портов. Используется во всех фильтрах и правилах трансляции IP-адресов.

Расписания

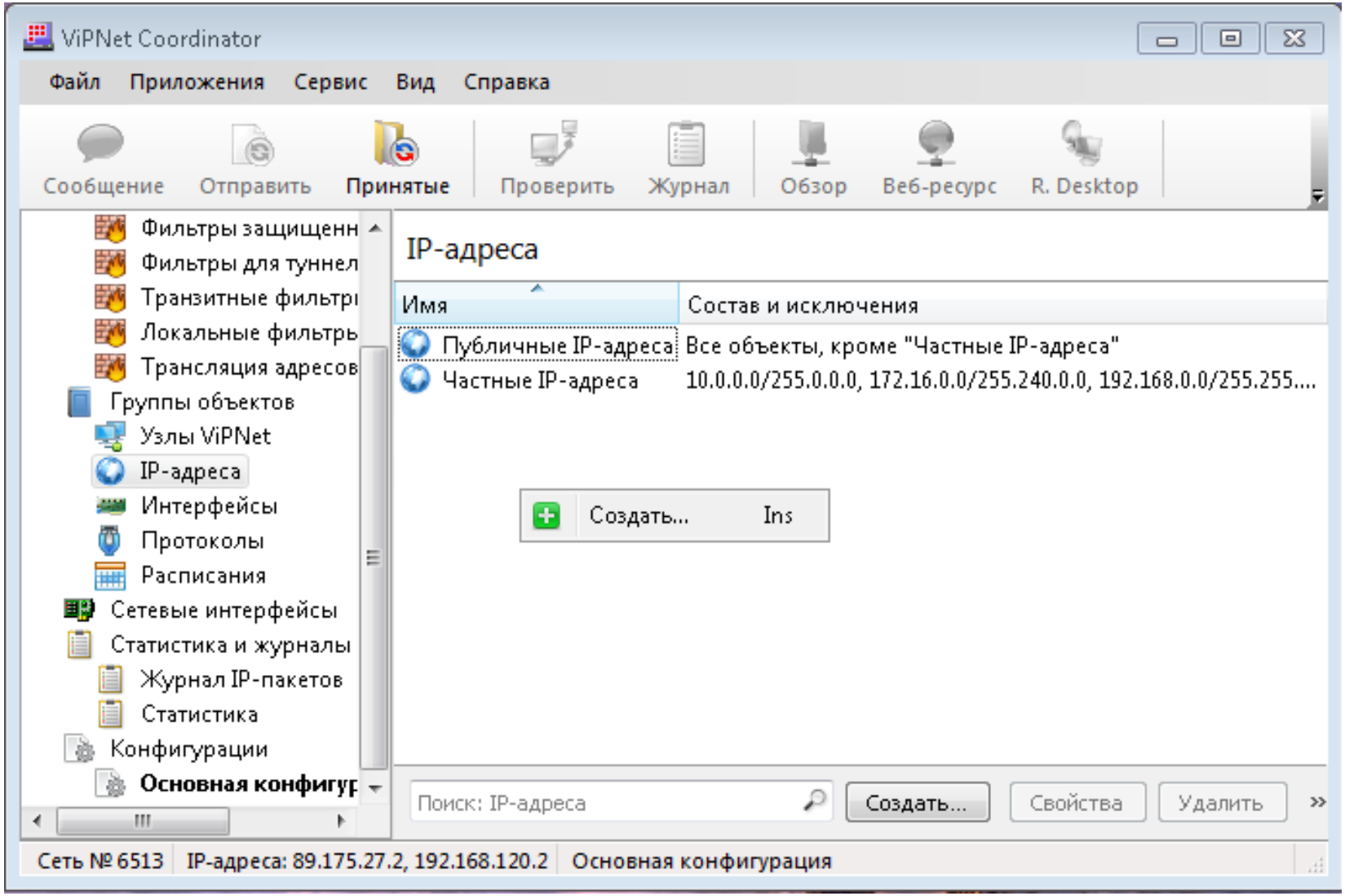
- любая комбинация условий применения сетевых фильтров по времени и дням недели. Используется во всех фильтрах.

Интерфейсы

- любая комбинация сетевых интерфейсов или IP-адресов интерфейсов. Используется в сетевых фильтрах только на координаторе (за исключением фильтров защищенной сети).

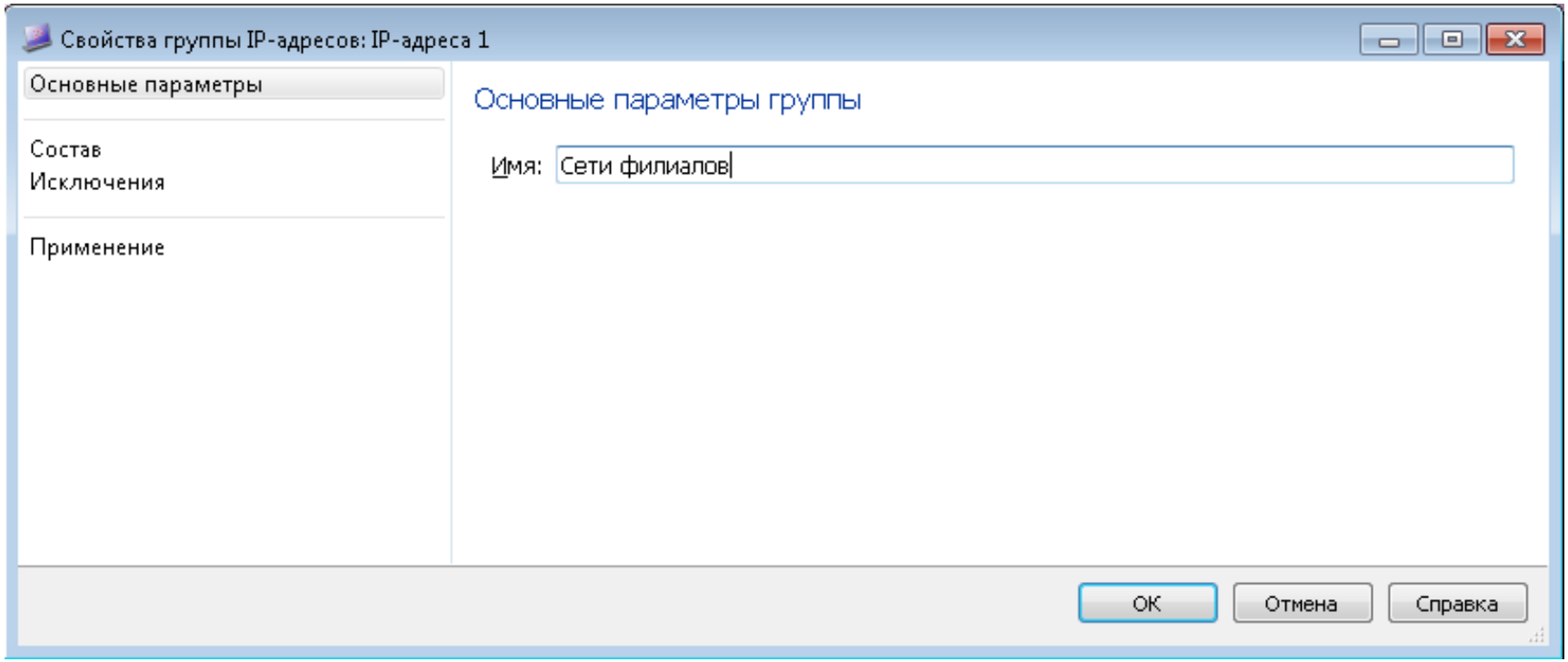
Настройка сетевого экрана

Создание группы объектов



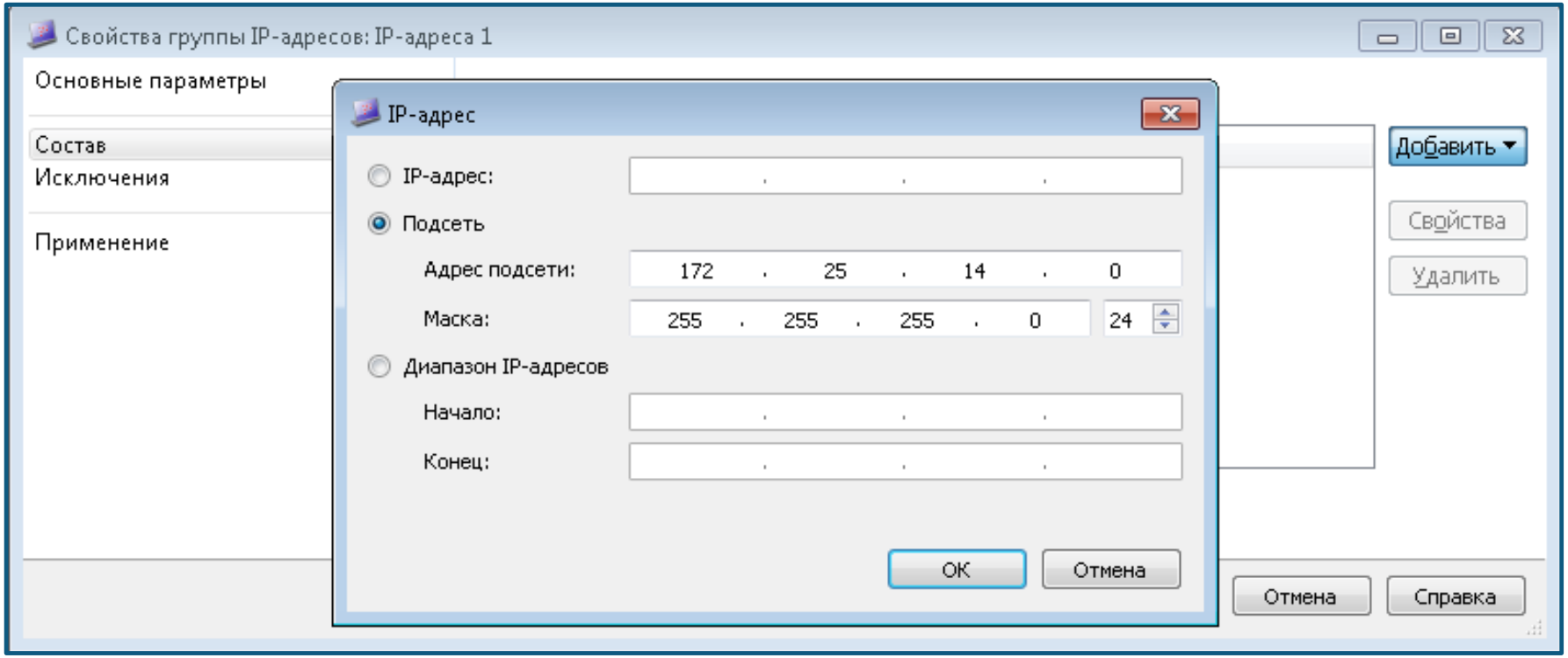
Настройка сетевого экрана

Создание группы объектов



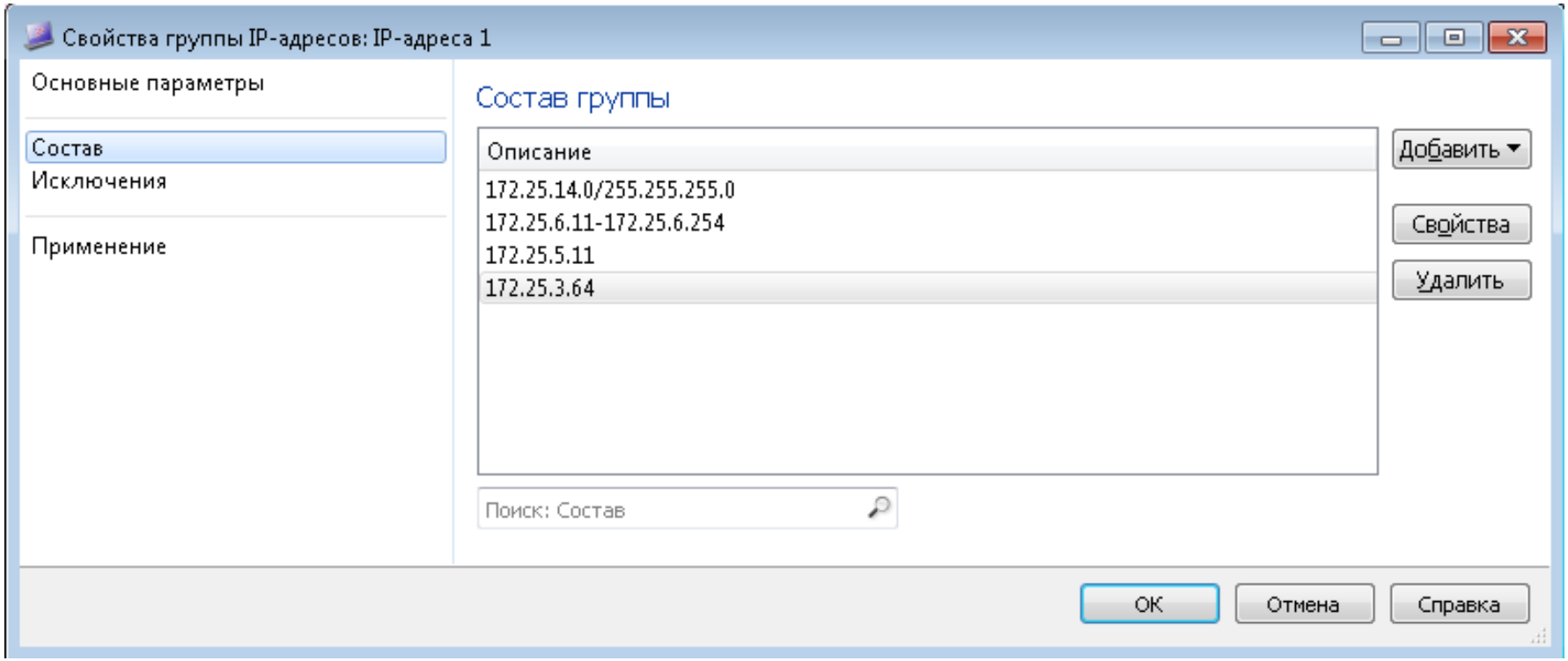
Настройка сетевого экрана

Создание группы объектов



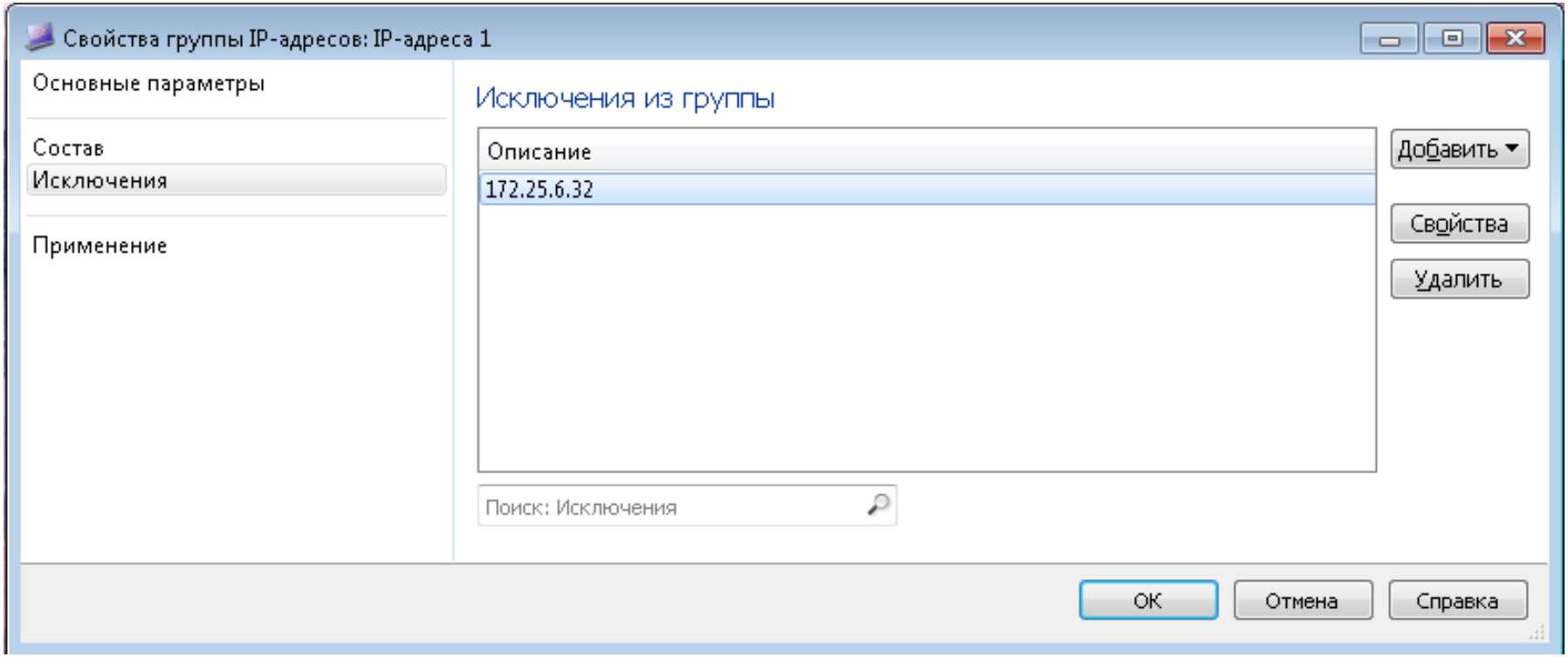
Настройка сетевого экрана

Создание группы объектов



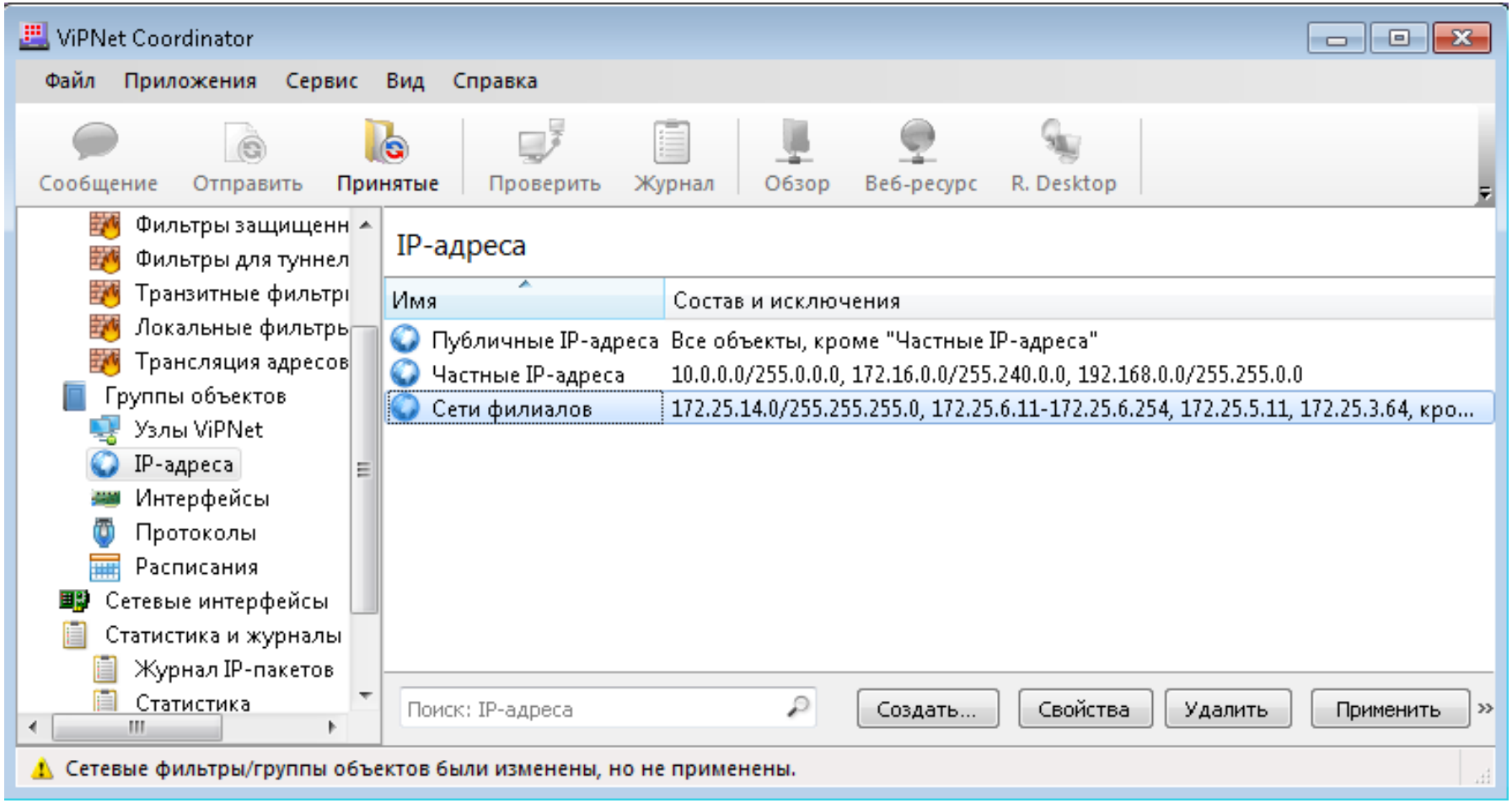
Настройка сетевого экрана

Создание группы объектов



Настройка сетевого экрана

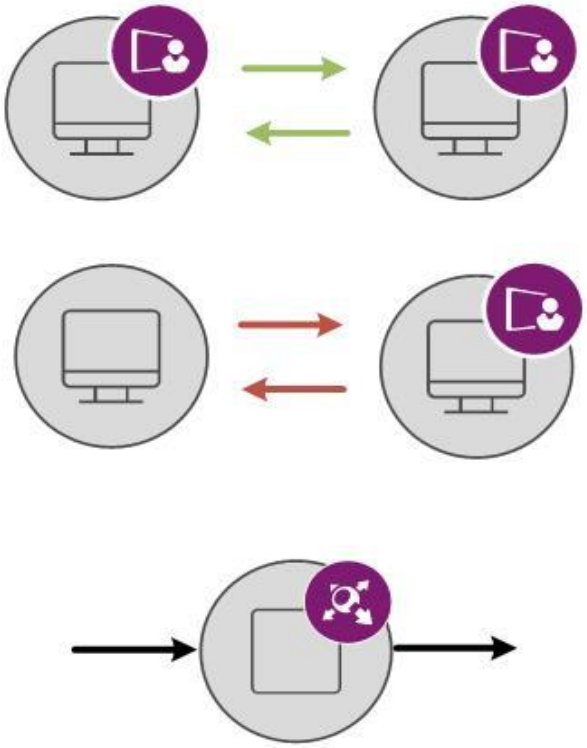
Создание группы объектов



Настройка сетевого экрана

Фильтрация трафика

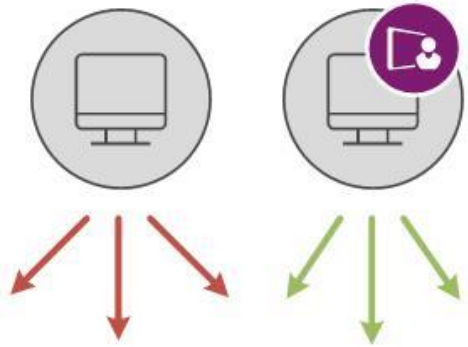
Фильтрации подвергается весь трафик, который проходит через сетевой узел ViPNet



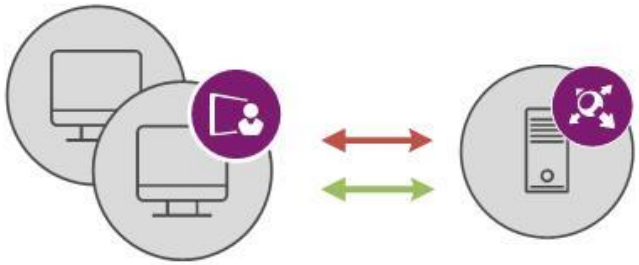
- защищенный (зашифрованный) трафик (перед его шифрованием и после расшифровки);
- открытый (нешифрованный) трафик;
- туннелируемый трафик (перед его шифрованием и после расшифровки).

Настройка сетевого экрана

Виды защищенного и открытого трафика



- Широковещательный трафик – IP-пакеты, у которых IP-адрес или MAC-адрес назначения является широковещательным адресом (то есть IP-пакеты передаются всем узлам определенного сегмента сети);



- Локальный трафик – входящий или исходящий трафик Координатора (то есть узел Координатора является отправителем или получателем IP-пакетов);

- Транзитный трафик – IP-пакеты, для которых Координатор не является ни отправителем, ни получателем. Транзитные IP-пакеты следуют через Координатор на другие узлы.

Настройка сетевого экрана

Последовательность фильтрации IP-пакетов:

- пакет проверяется системой обнаружения атак;
- пакет проверяется на соответствие правилам антиспуфинга;
- если IP-пакет соответствует параметрам одного из имеющихся сетевых фильтров, то он пропускается или блокируется в соответствии с этим фильтром;
- если пакет не соответствует ни одному из заданных фильтров, то он блокируется;
- как только пакет пропускается или блокируется, все последующие фильтры уже не действуют;
- сетевые фильтры к зашифрованным IP-пакетам применяются только после их успешной расшифровки и идентификации узла-источника.

Настройка сетевого экрана

Локальные и транзитные фильтры открытой сети:

- разрешают либо запрещают обмен IP-трафиком с открытыми узлами.

Локальные фильтры открытой сети

Вкл.	Действие	Имя	Источник	Назначение	Протокол	Расписание
Настраиваемые фильтры						
☑	Разрешить	DHCP-тра...	Все	Все	DHCP	Все
☑	Разрешить	NetBIOS- и...	Все	Все	NetBIOS-DGM	Все
☑	Разрешить	IGMP-траф...	Все	Все	IGMP	Все
☑	Разрешить	PING	Все	Все	PING	Все
Фильтры по умолчанию						
☑	Блокировать	Прочий тр...	Все	Все	Все	Все

Транзитные фильтры открытой сети

Вкл.	Действие	Имя	Источник	Назначение	Протокол	Расписание
Настраиваемые фильтры						
Фильтры по умолчанию						
☑	Блокировать	Прочий тр...	Все	Все	Все	Все

Настройка сетевого экрана

Фильтры для туннелируемых узлов:

- определяют правила для IP-пакетов, передаваемых между туннелируемыми узлами и узлами сети ViPNet, с которыми координатор имеет связь.

Фильтры для туннелируемых узлов

Вкл.	Действие	Имя	Источник	Назначение	Протокол	Расписание
Настраиваемые фильтры						
☑	Разрешить	Трафик от ...	Все	Туннелируемые IP-адреса	Все	Все
☑	Разрешить	Трафик от ...	Туннелируемые IP-адреса	Все	Все	Все
Фильтры по умолчанию						
☑	Блокировать	Прочий тр...	Все	Все	Все	Все

Настройка сетевого экрана

Порядок применения фильтров

Фильтры, определенные специальными конфигурациями:

- недоступны для редактирования;
- задаются конфигурацией или полномочиями.

1

Фильтры, поступившие в составе политик безопасности:

- недоступны для редактирования;
- создаются в программе ViPNet Policy Manager.

2

Предустановленные фильтры, фильтры, заданные пользователем:

- доступны для редактирования;
- предустановленные фильтры создаются программой.

3

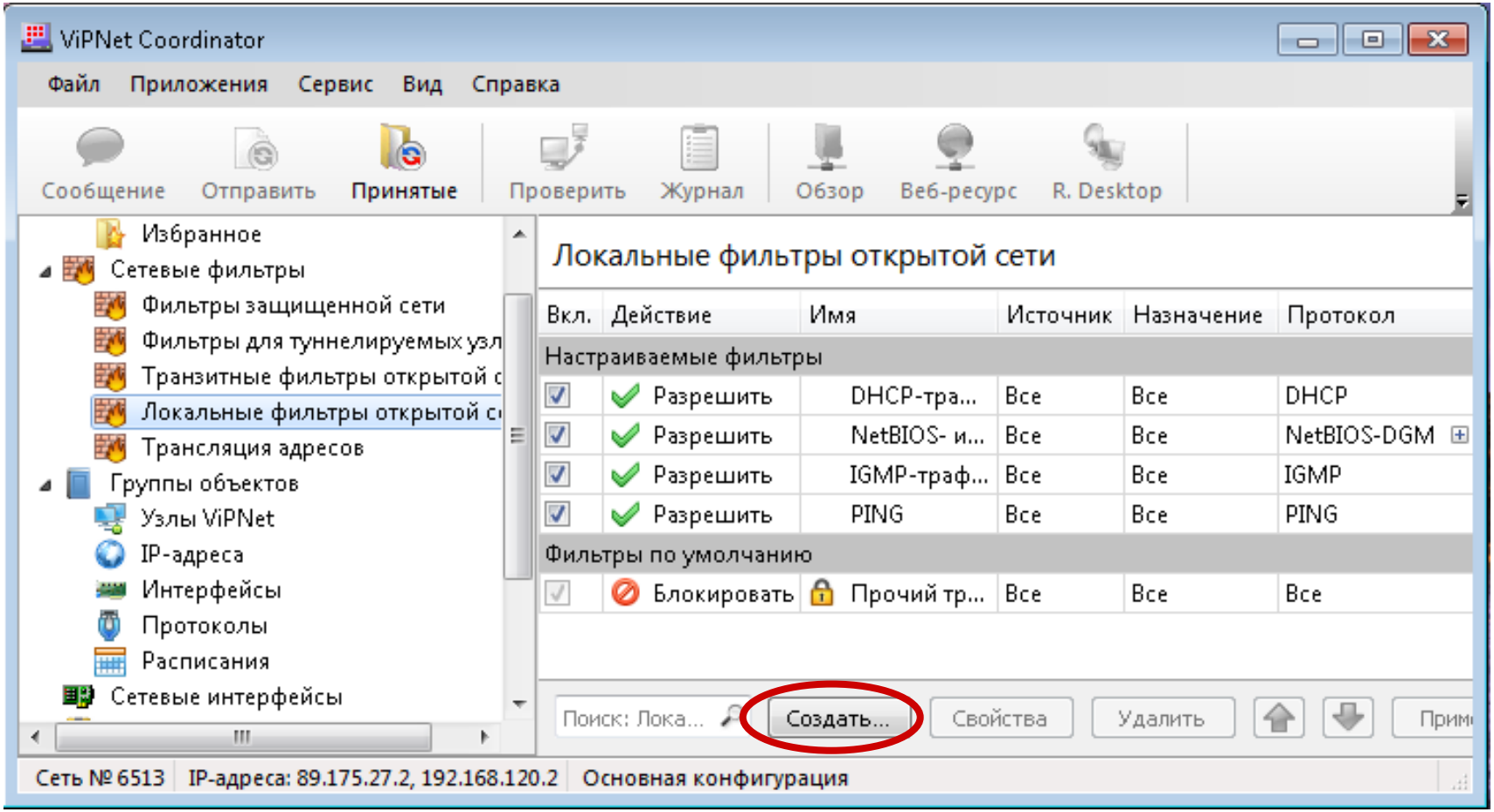
Фильтры, настроенные по умолчанию:

- недоступны для редактирования;
- создаются программой автоматически.

4

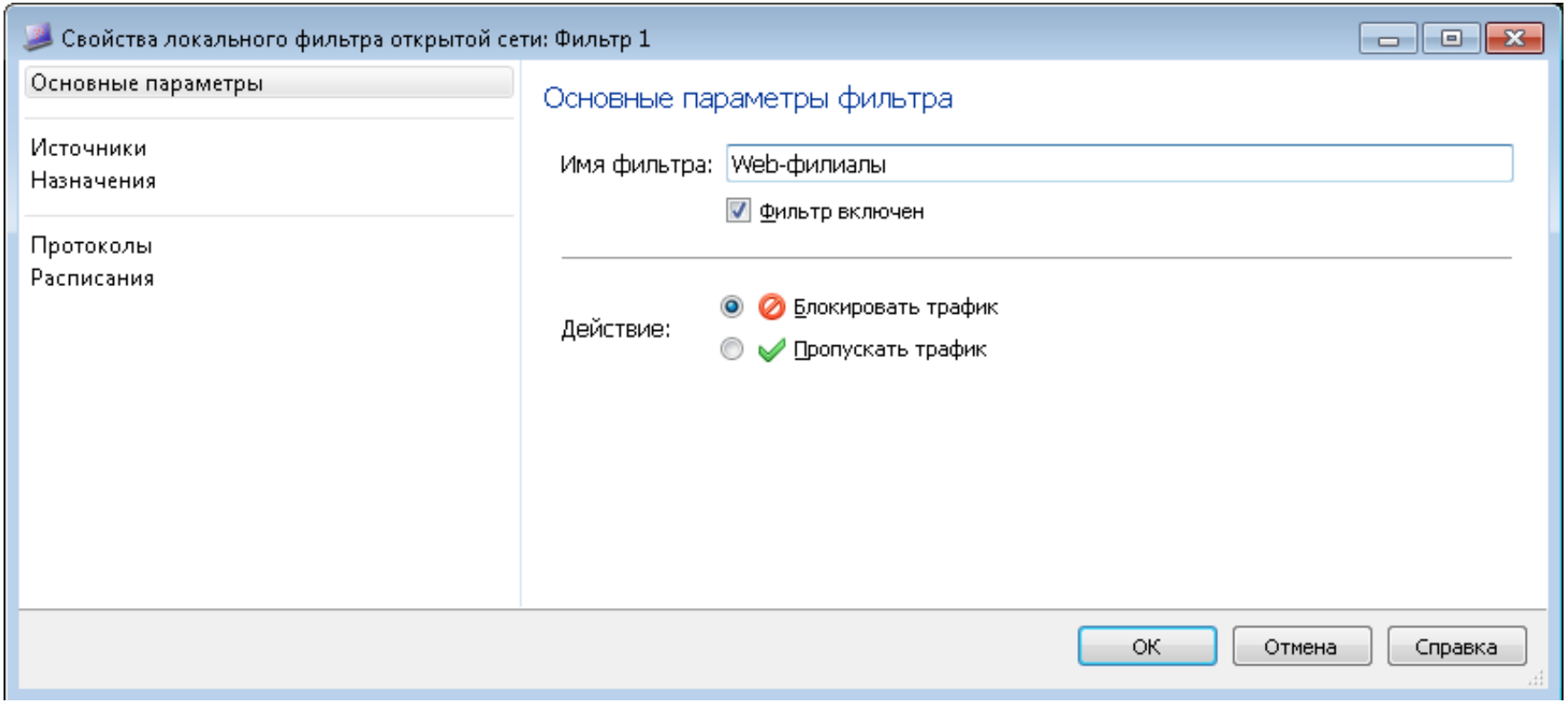
Настройка сетевого экрана

Создание сетевого фильтра



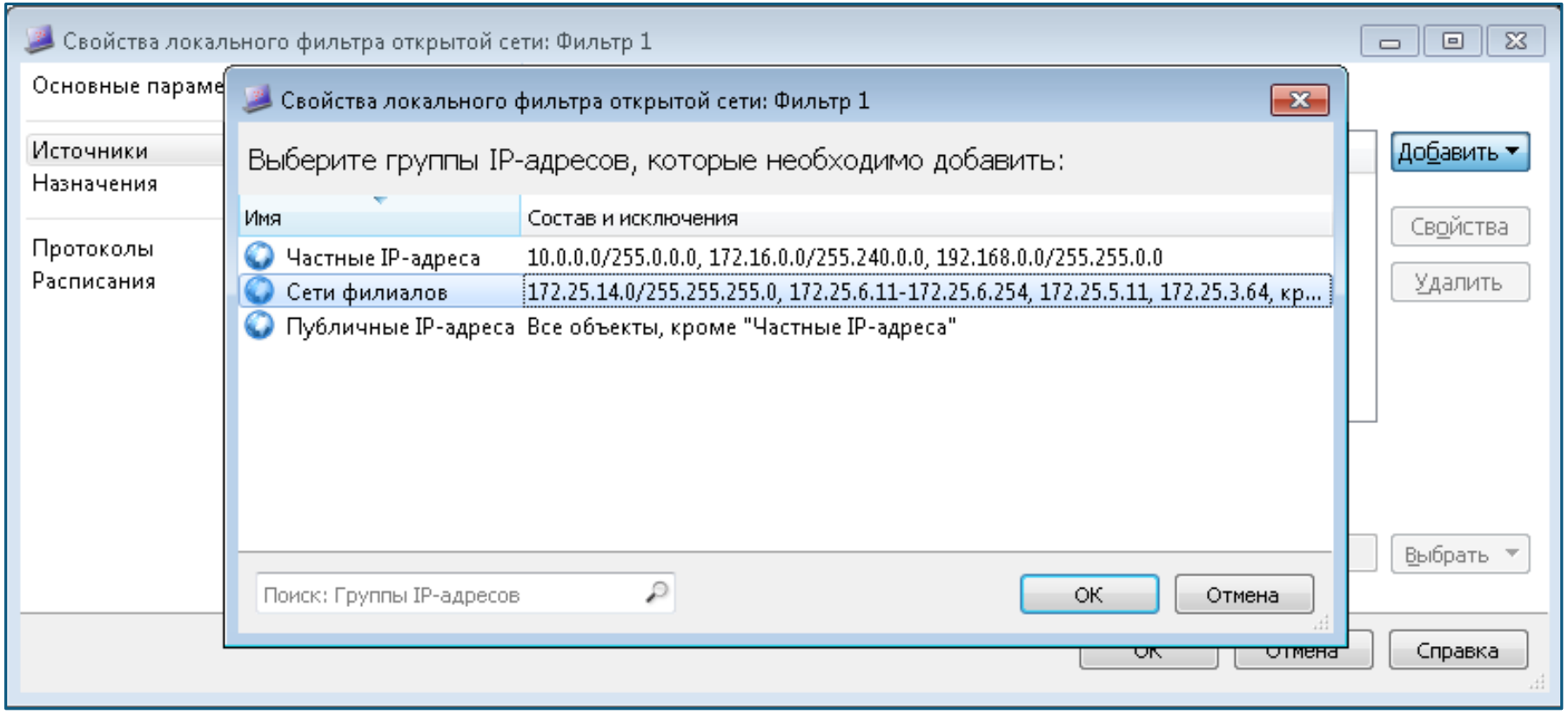
Настройка сетевого экрана

Создание сетевого фильтра



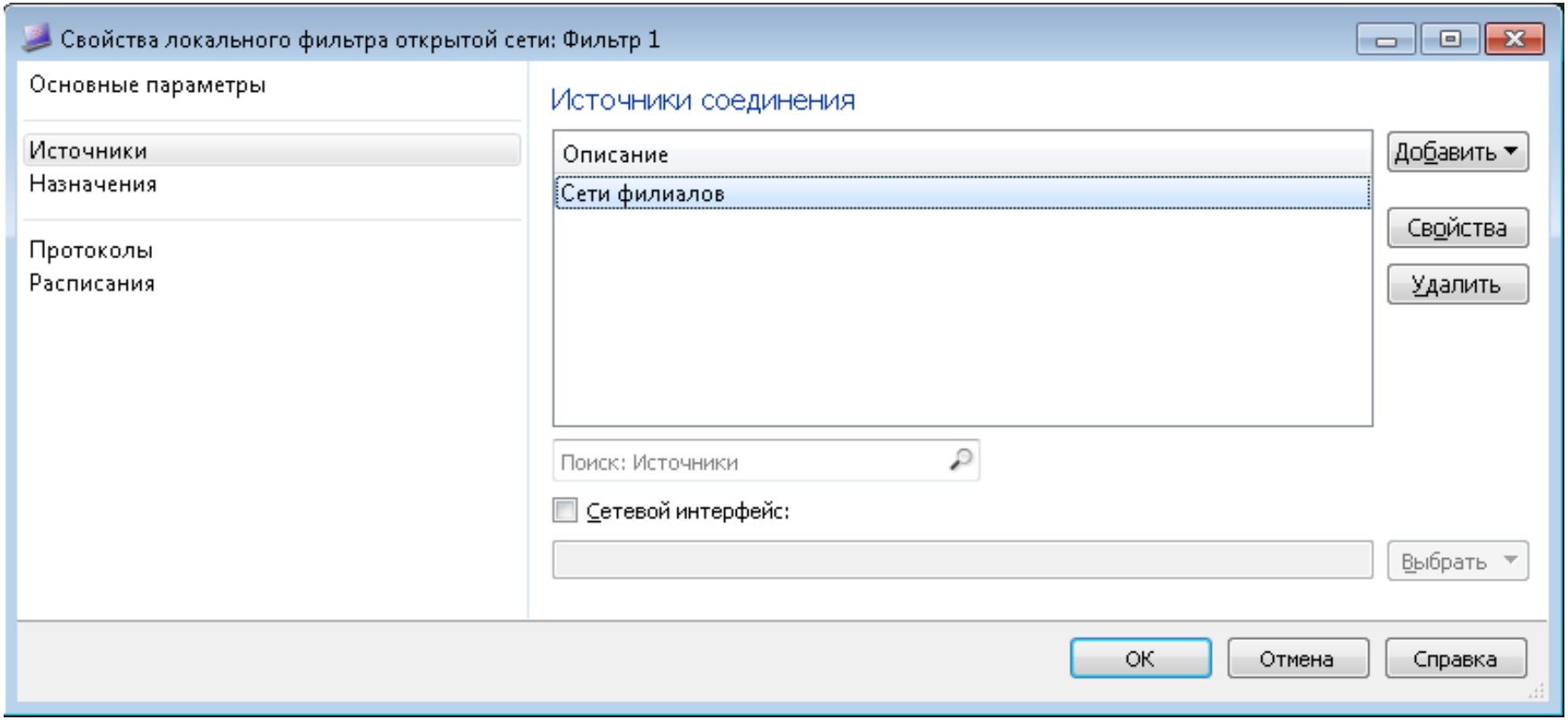
Настройка сетевого экрана

Создание сетевого фильтра



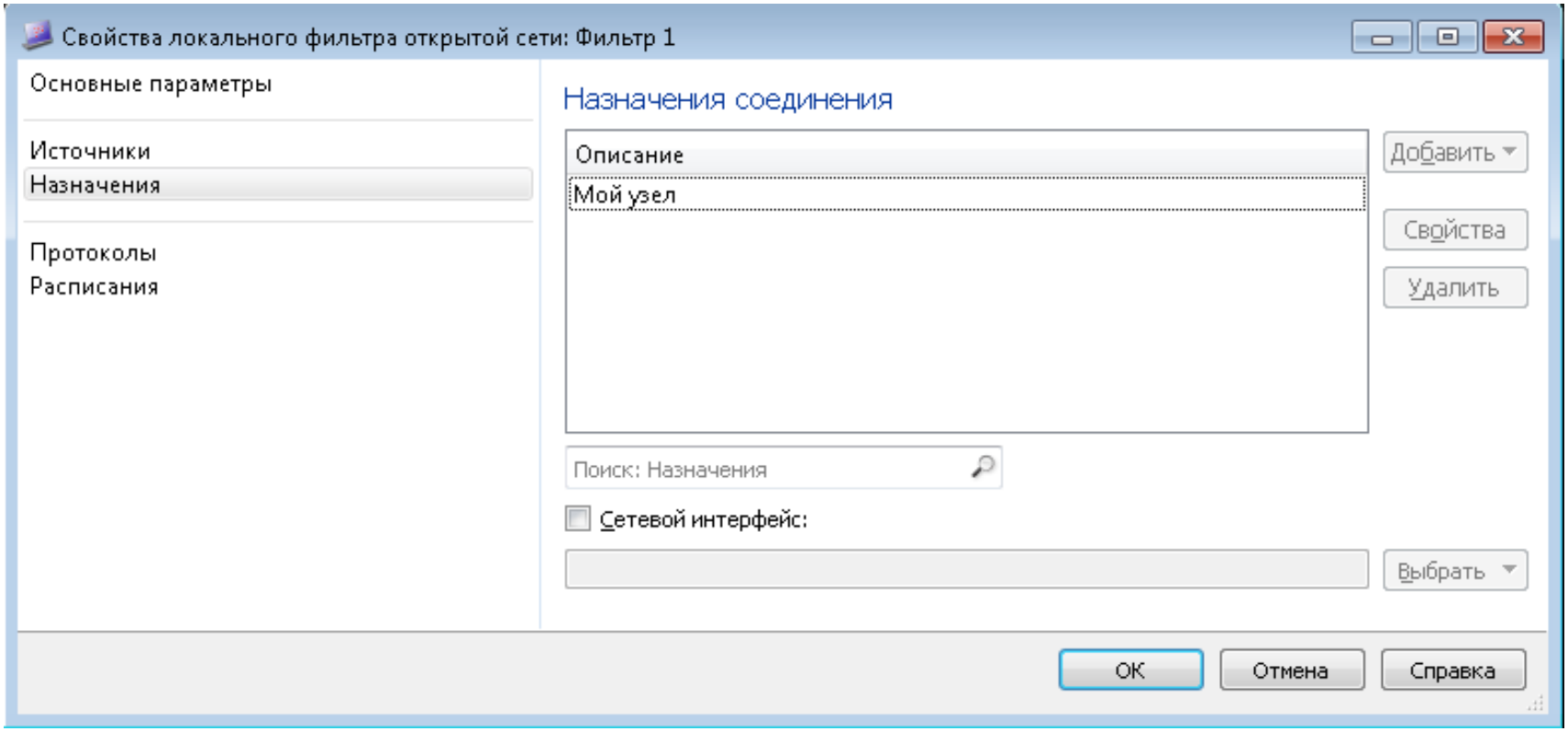
Настройка сетевого экрана

Создание сетевого фильтра



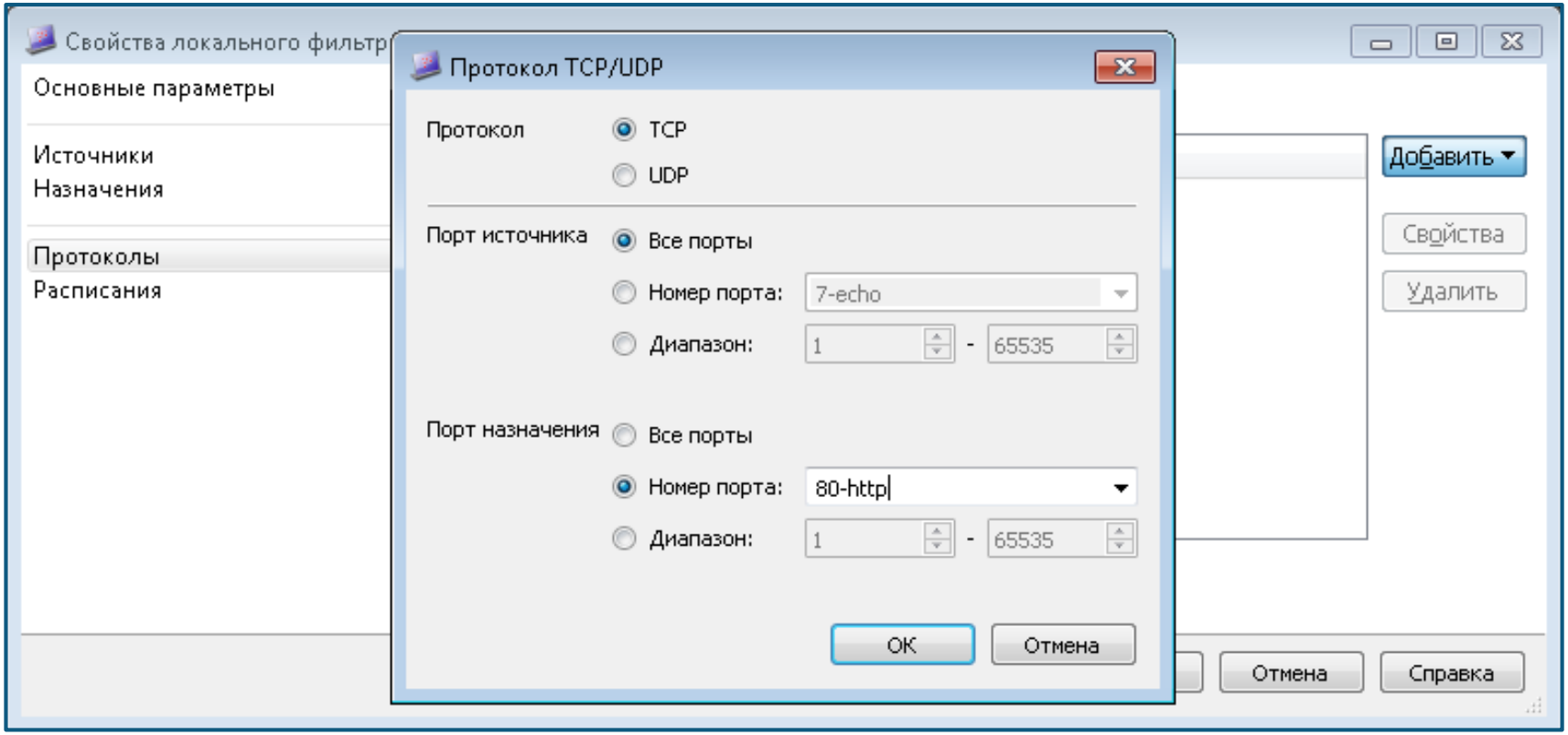
Настройка сетевого экрана

Создание сетевого фильтра



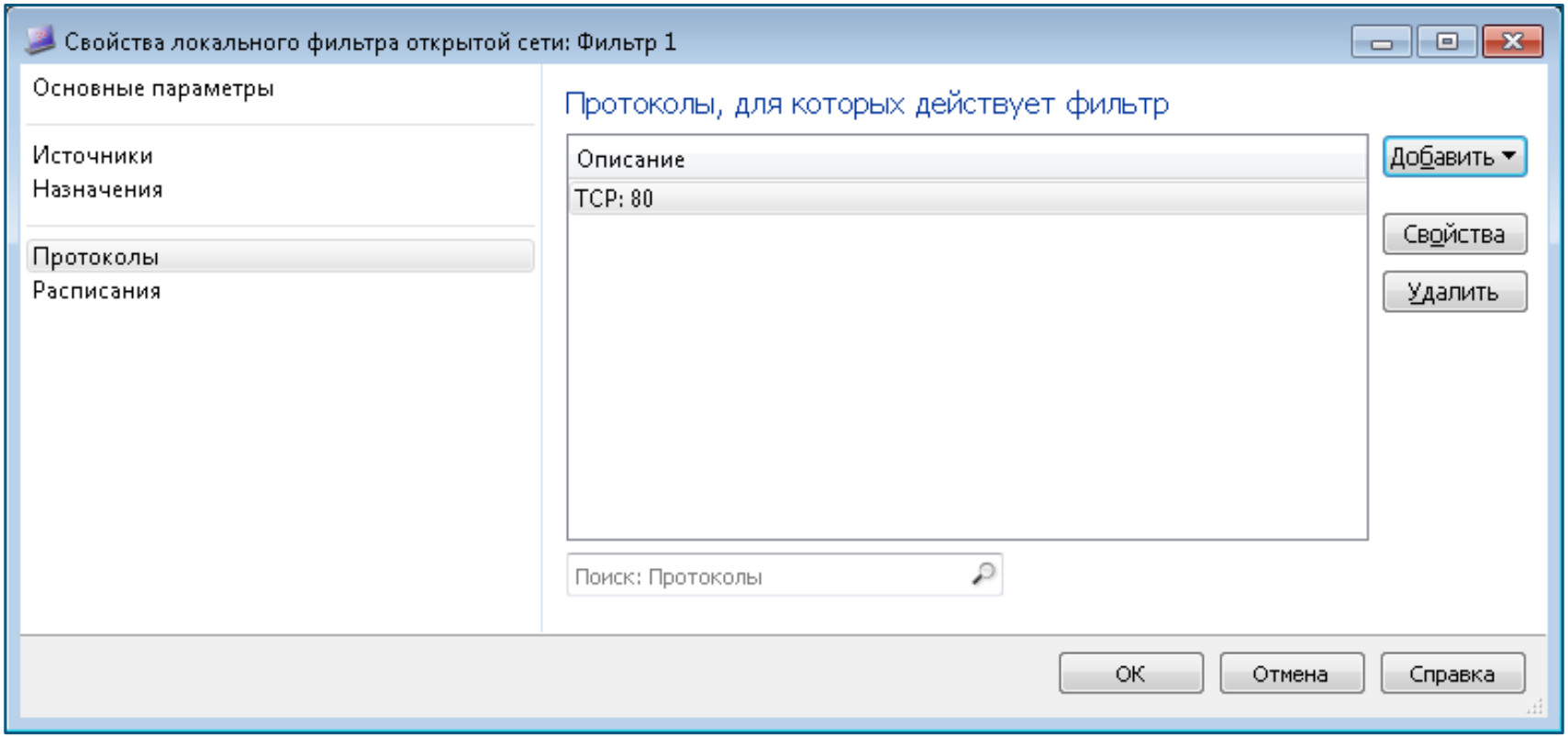
Настройка сетевого экрана

Создание сетевого фильтра



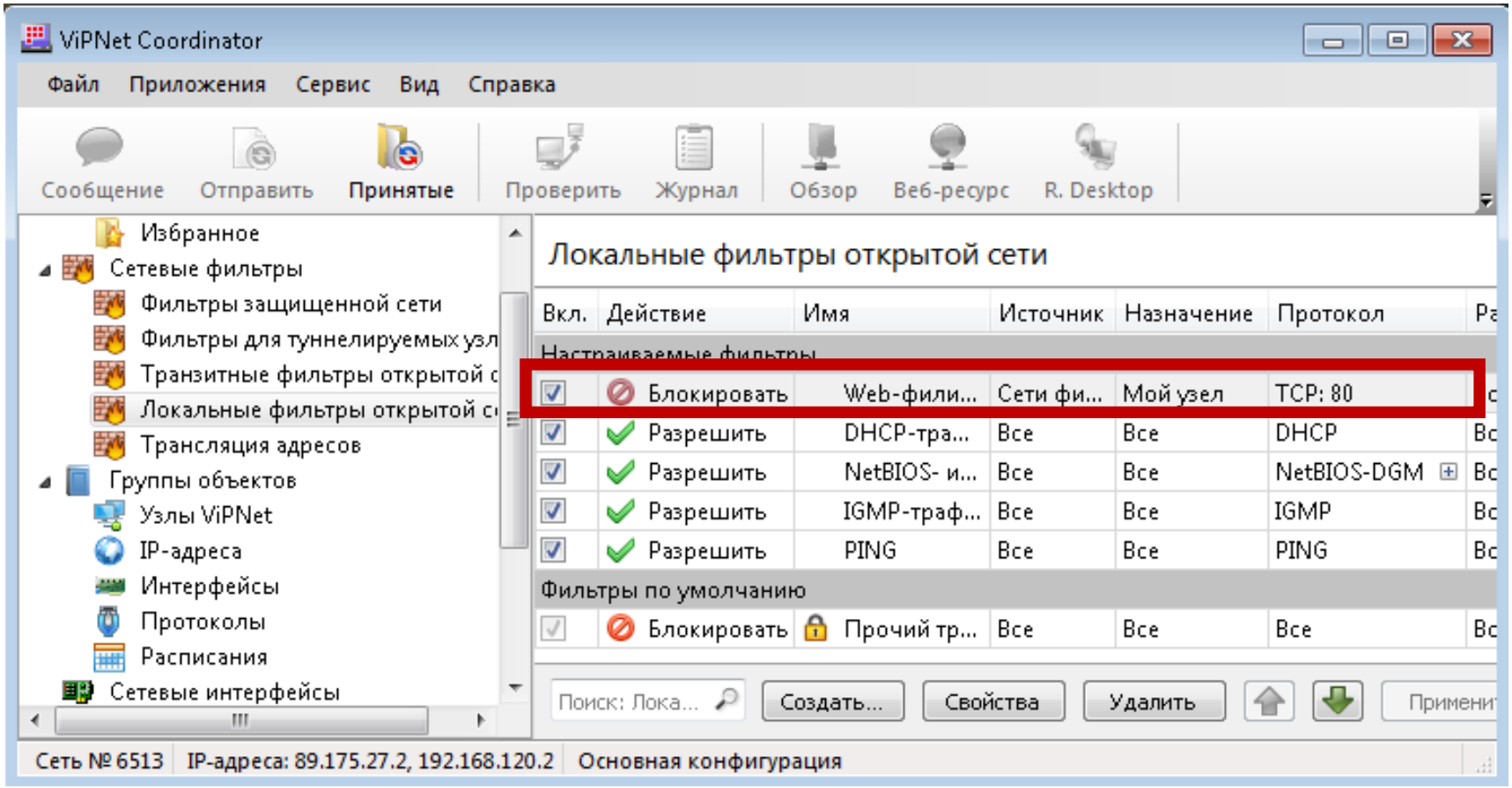
Настройка сетевого экрана

Создание сетевого фильтра



Настройка сетевого экрана

Создание сетевого фильтра



Настройка сетевого экрана

Трансляция сетевых адресов (NAT)

- **Трансляция сетевых адресов (Network Address Translation)** — это механизм преобразования IP-адресов одной сети в IP-адреса другой сети.

- Трансляция сетевых адресов применяется для решения двух основных задач:
  - для организации доступа из локальной сети с частными IP-адресами к ресурсам Интернета;
  - для организации доступа к внутренним ресурсам из внешней сети.
- Трансляция сетевых адресов осуществляется для IP-пакетов, проходящих через межсетевой экран из внутренней сети во внешнюю или наоборот.

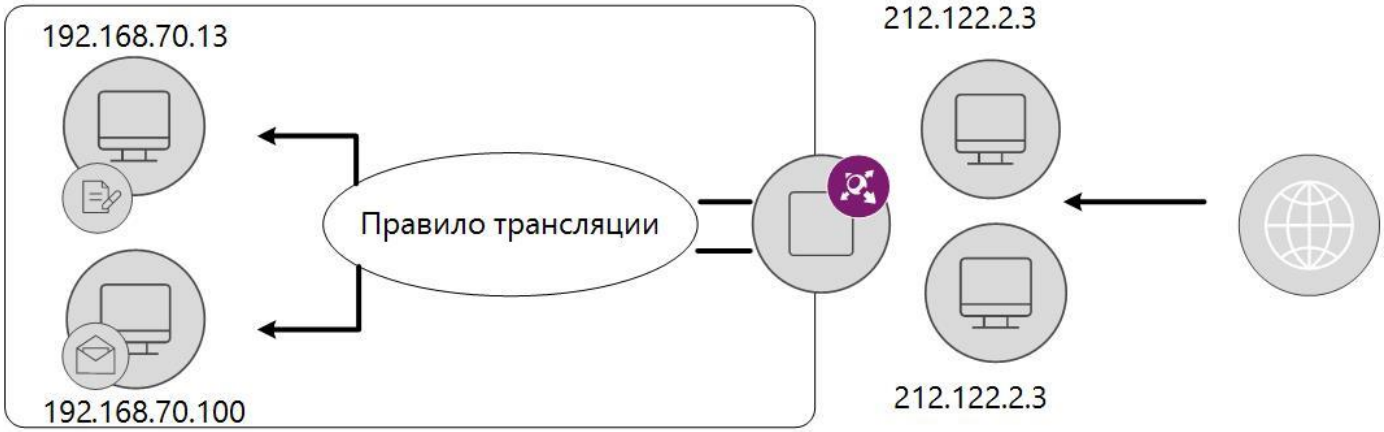
Внимание!

Правила трансляции относятся только к открытому трафику.
Для защищенного трафика действуют автоматически заданные механизмы трансляции адресов, параметры которых не могут быть изменены.

Настройка сетевого экрана

Трансляция адреса узла назначения

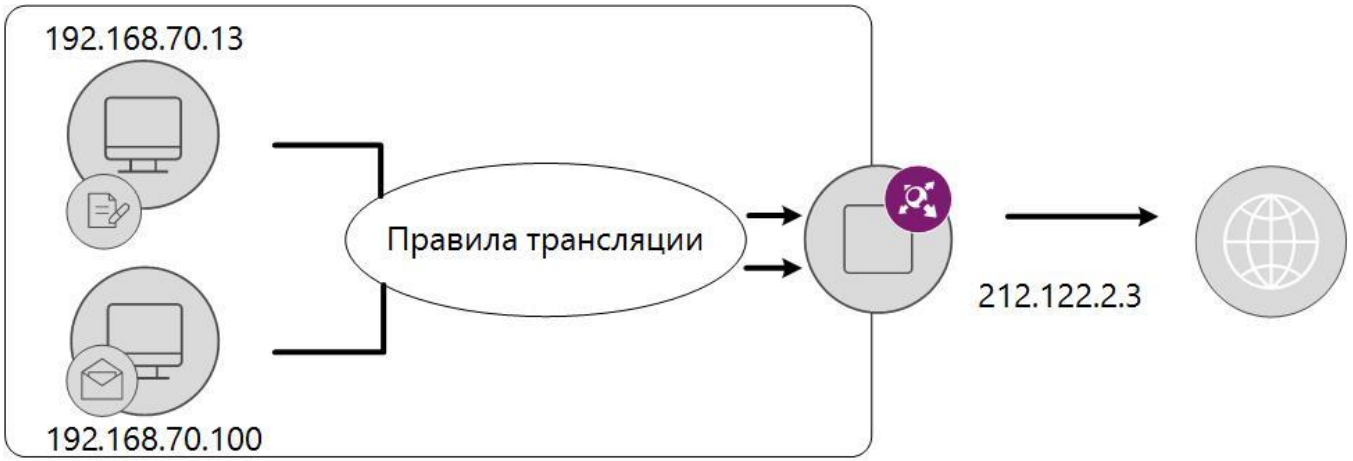
- Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных узлов публичный IP-адрес координатора.
- В заголовках IP-пакетов публичный IP-адрес назначения заменяется на частный адрес локальной сети. По публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.
- Трансляция адреса узла назначения предназначена для организации доступа из Интернета к серверам локальной сети, не имеющим публичного IP-адреса.



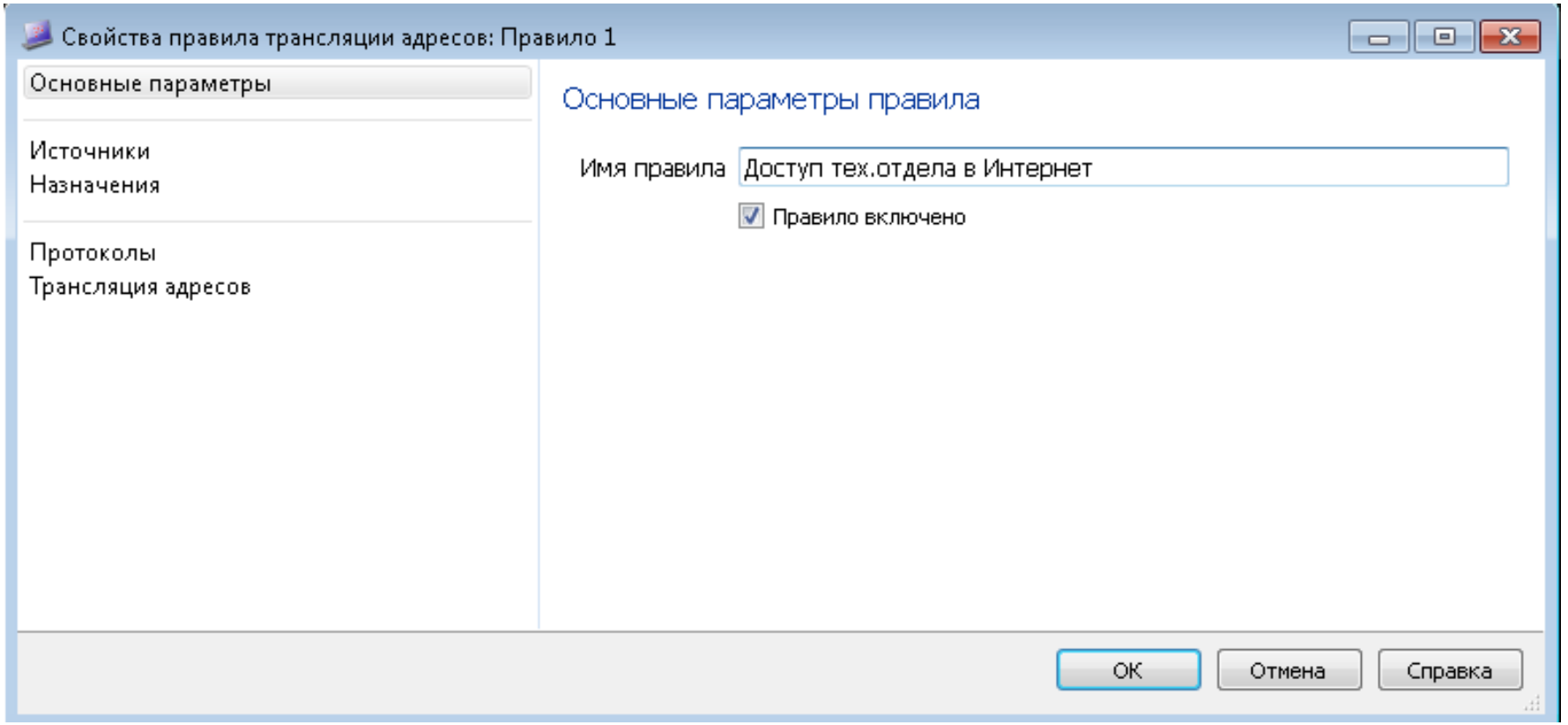
Настройка сетевого экрана

Трансляция адреса источника

- Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных узлов публичный IP-адрес координатора.
- В заголовках IP-пакетов частные IP-адреса источника заменяются на публичный IP-адрес координатора. Узлы локальной сети могут устанавливать соединения с узлами в Интернете от имени публичного IP-адреса координатора.
- Трансляция адреса источника предназначена для организации доступа компьютеров с частными IP-адресам в Интернет.

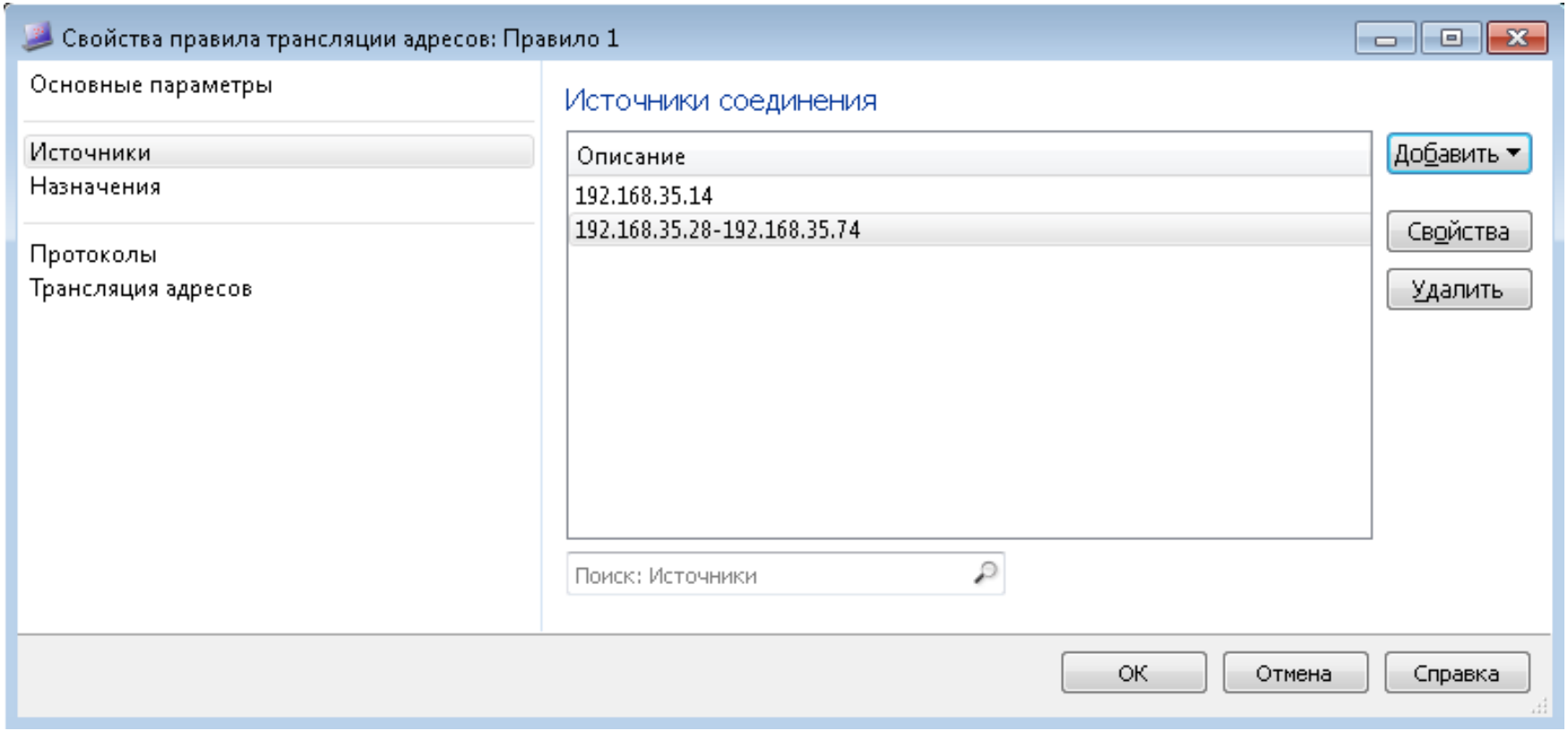


Создание правила трансляции адресов



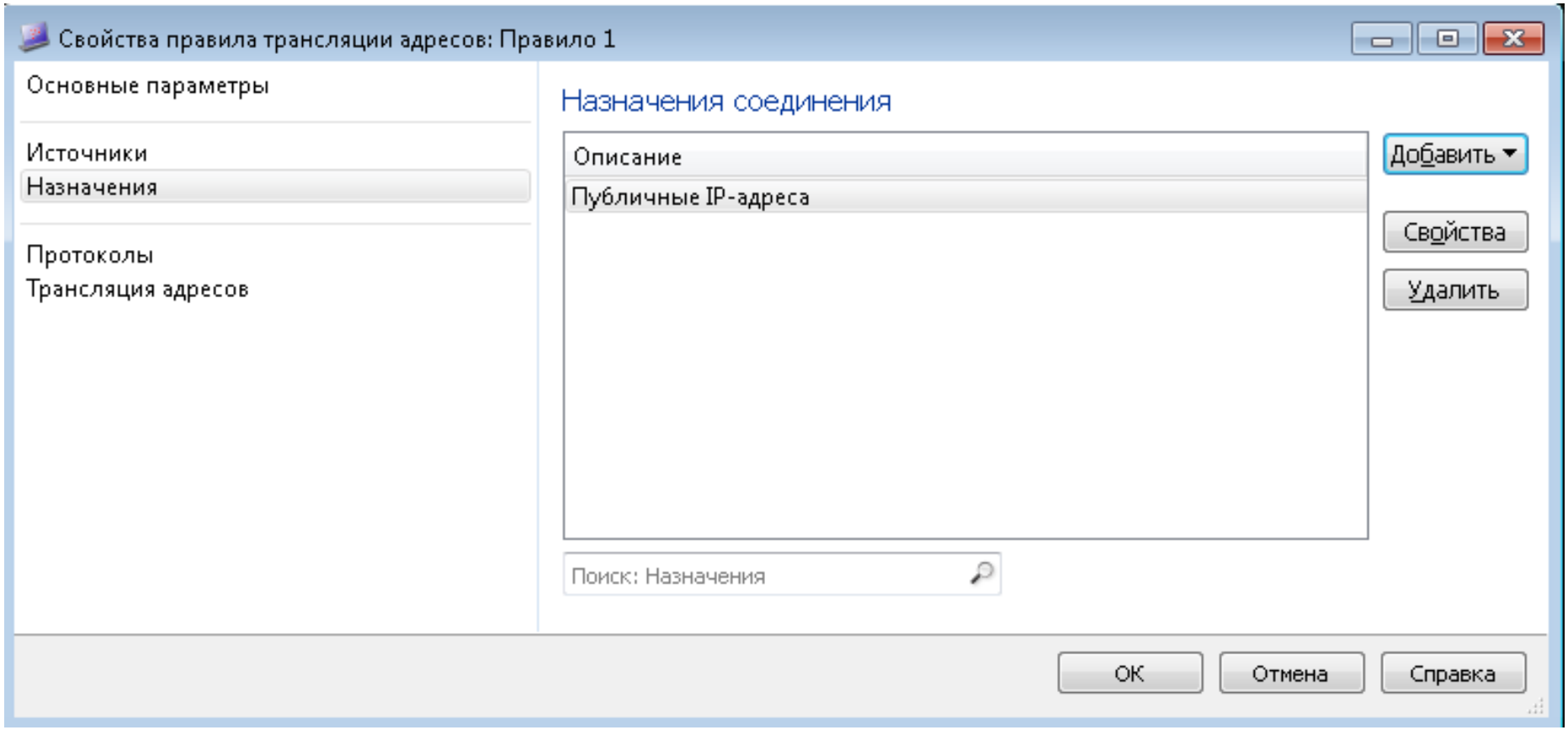
Настройка сетевого экрана

Создание правила трансляции адресов



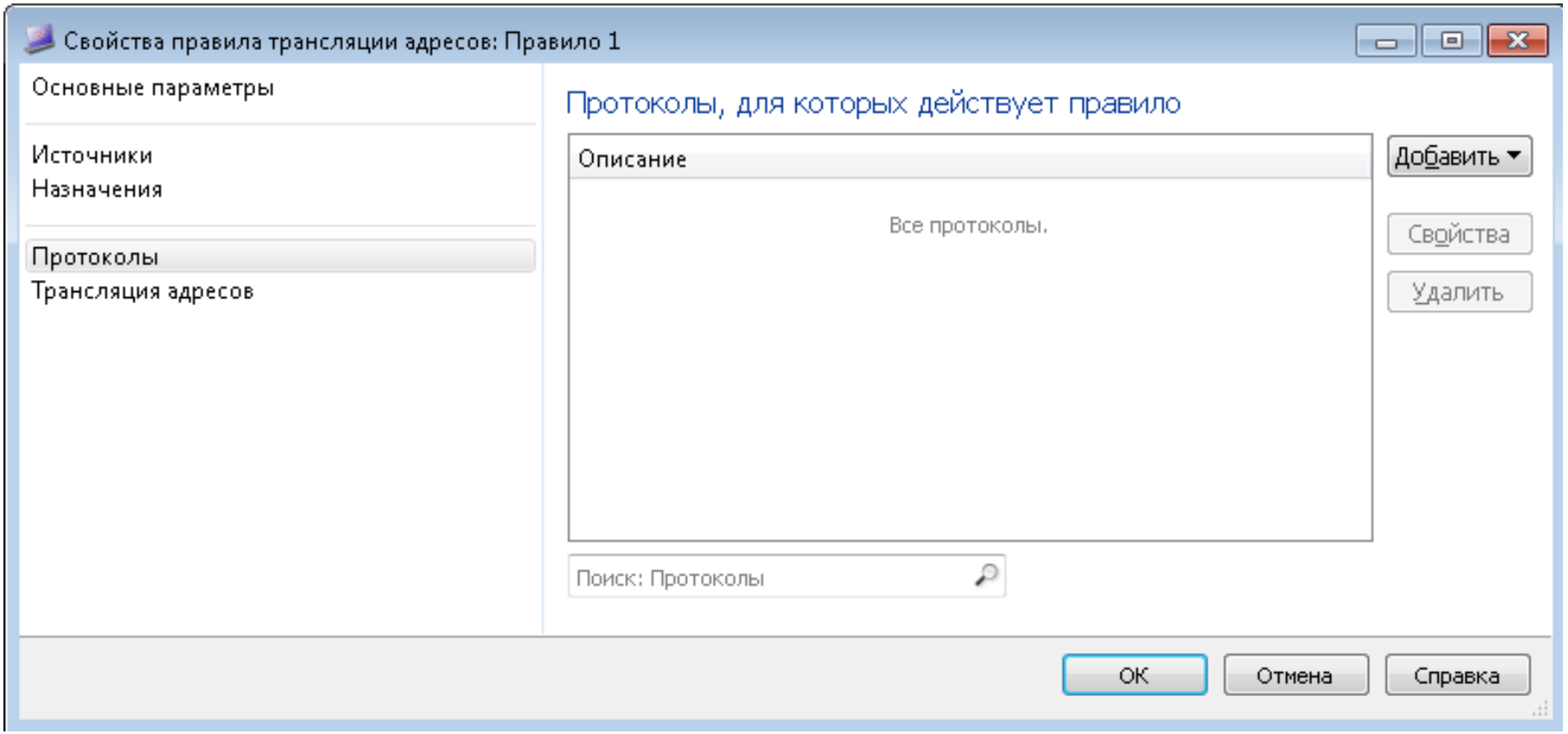
Настройка сетевого экрана

Создание правила трансляции адресов



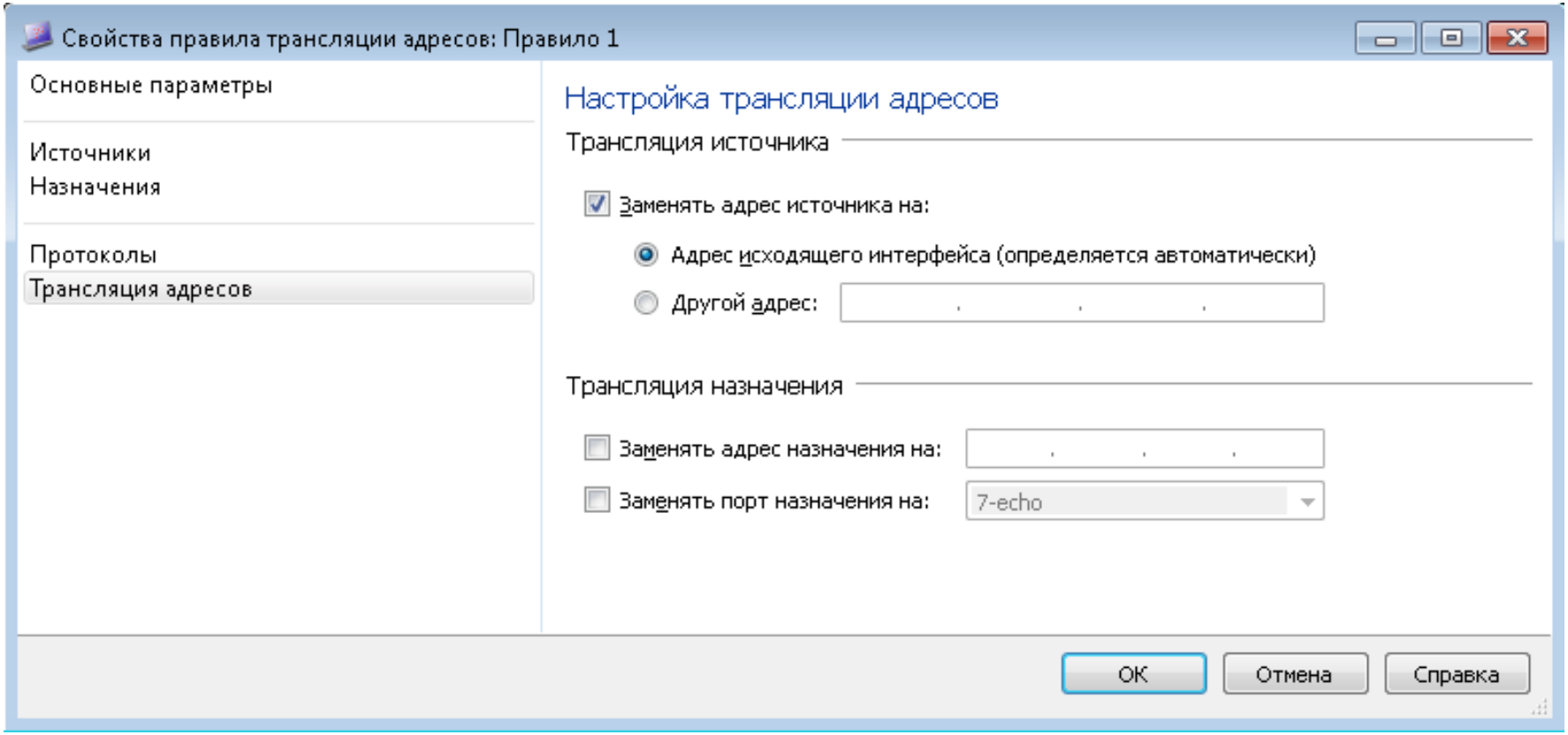
Настройка сетевого экрана

Создание правила трансляции адресов



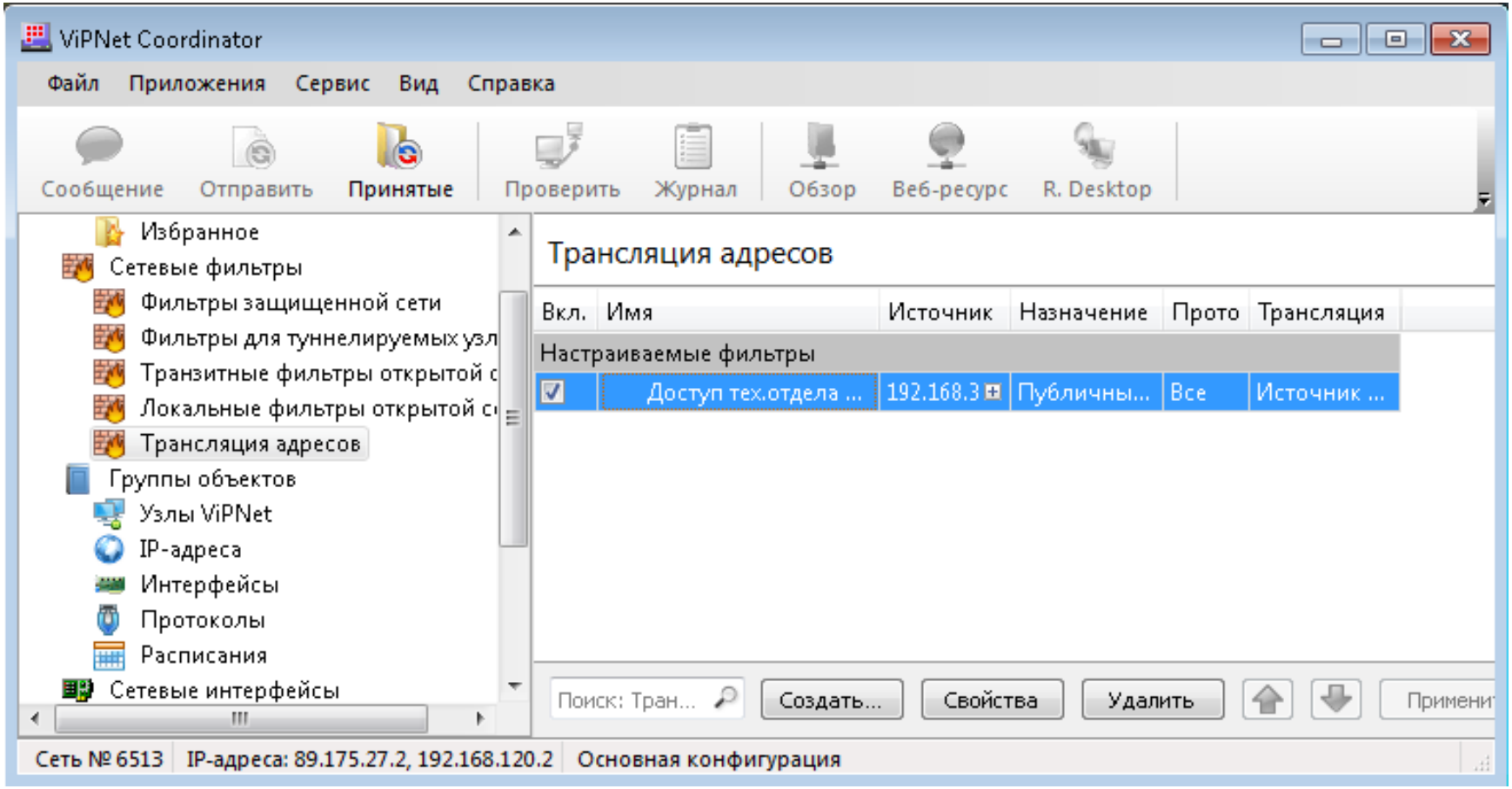
Настройка сетевого экрана

Создание правила трансляции адресов



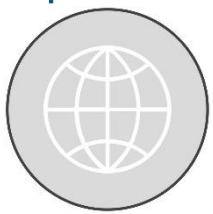
Настройка сетевого экрана

Создание правила трансляции адресов



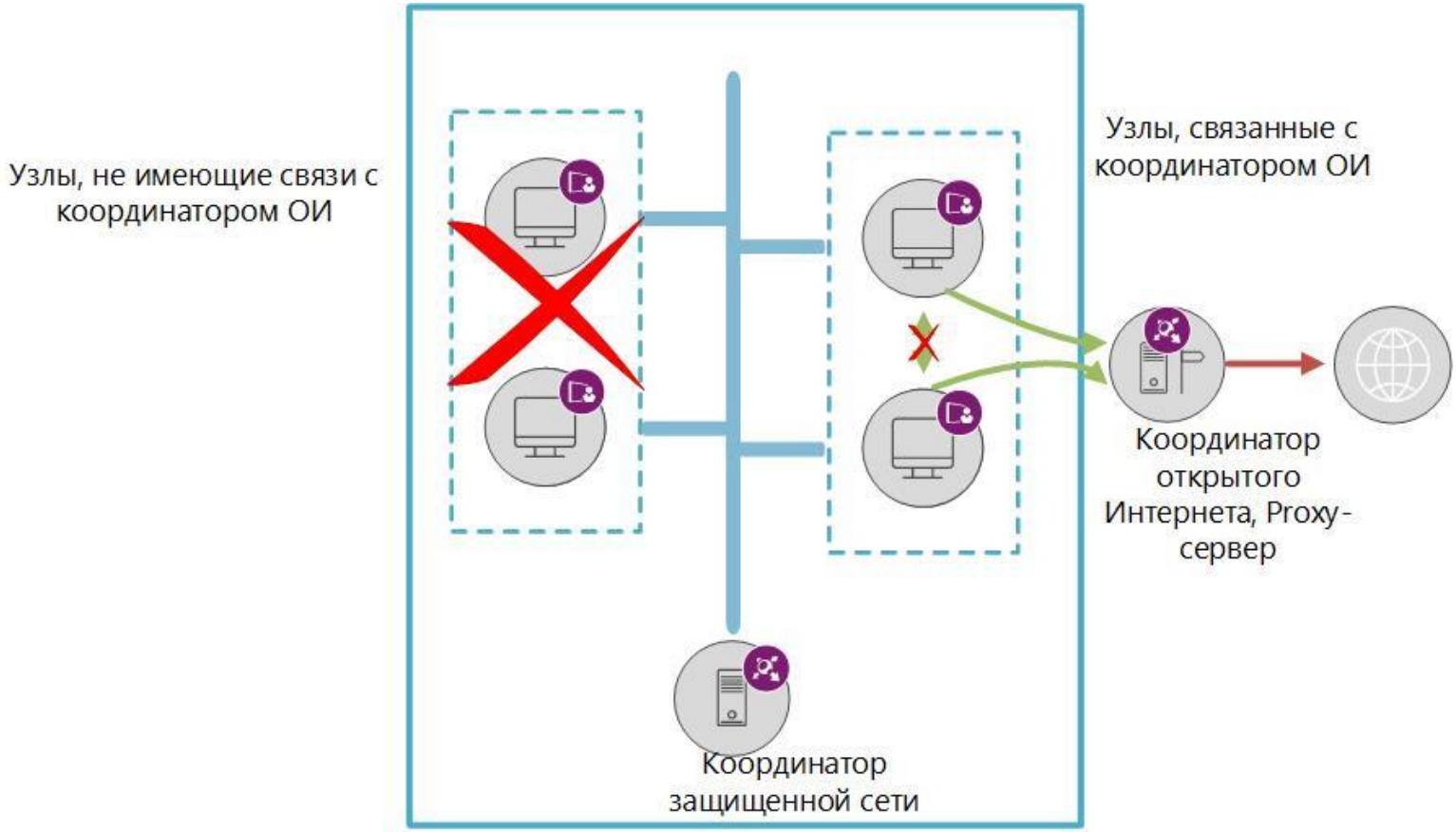
Технология «Открытый Интернет»

- **Технология «Открытый Интернет» позволяет организовать защищенный доступ к сети Интернет без физического отключения компьютеров от локальной сети.**
- **Использование технологии «Открытый Интернет» позволяет решить несколько задач:**
  - предоставить пользователям безопасный доступ в сеть Интернет;
  - исключить затраты на создание и обслуживание специальной выделенной сети, через которую пользователи получают доступ в сеть Интернет;
  - выполнить требования Российского законодательства по организации доступа к сети Интернет с компьютеров, на которых обрабатывается конфиденциальная информация.



Технология «Открытый Интернет»

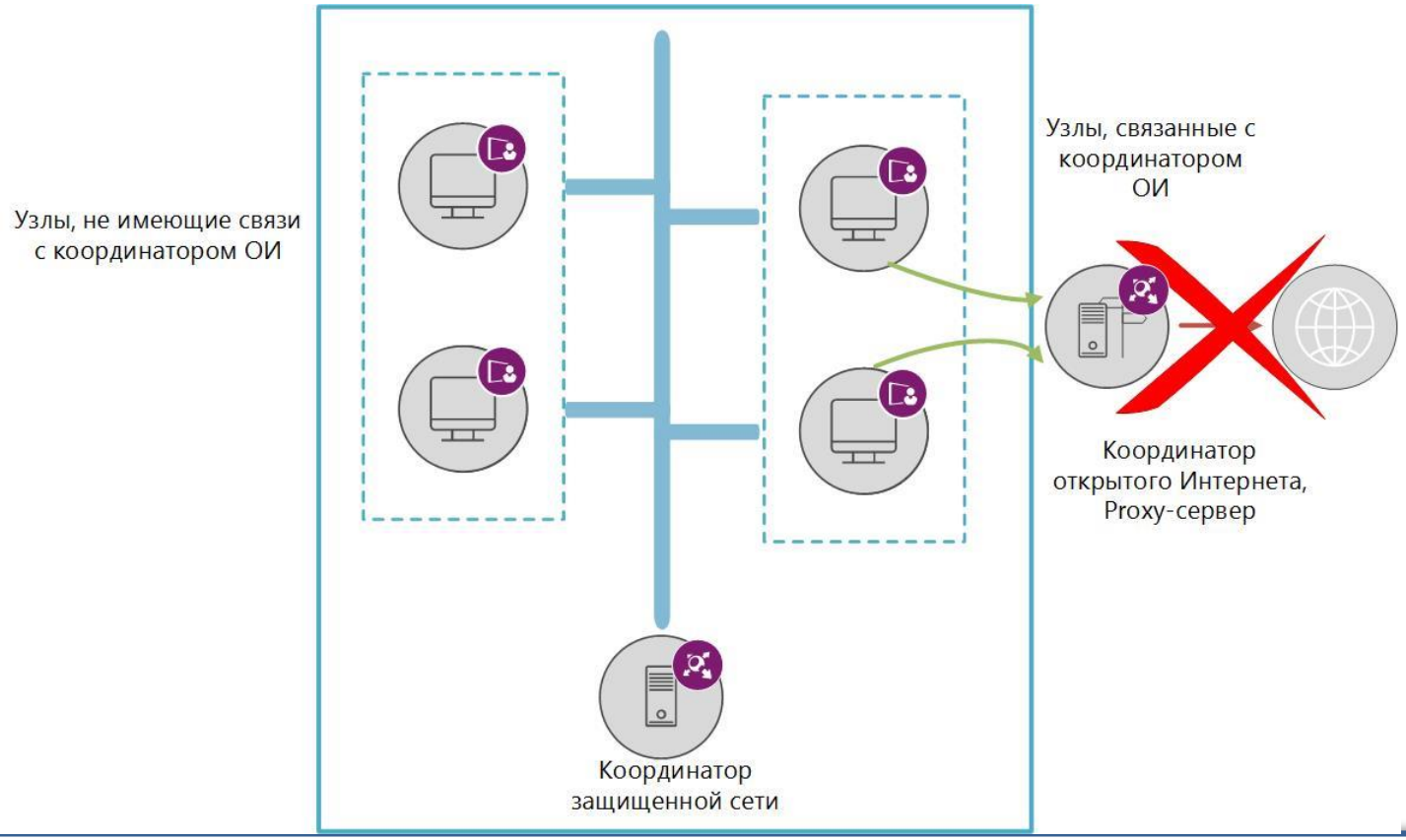
Работа в конфигурации «Открытый Интернет»



В конфигурации «Открытый Интернет» заблокированы соединения со всеми узлами (как защищенными так и открытыми), кроме координатора открытого Интернета.

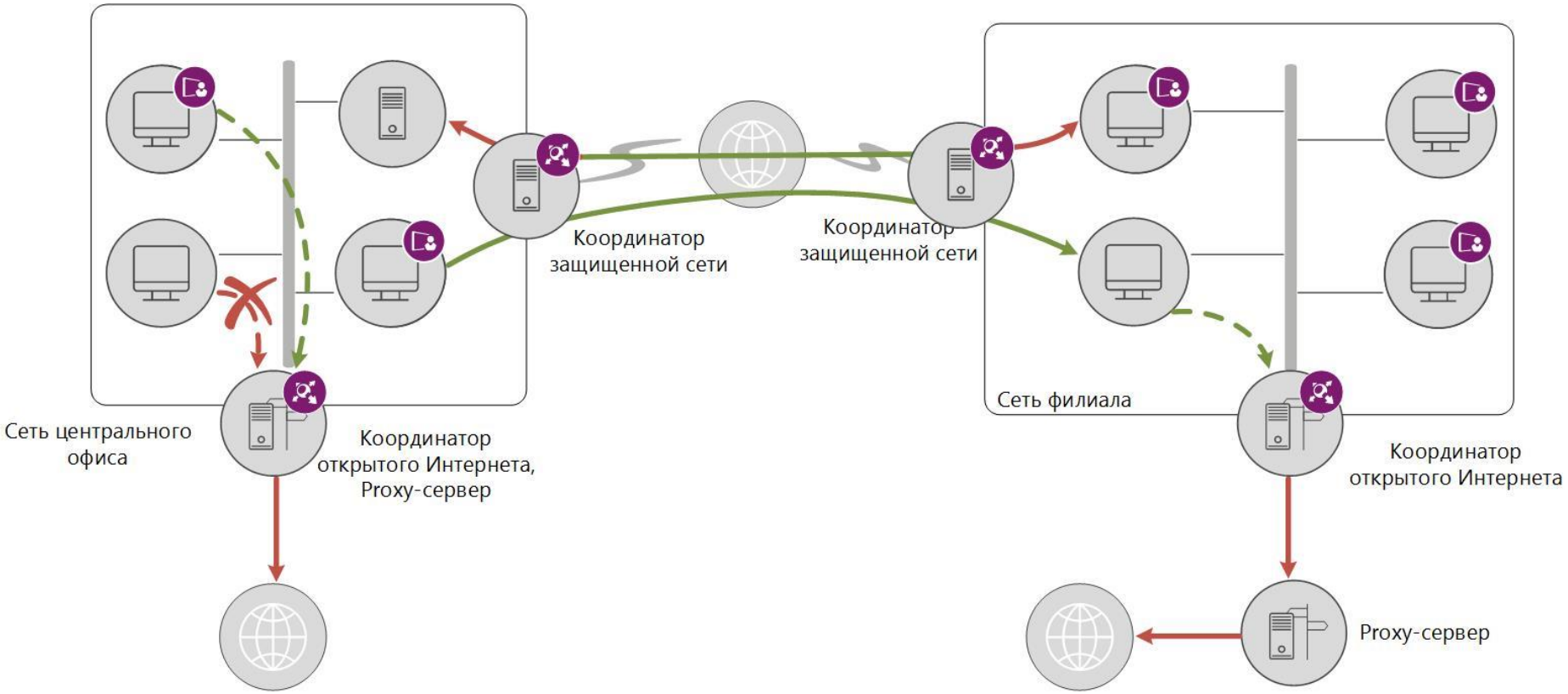
Технология «Открытый Интернет»

Работа в основной конфигурации



В любой конфигурации (кроме конфигурации «Открытый Интернет») соединения с координатором открытого Интернета заблокированы, доступ в Интернет невозможен.

Технология «Открытый Интернет»



Технология «Открытый Интернет»

Порядок настройки схемы «Открытый Интернет»

Установить на выделенный сервер ViPNet Coordinator. Установить дистрибутив ключей координатора, для которого включена функция сервера открытого Интернета.

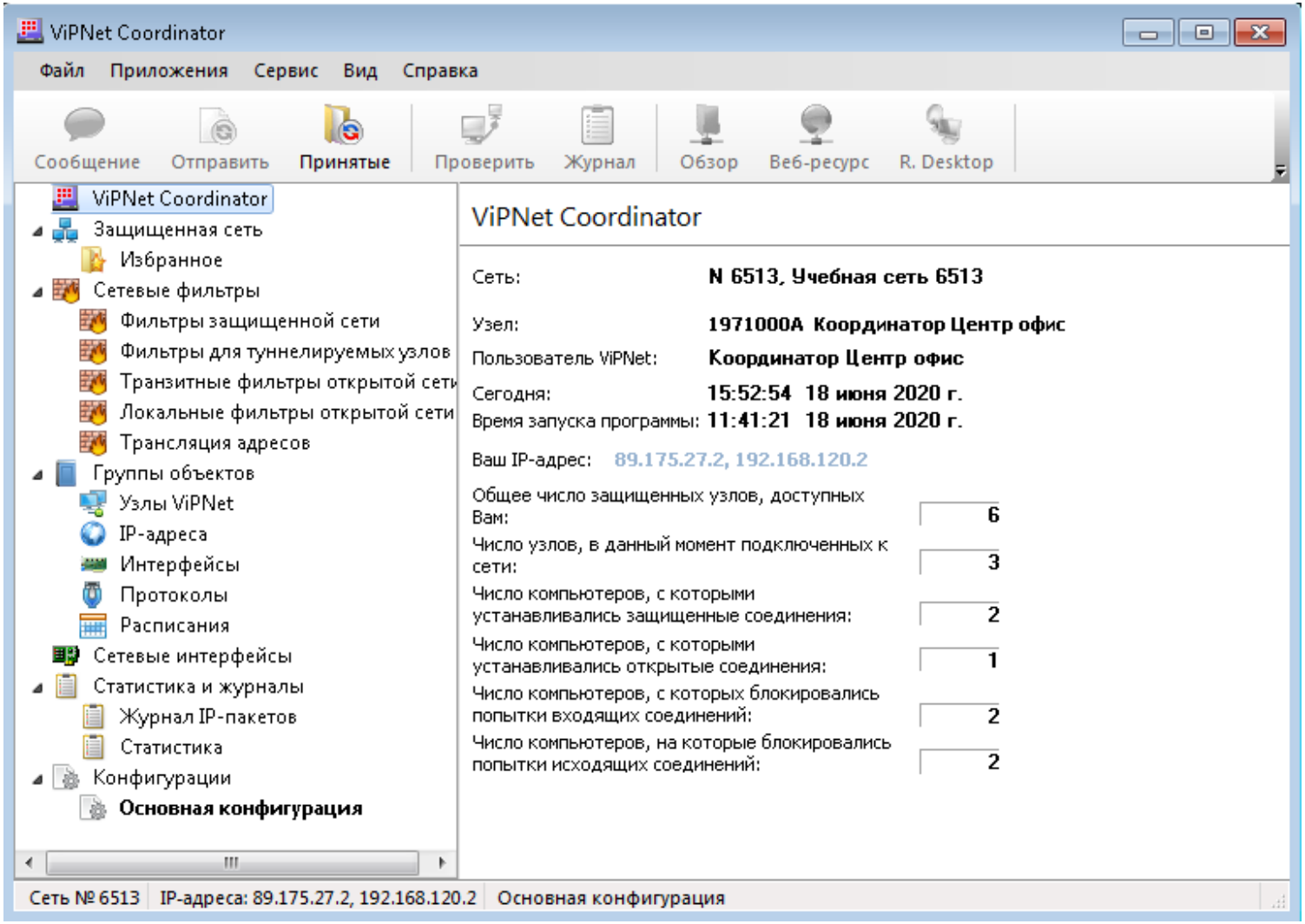
На сервере с ViPNet Coordinator, или на выделенном сервере установить ПО, выполняющее функции proxy-сервера. Выполнить на proxy-сервере необходимые настройки для доступа клиентов в Интернет.

Если proxy-сервер расположен на отдельном компьютере, добавить его в список туннелируемых узлов координатора Открытого Интернета.

Настроить на координаторе набор сетевых фильтров, обеспечивающих безопасный доступ пользователей в Интернет.

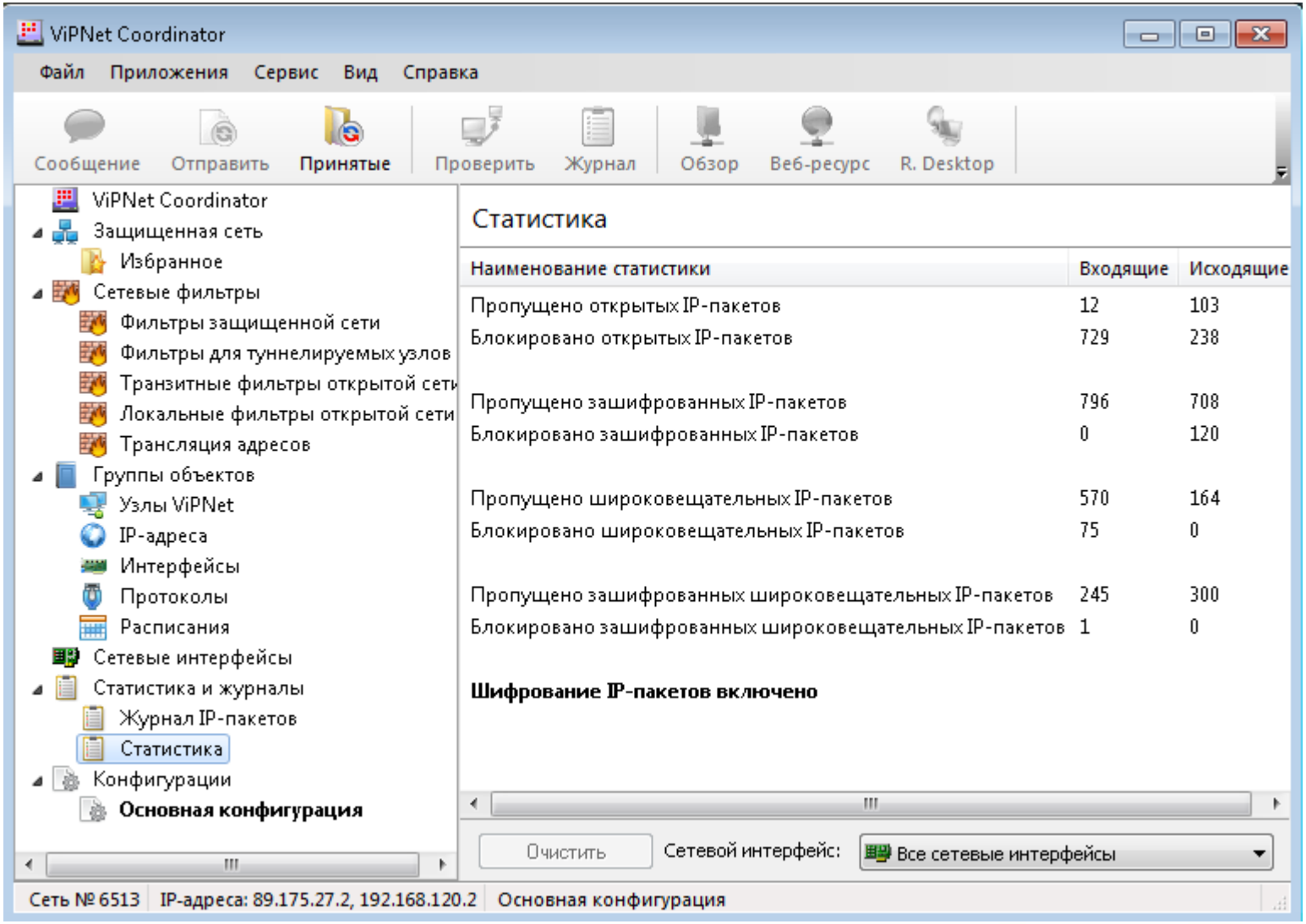
Административные функции

Просмотр информации о ViPNet Coordinator



Работа с журналами

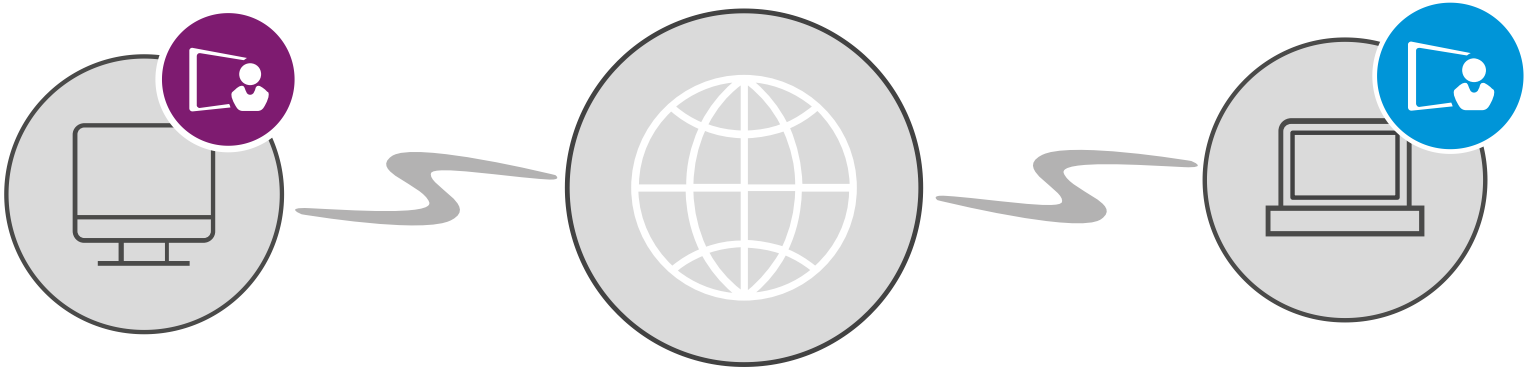
Просмотр статистики IP-пакетов



Работа с журналами

Журнал IP-пакетов

- **В журнале IP-пакетов регистрируется информация о всех пакетах, проходящих через сетевые интерфейсы:**
  - направление пакета;
  - время прохождения пакета;
  - IP-адрес источника;
  - IP-адрес назначения;
  - протокол;
  - порт источники и порт назначения;
  - **код события;**
  - …



Работа с журналами

События, отслеживаемые ViPNet

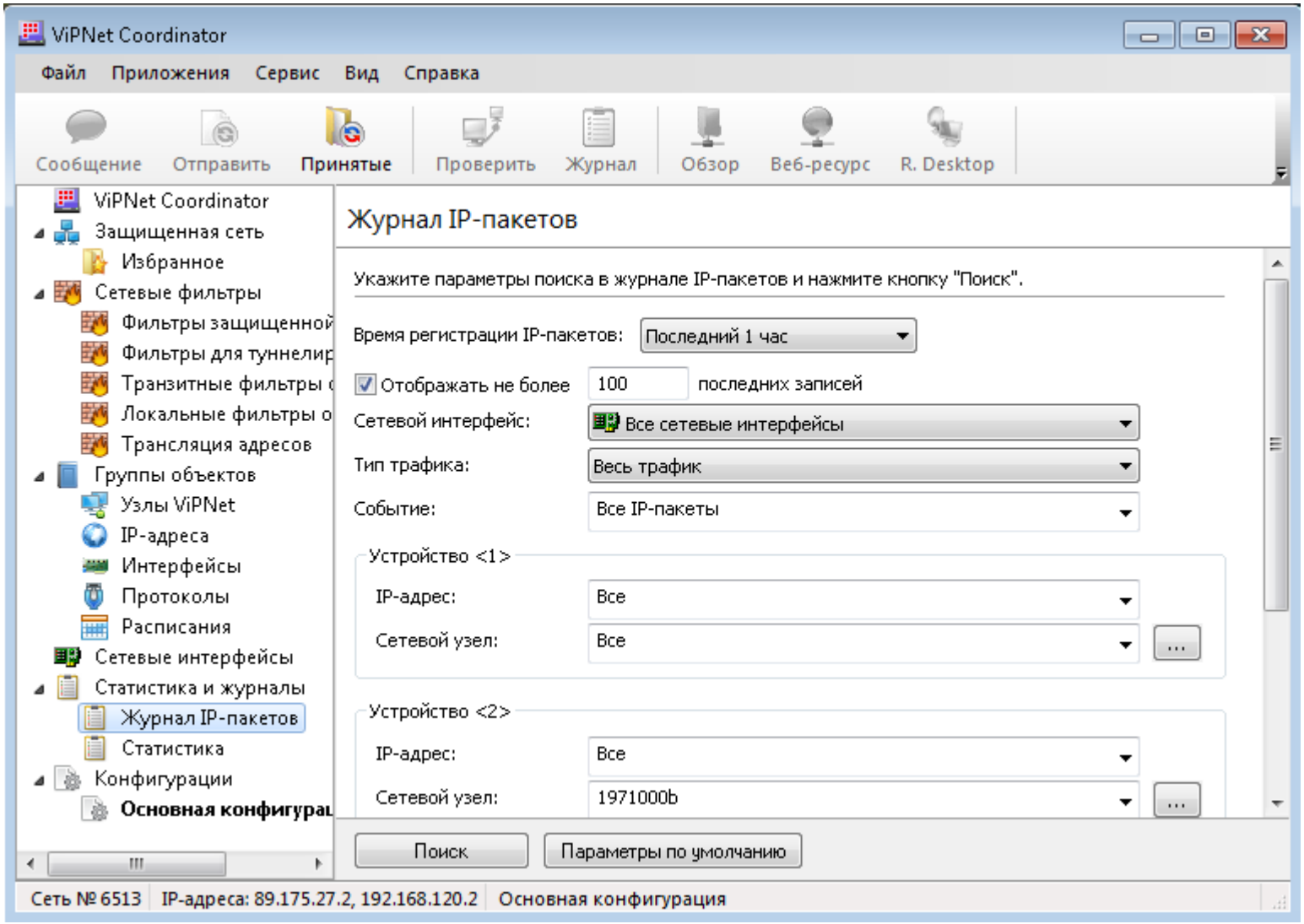
события, связанные с фильтрацией трафика

- **Блокированные IP-пакеты:**
  - фильтрами защищенной сети;
  - фильтрами открытой сети;
  - по другим причинам.
- **Все пропущенные IP-пакеты:**
  - зашифрованные;
  - незашифрованные.
- **События системы обнаружения атак:**
  - атаки протокола IP, атаки протокола ICMP, атаки протокола TCP, атаки протокола UDP

служебные события

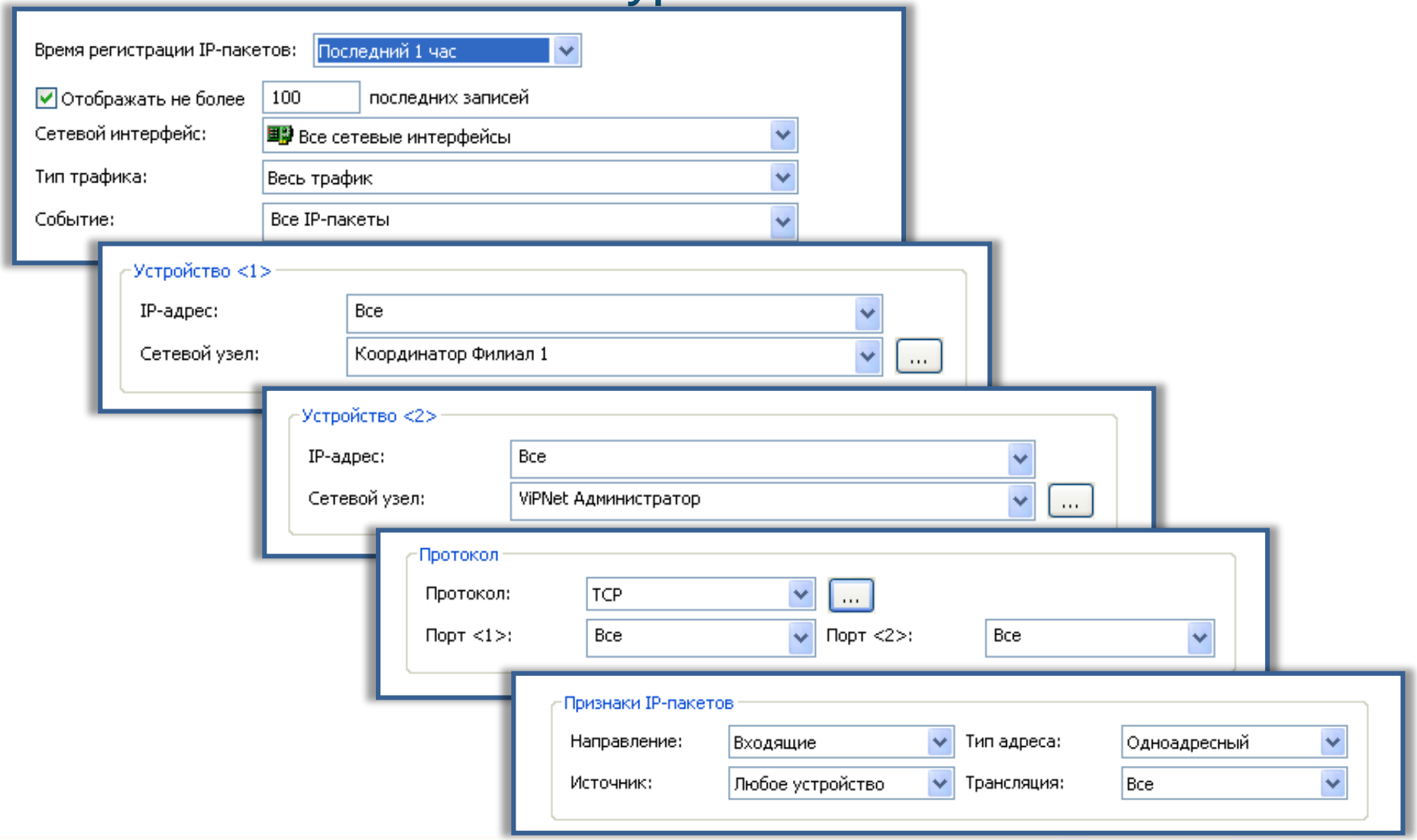
Работа с журналами

Поиск в журнале IP-пакетов



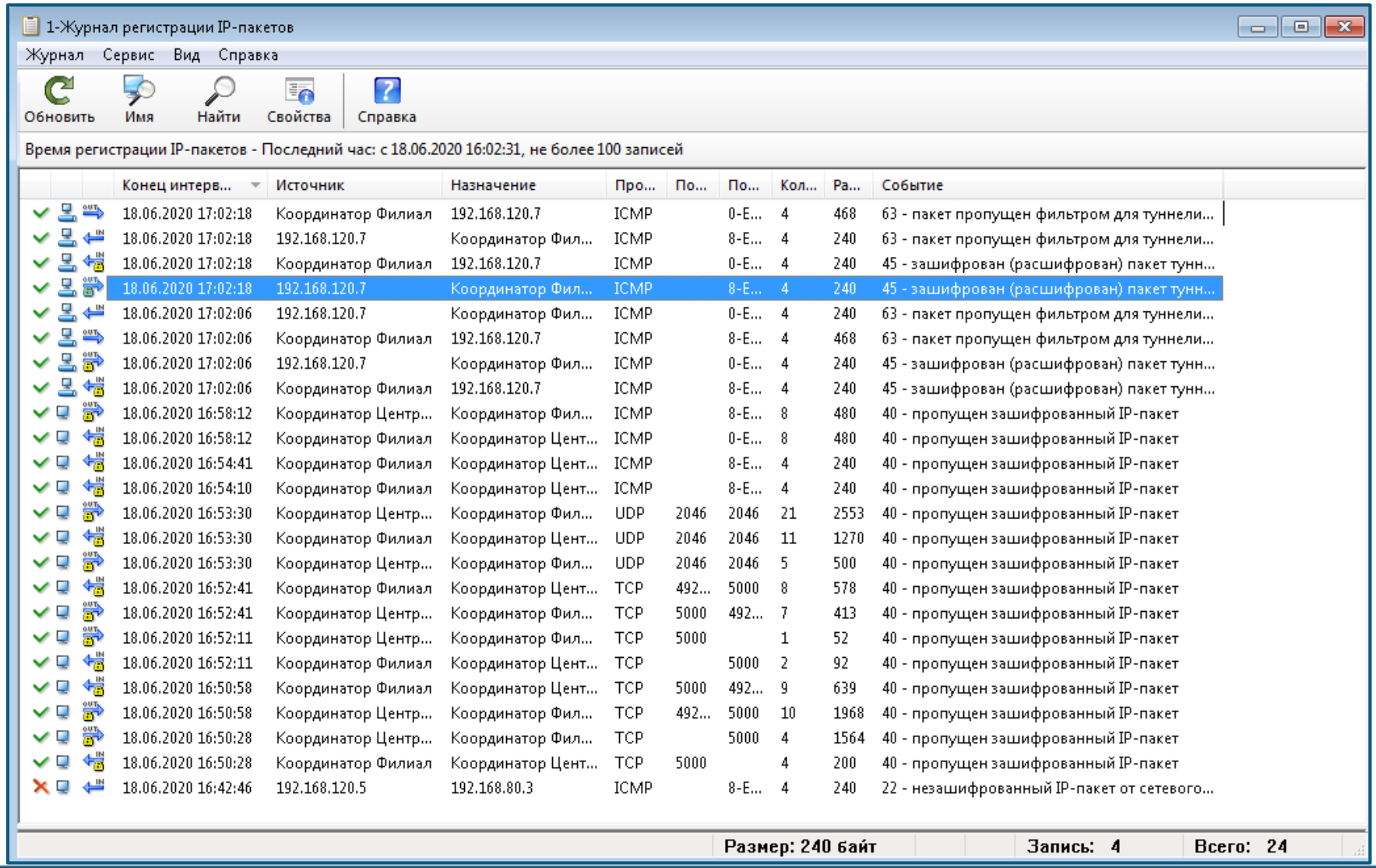
Работа с журналами

Поиск в журнале IP-пакетов



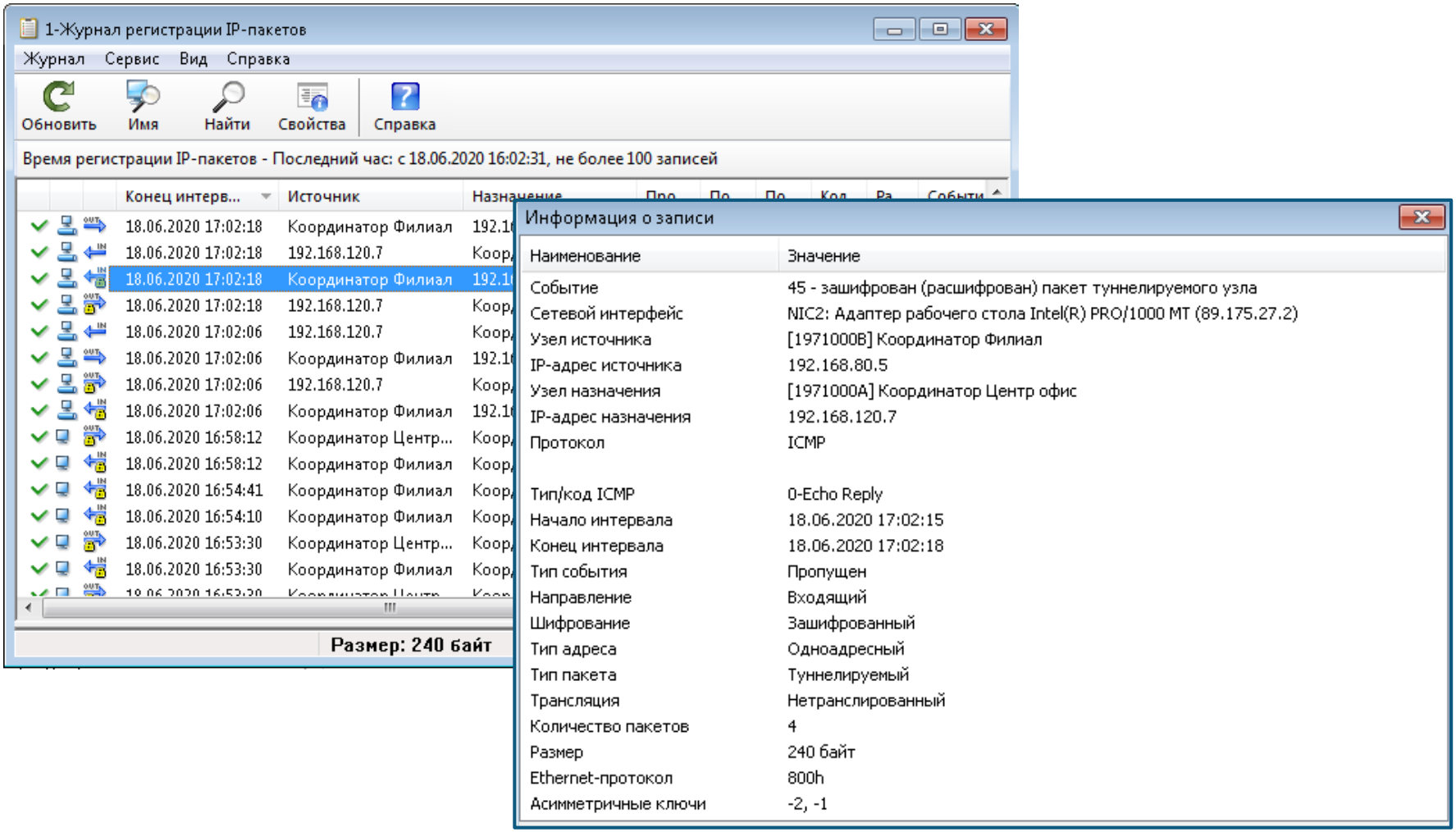
Работа с журналами

Просмотр информации об IP-пакетах



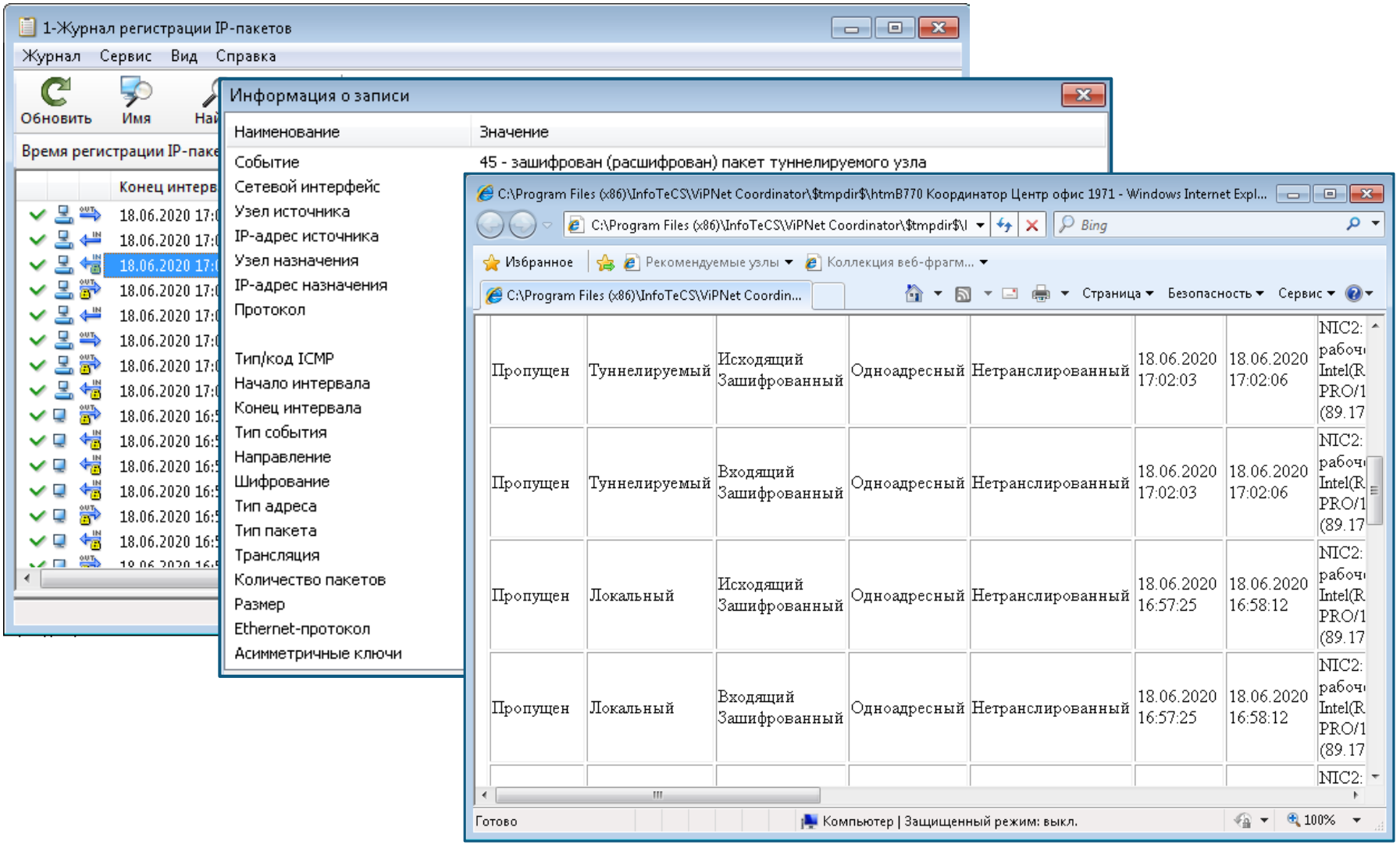
Работа с журналами

Просмотр информации об IP-пакетах



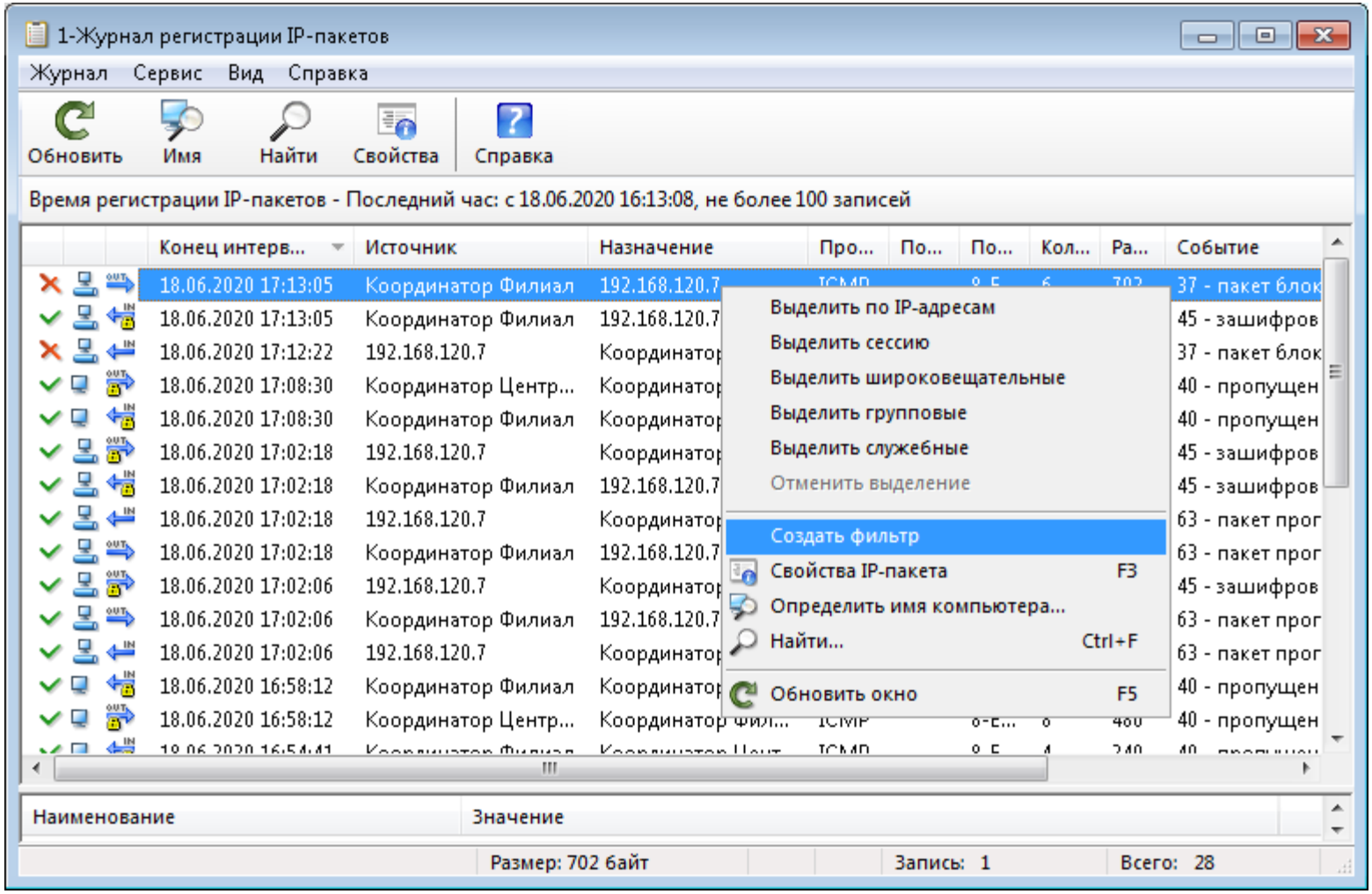
Работа с журналами

Просмотр информации об IP-пакетах в веб-браузере



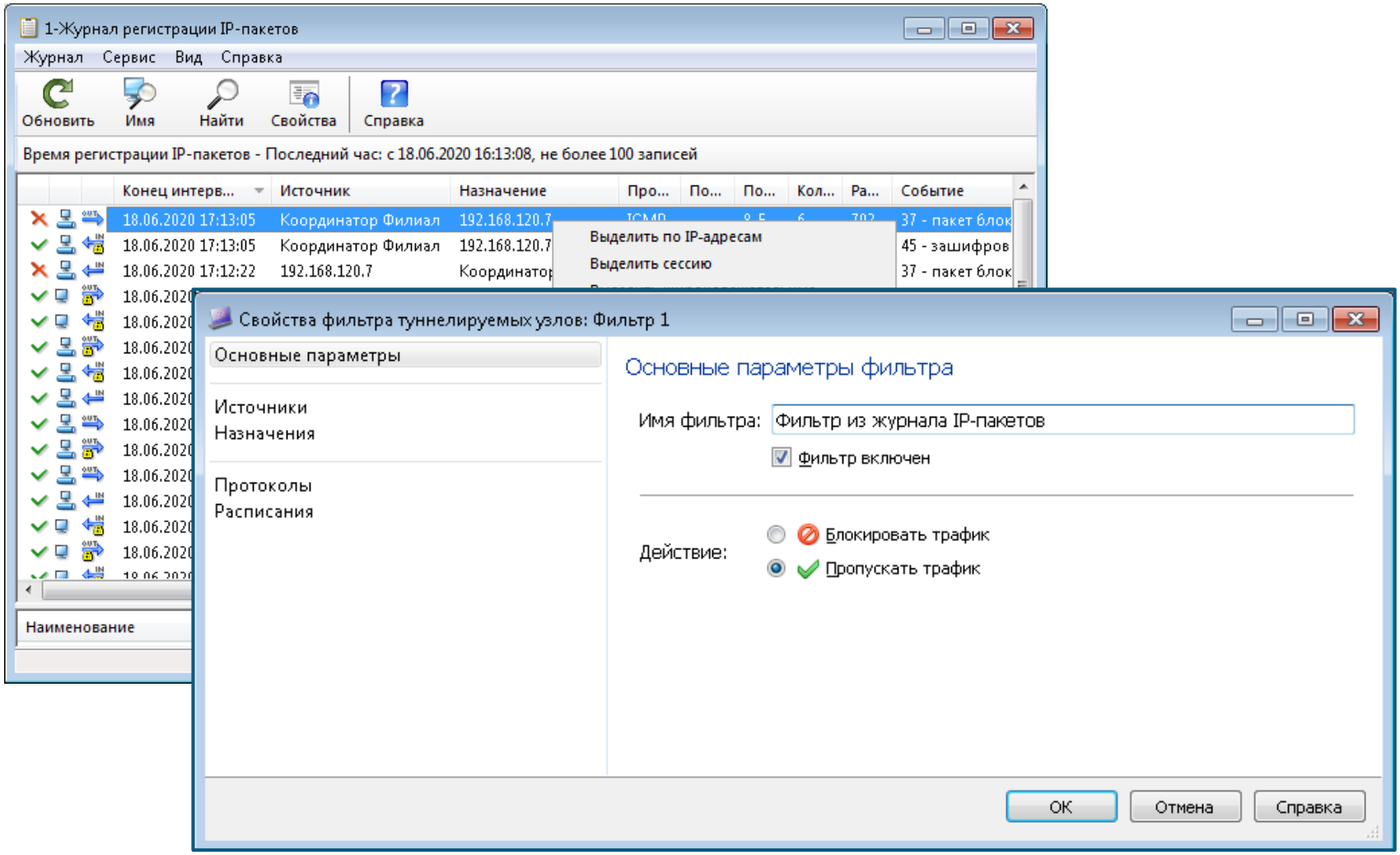
Работа с журналами

Создание сетевого фильтра из журнала IP-пакетов



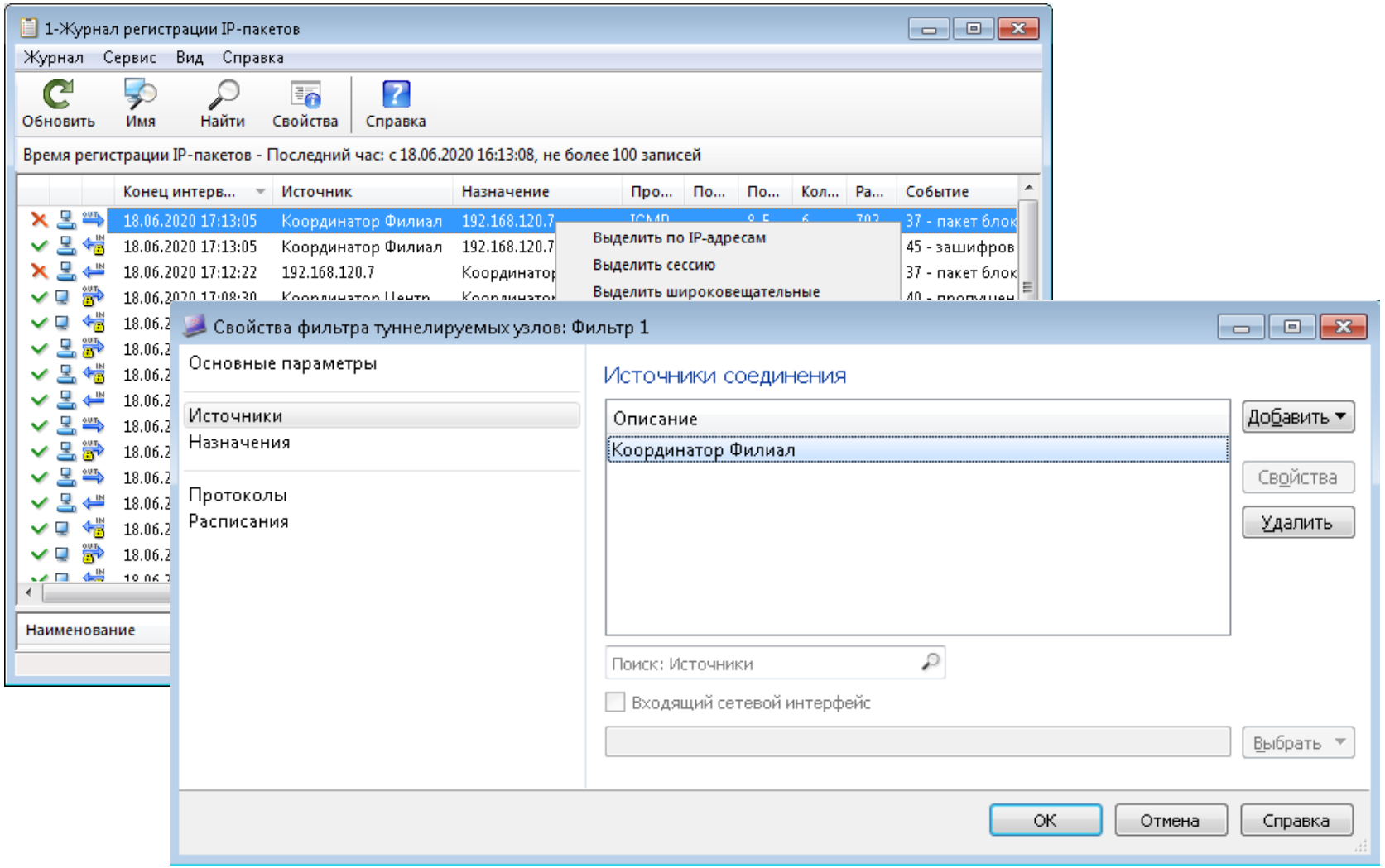
Работа с журналами

Создание сетевого фильтра из журнала IP-пакетов



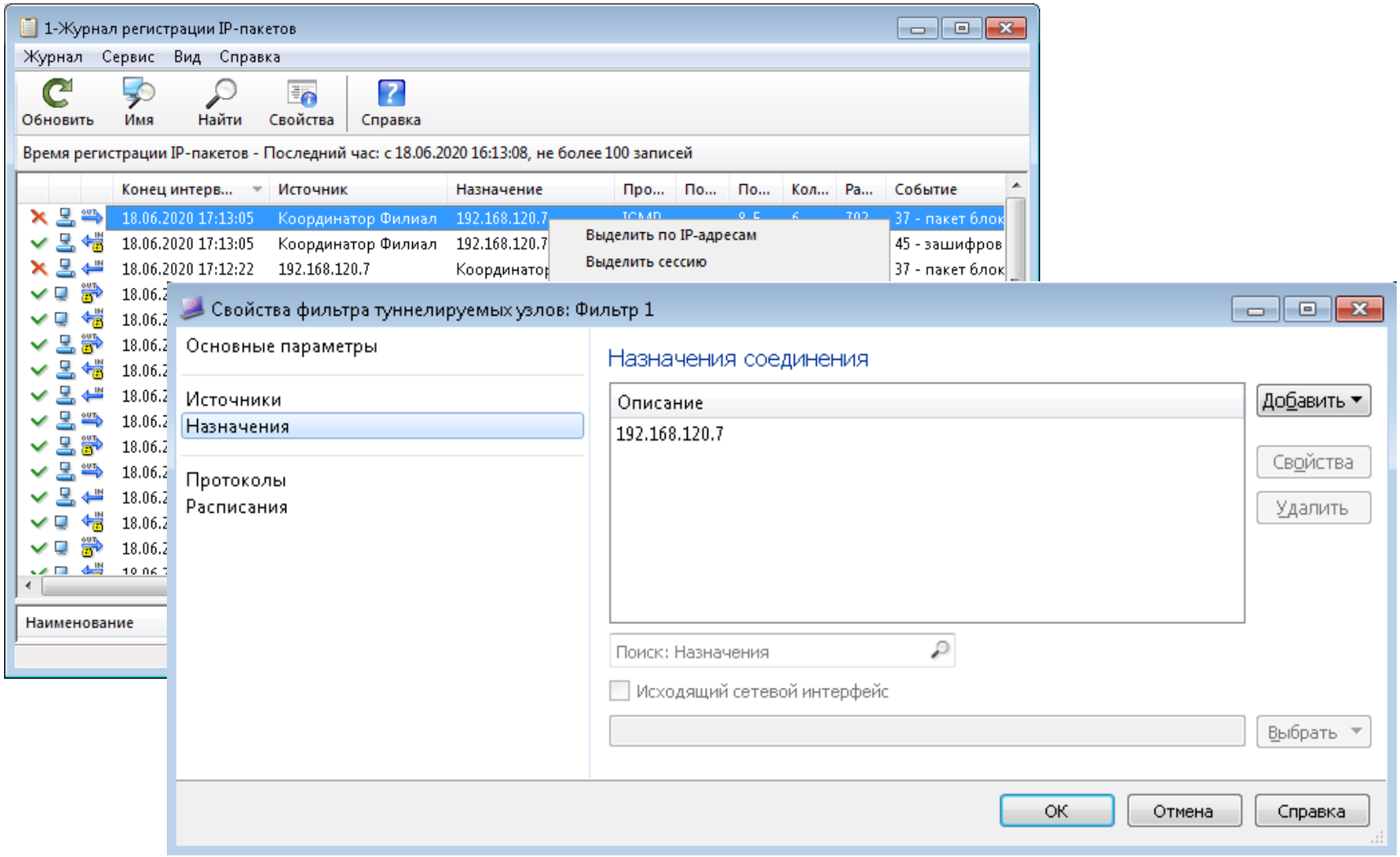
Работа с журналами

Создание сетевого фильтра из журнала IP-пакетов



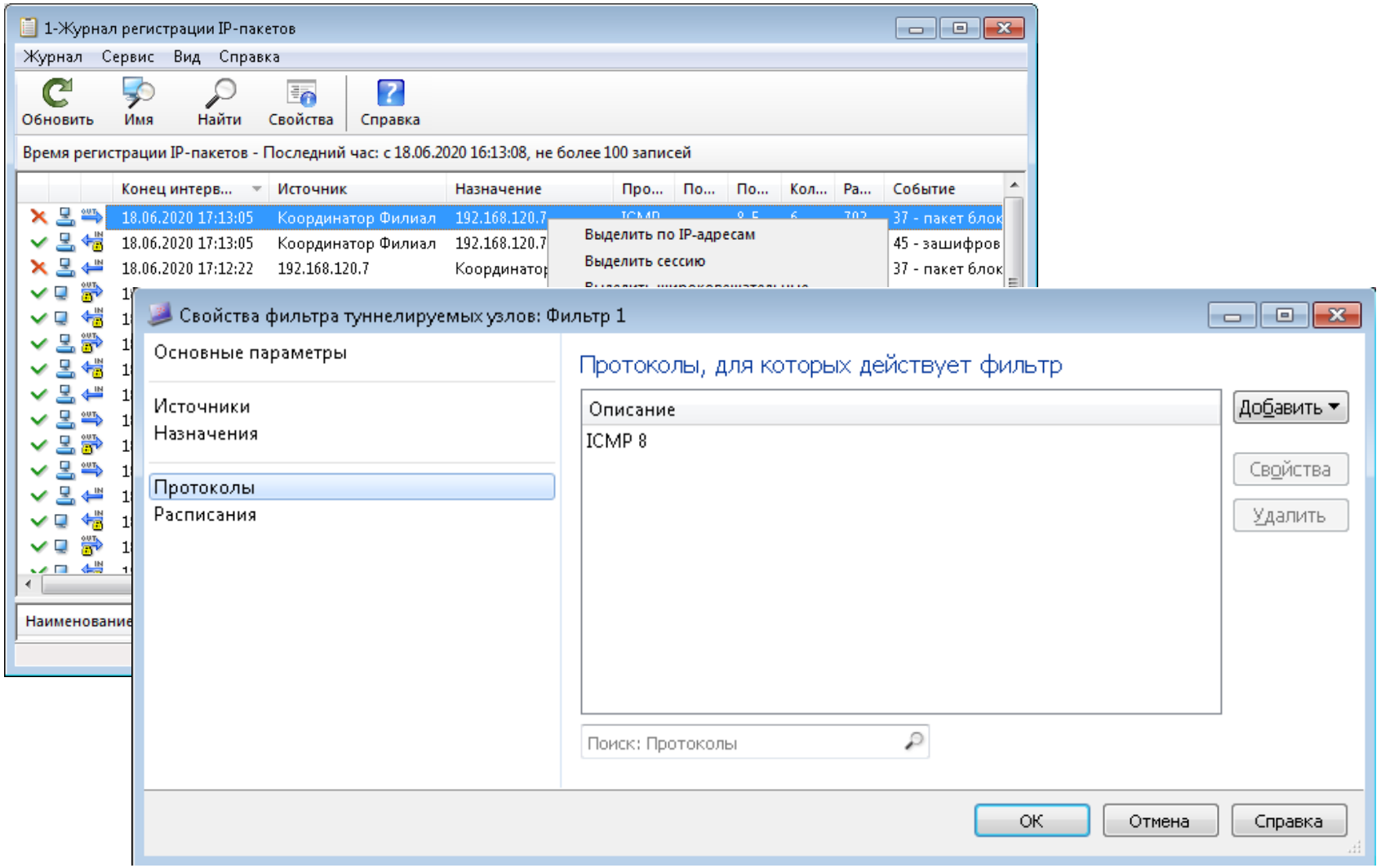
Работа с журналами

Создание сетевого фильтра из журнала IP-пакетов



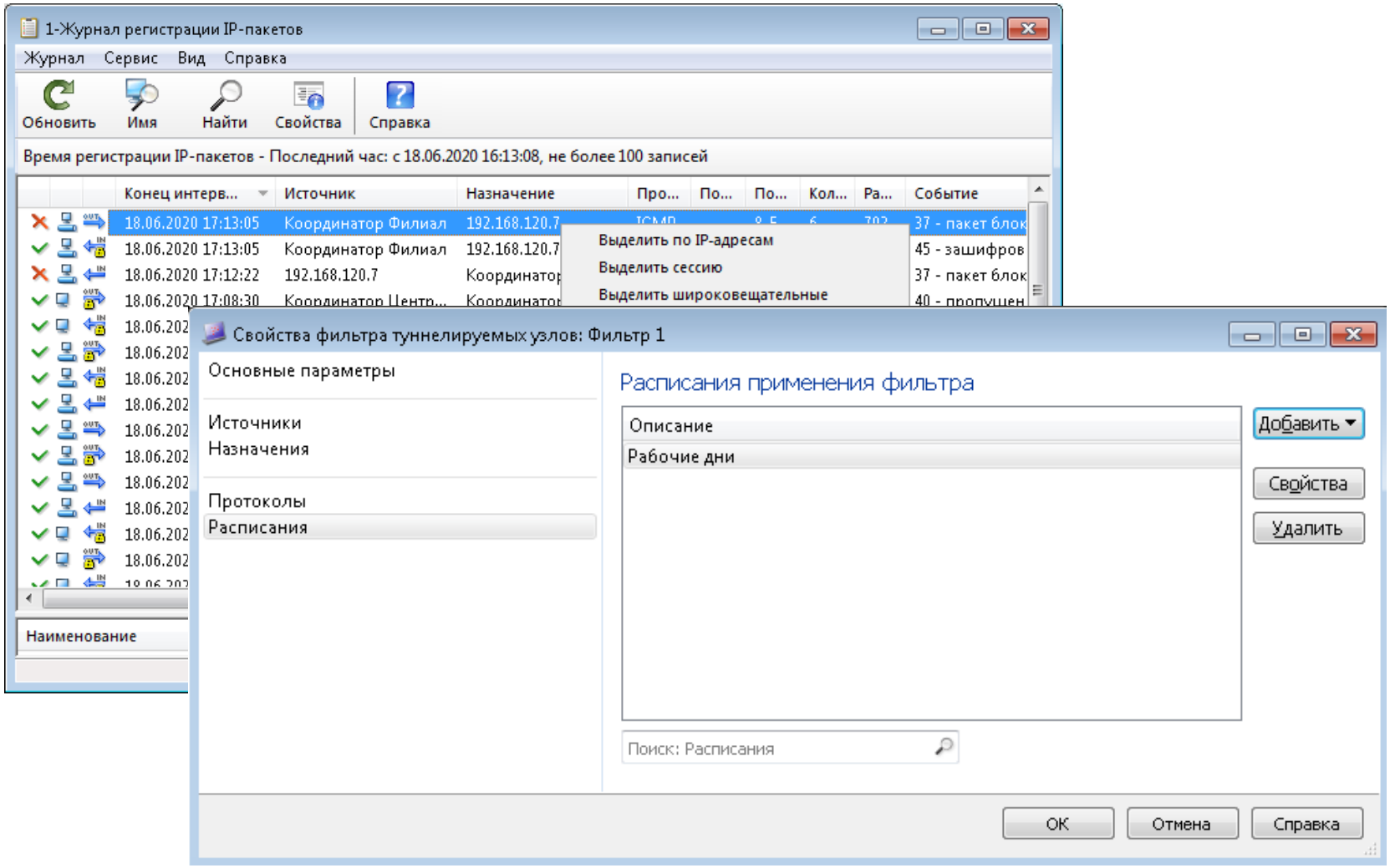
Работа с журналами

Создание сетевого фильтра из журнала IP-пакетов



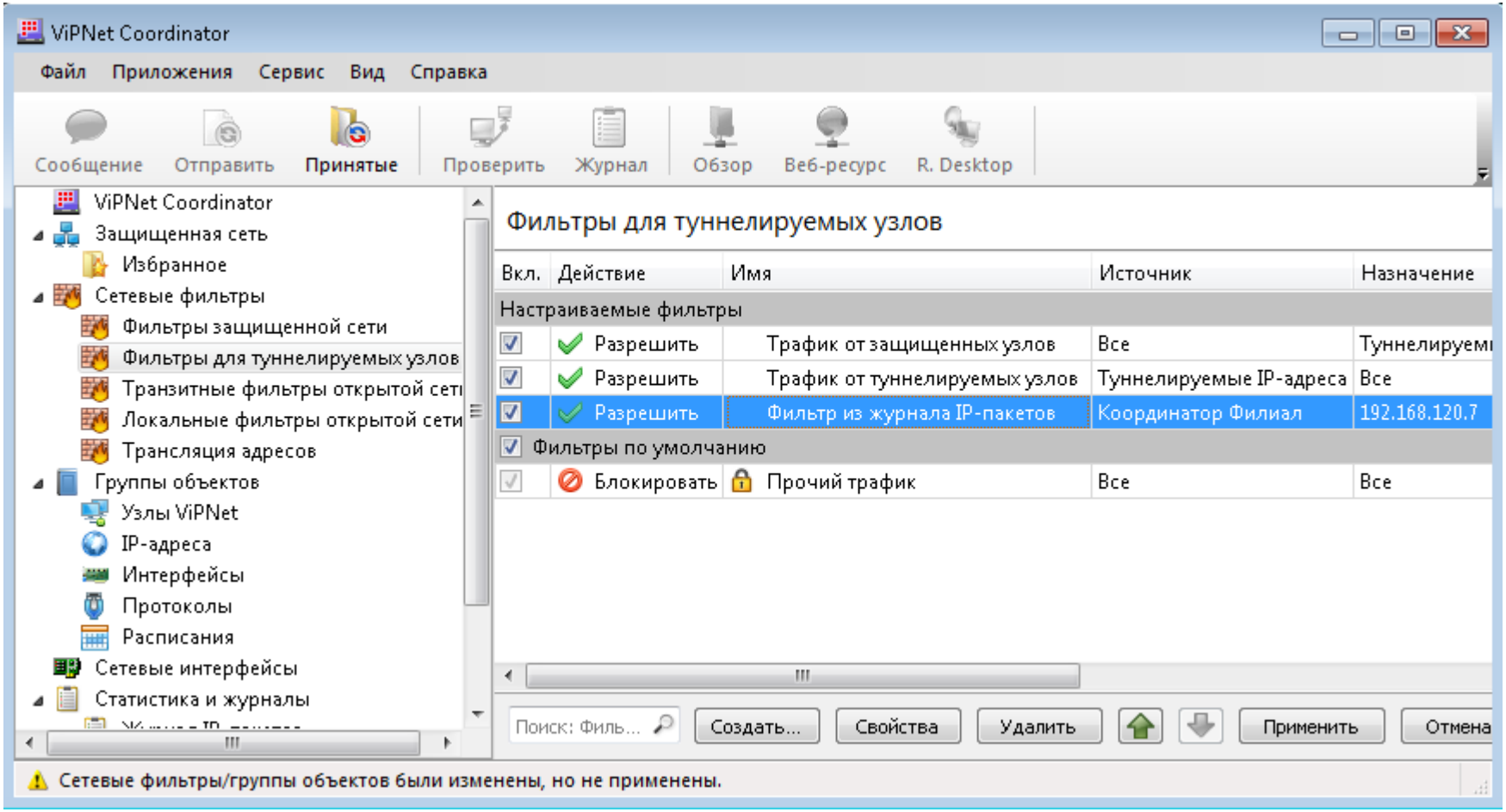
Работа с журналами

Создание сетевого фильтра из журнала IP-пакетов



Работа с журналами

Создание сетевого фильтра из журнала IP-пакетов



Работа с правами администратора

Администратор сетевого узла

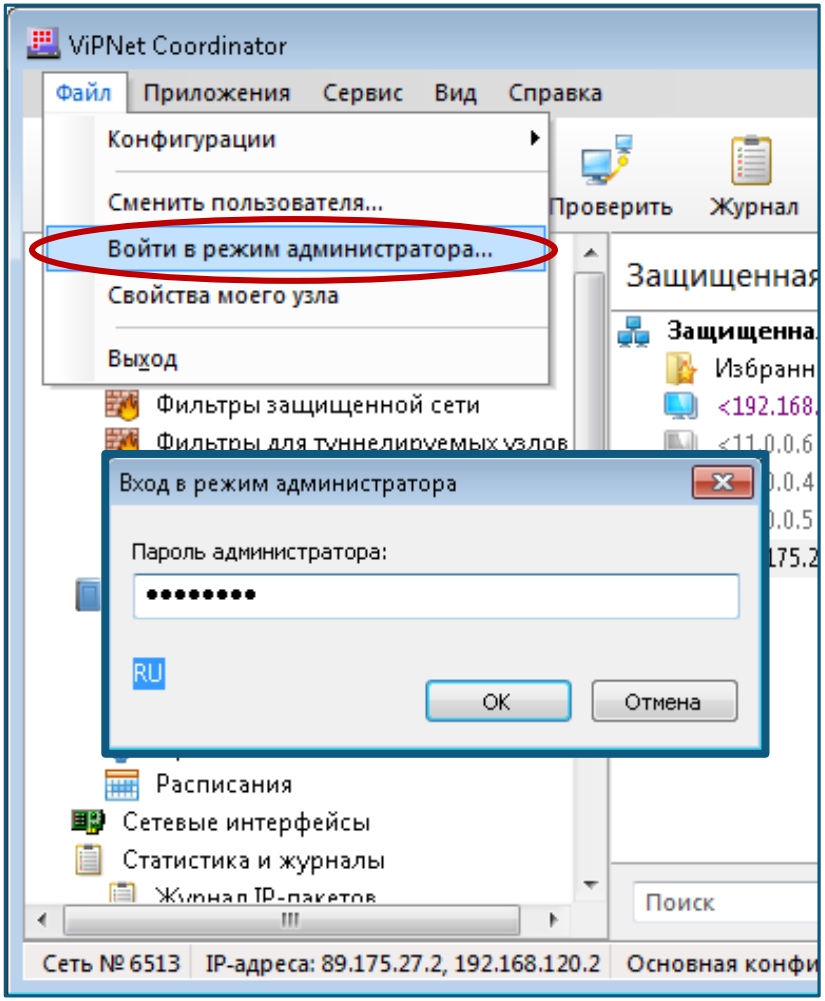
- режим администратора - режим, в котором пользователь получает полный доступ к настройкам системы защиты ViPNet и специальные полномочия, которые дают дополнительные возможности настройки приложений ViPNet

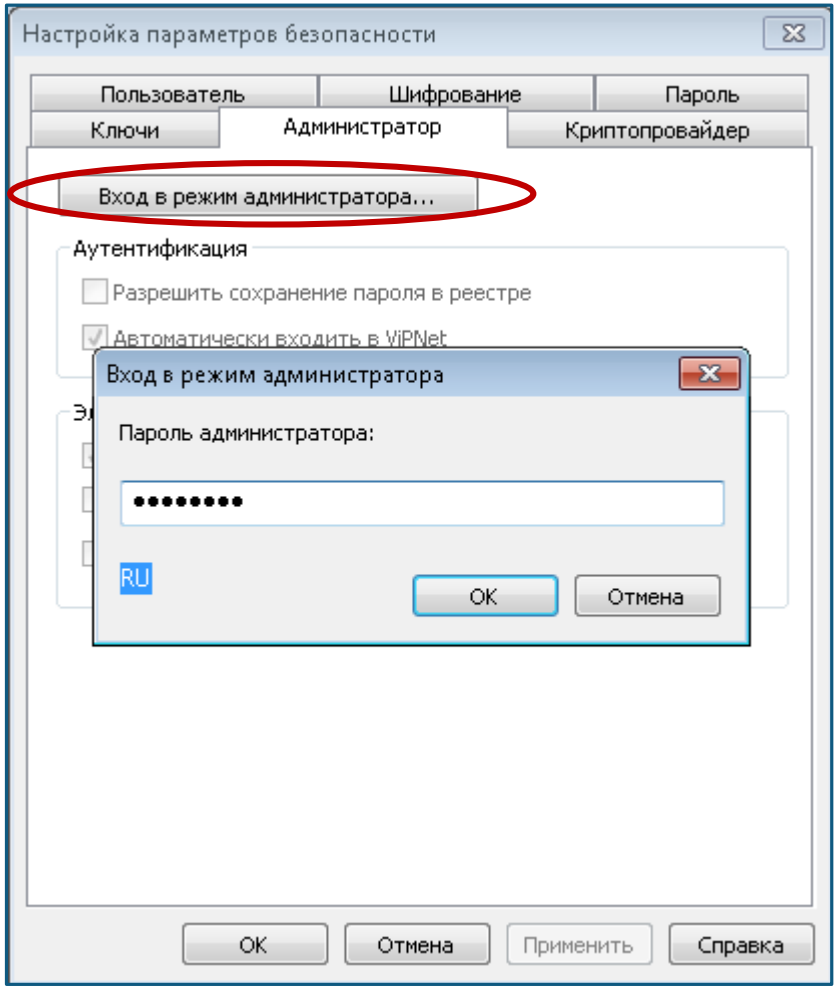
- пароль администратора - пароль, с помощью которого пользователь получает возможность работать в режиме администратора

- пароль администратора сетевого узла ViPNet создается в УКЦ администратором сети ViPNet

Работа с правами администратора

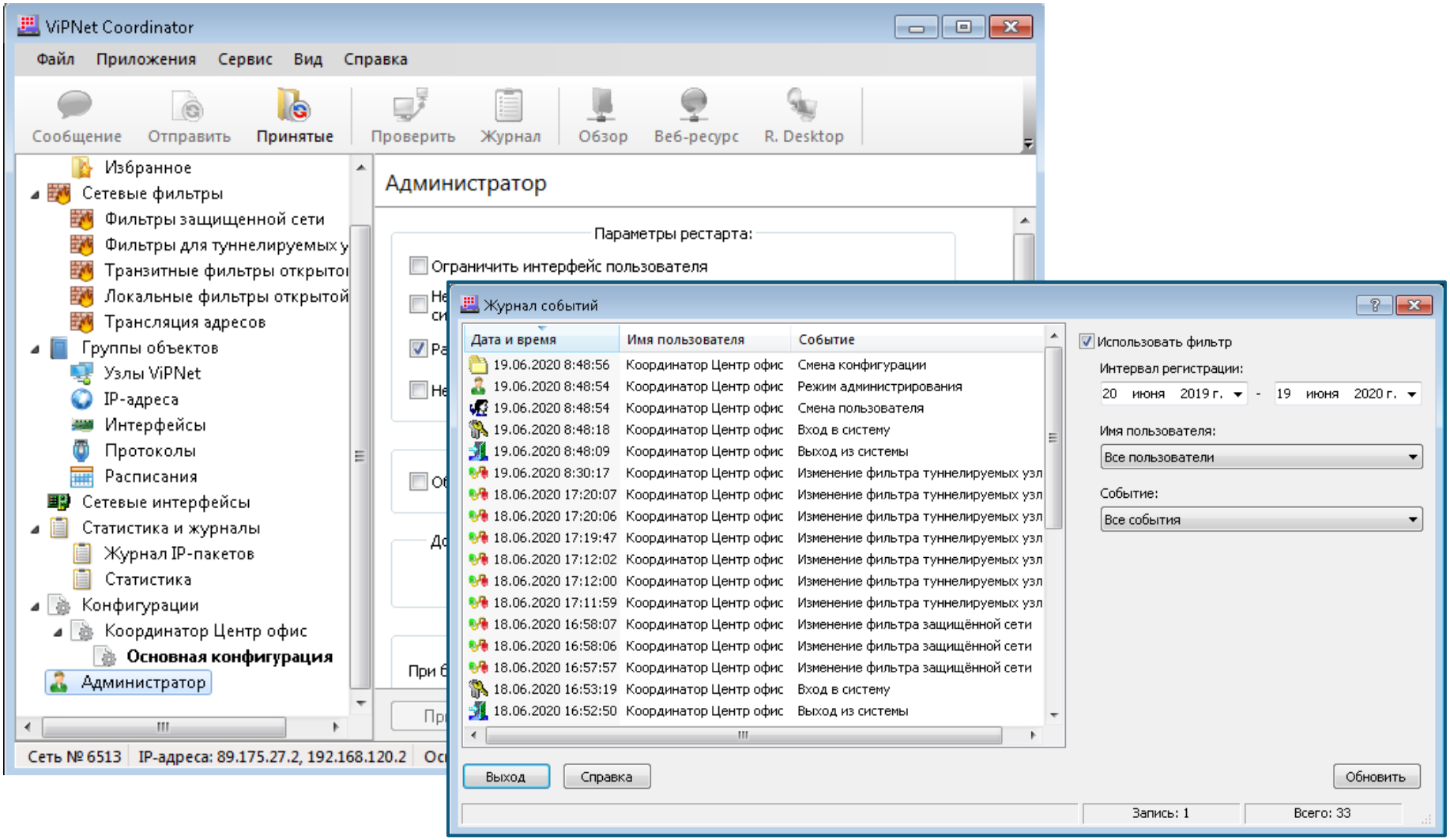
Вход в режим администратор сетевого узла





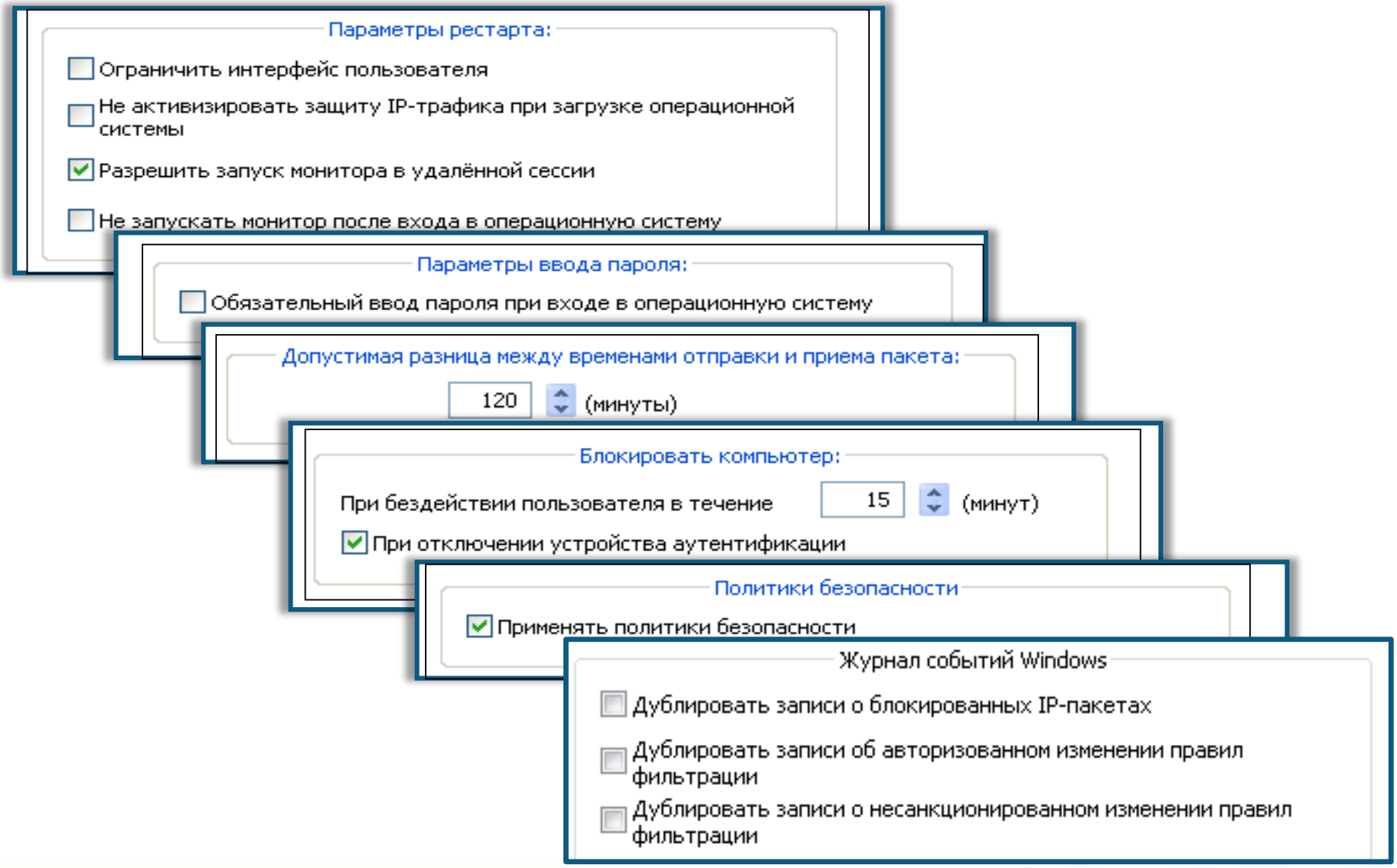
Работа с правами администратора

Просмотр журнала событий



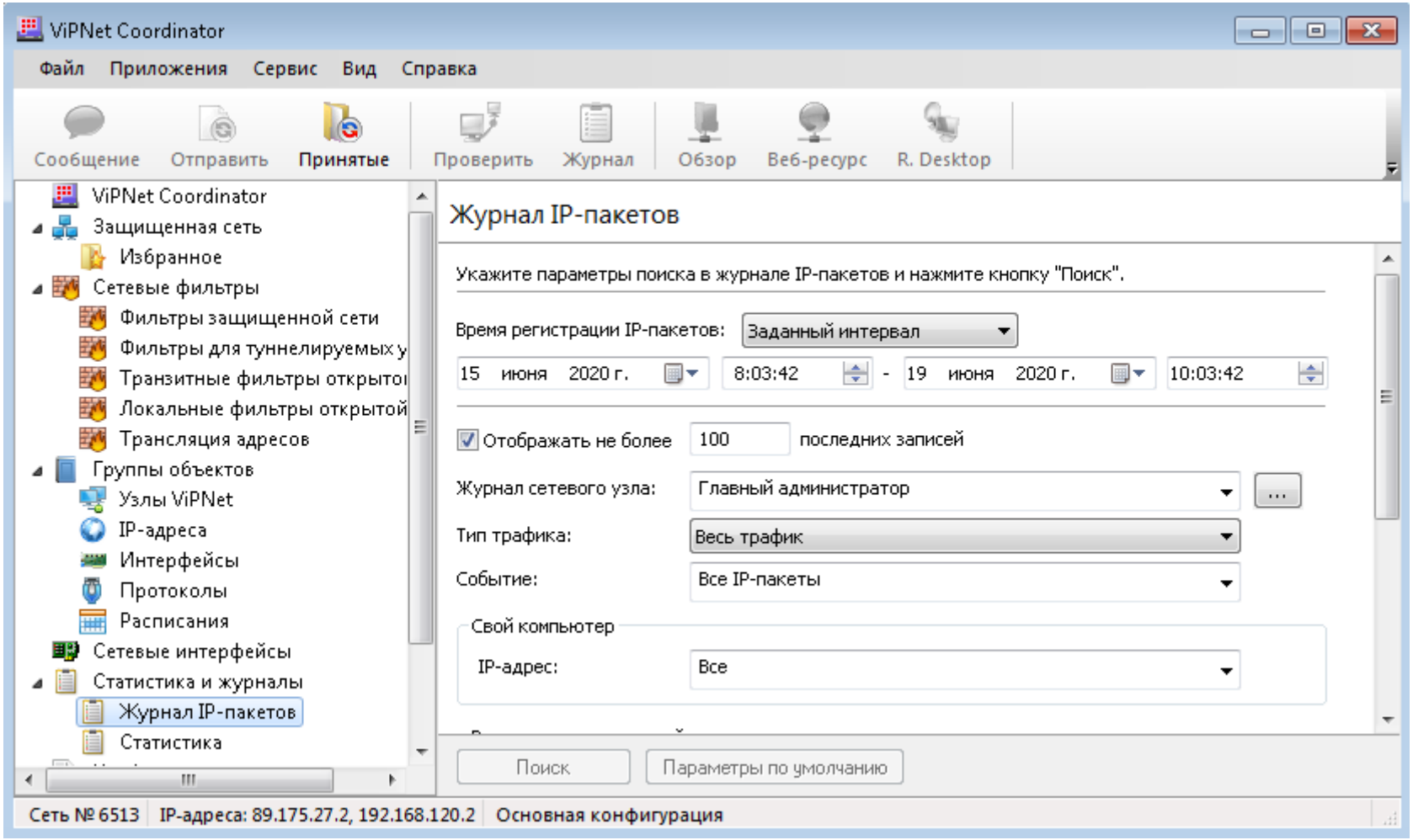
Работа с правами администратора

Дополнительные настройки программы ViPNet Монитор



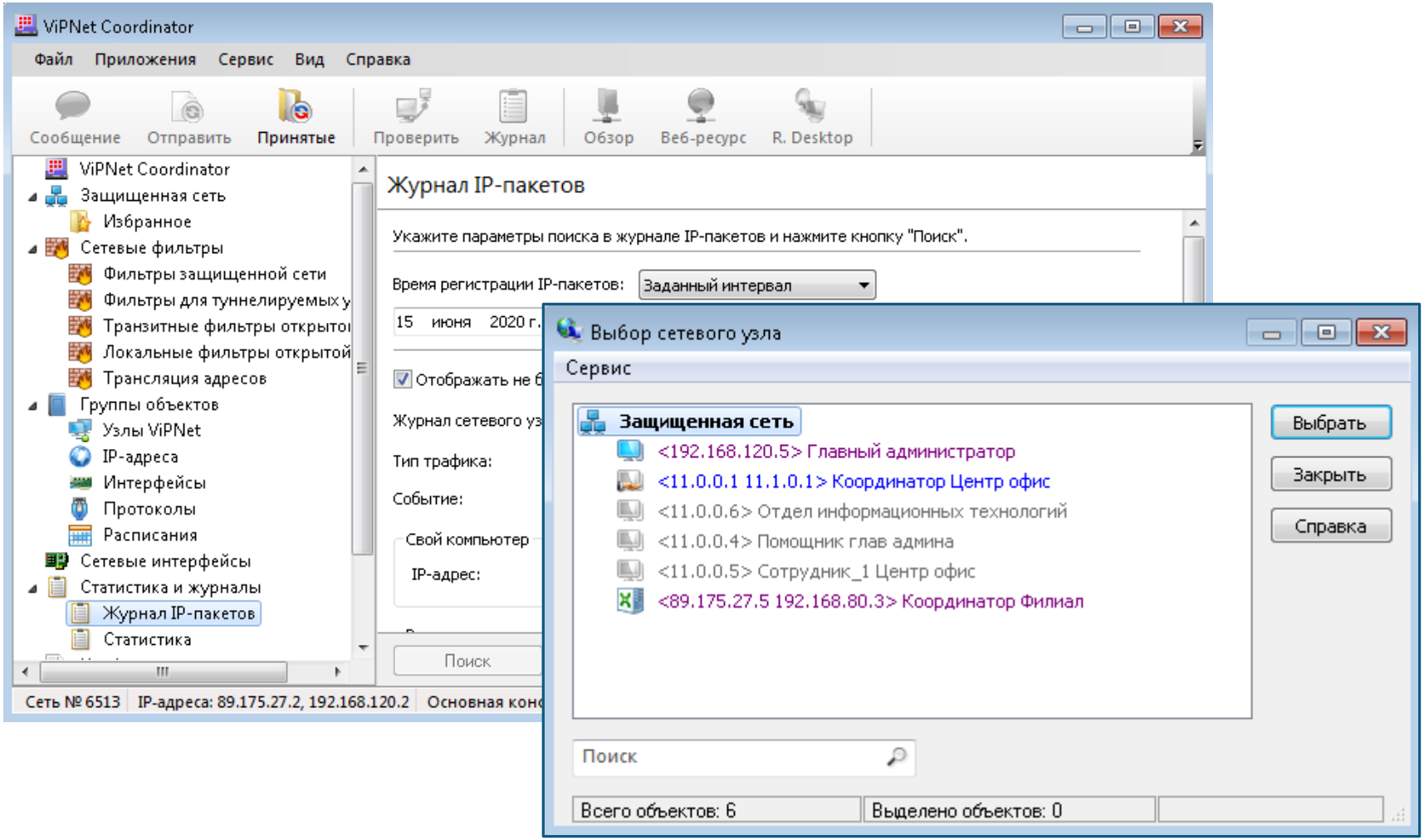
Работа с правами администратора

Просмотр журнала IP-пакетов другого сетевого узла



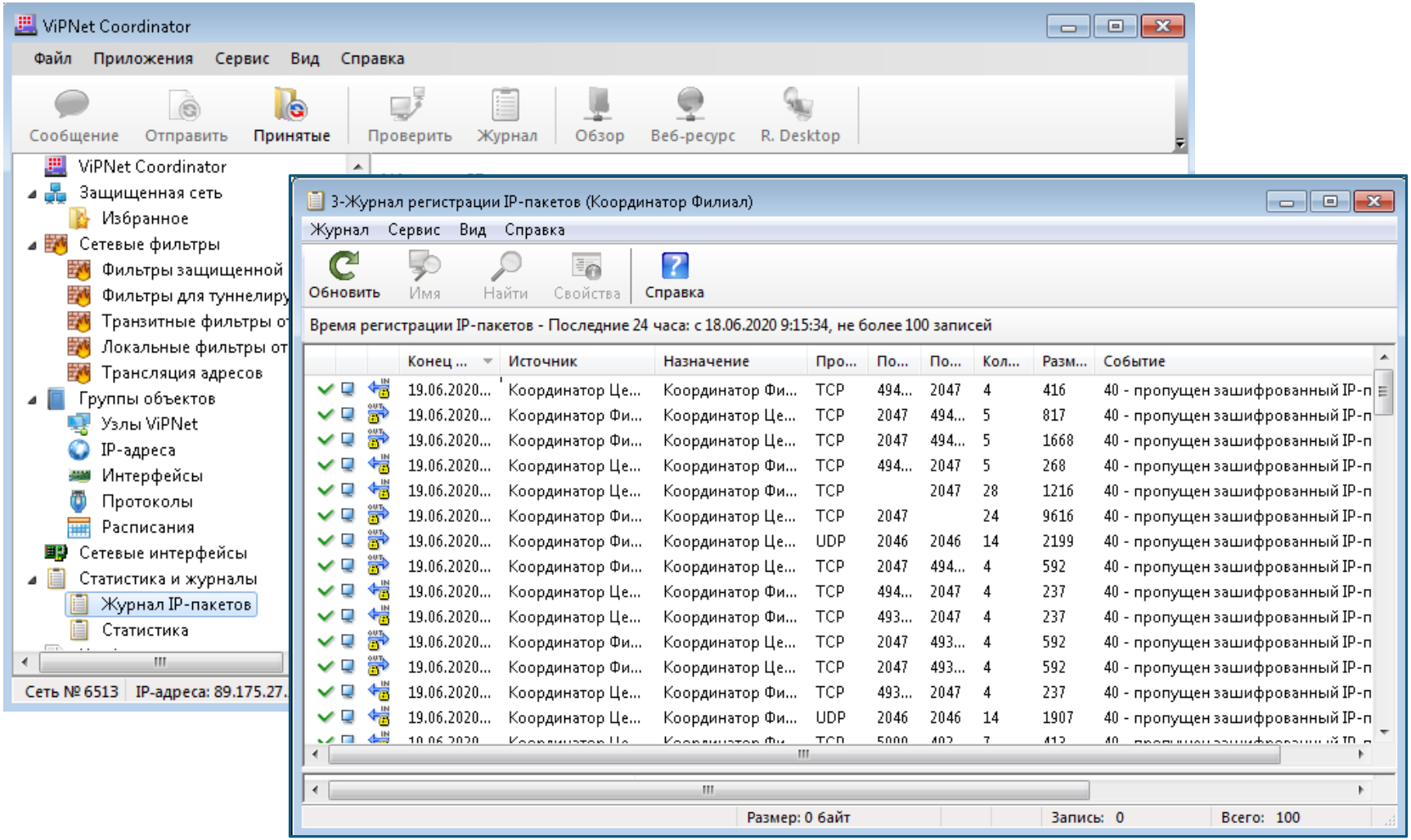
Работа с правами администратора

Просмотр журнала IP-пакетов другого сетевого узла



Работа с правами администратора

Просмотр журнала IP-пакетов другого сетевого узла



Транспортный модуль ViPNet MFTP

Транспортный модуль ViPNet MFTP

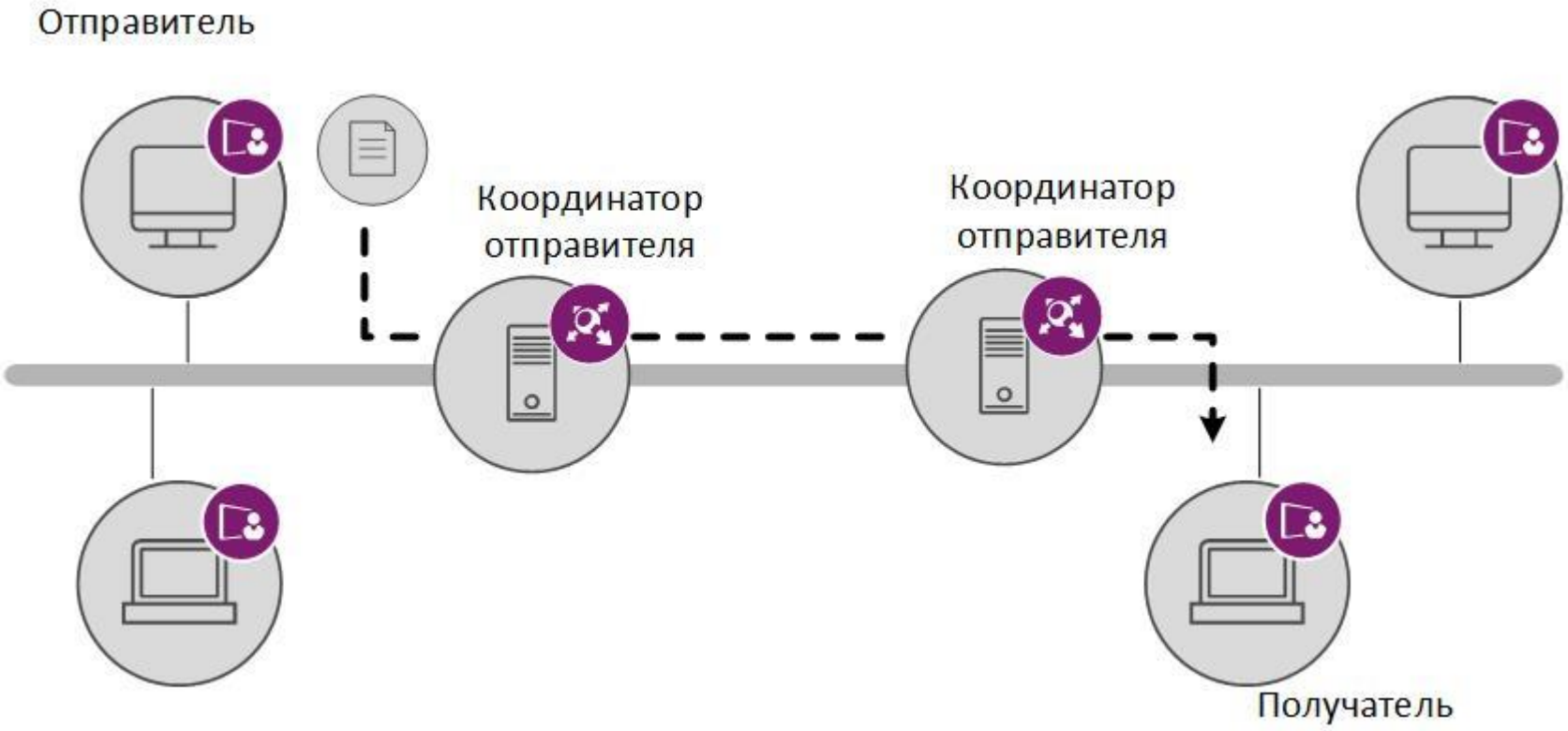
Транспортный модуль ViPNet MFTP :

- **Обеспечивает надежную и безопасную передачу транспортных конвертов между узлами сети ViPNet.**
- Запускается вместе с ПО ViPNet, в состав которого входит.
- Устанавливается только в комплекте с другим ПО ViPNet.

Расширенная настройка параметров работы транспортного модуля ViPNet MFTP производится в файле **mftp.ini**

Транспортный модуль ViPNet MFTP

Принцип работы транспортного модуля



Режимы работы транспортного модуля

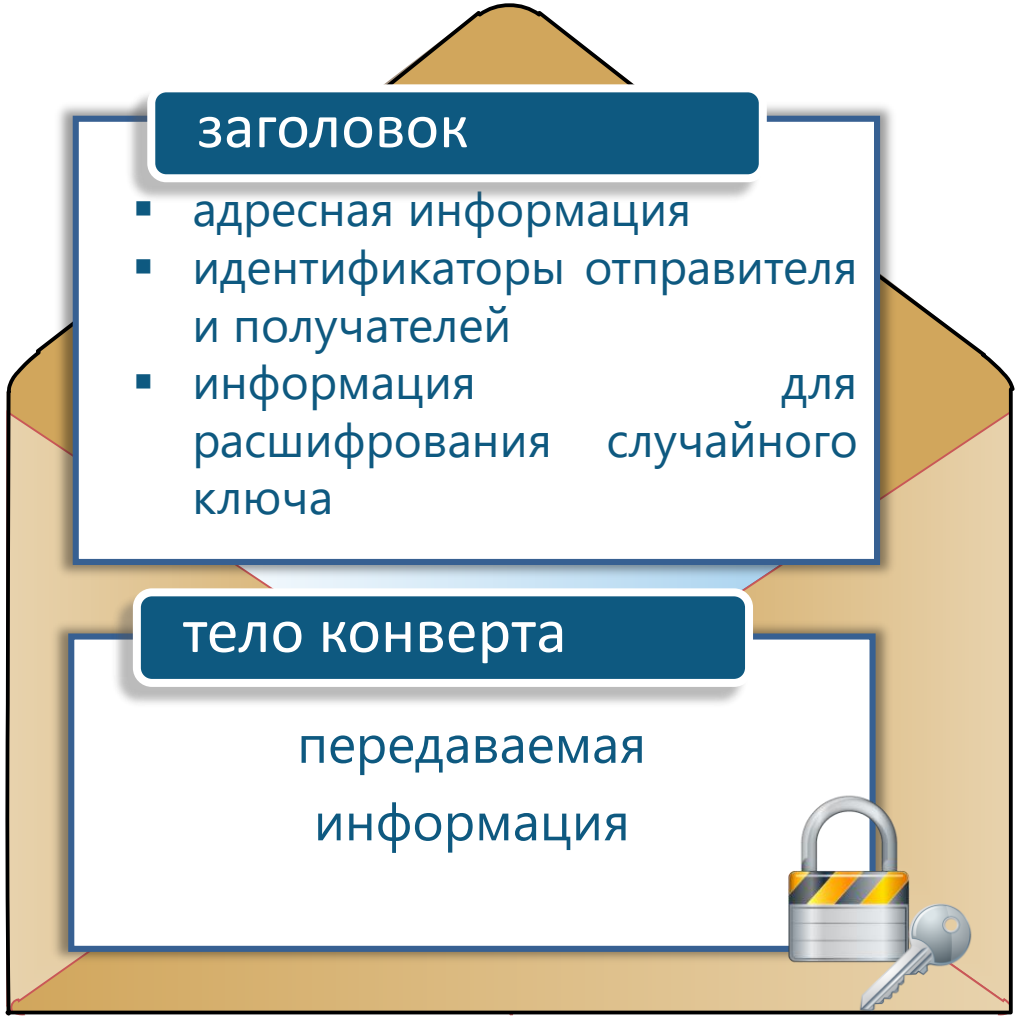
серверный режим работы

- **В серверном режиме транспортный модуль MFTP:**
  - работает на компьютере с установленным ПО ViPNet Coordinator или ViPNet CryptoService;
  - запускается одновременно с ViPNet, в состав которого входит, и остается активным в течение всего времени работы программы;
  - взаимодействует с клиентам, зарегистрированными на данном координаторе, и с другими координаторами, связь с которыми установил администратор сети ViPNet;
  - определяет маршрут передачи конвертов на сетевые узлы.

клиентский режим работы

Типы конвертов транспортного модуля

- **Прикладной конверт**
- **Прикладная квитанция**
- **Транспортная квитанция**
- **Служебный конверт**



Типы конвертов транспортного модуля

прикладной конверт

- файл, формируемый приложениями ViPNet (например, «Деловая почта», «Файловый обмен») для передачи другим сетевым узлам

прикладная квитанция

- файл, оповещающий отправителя о доставке и (или) прочтении прикладного конверта

транспортная квитанция

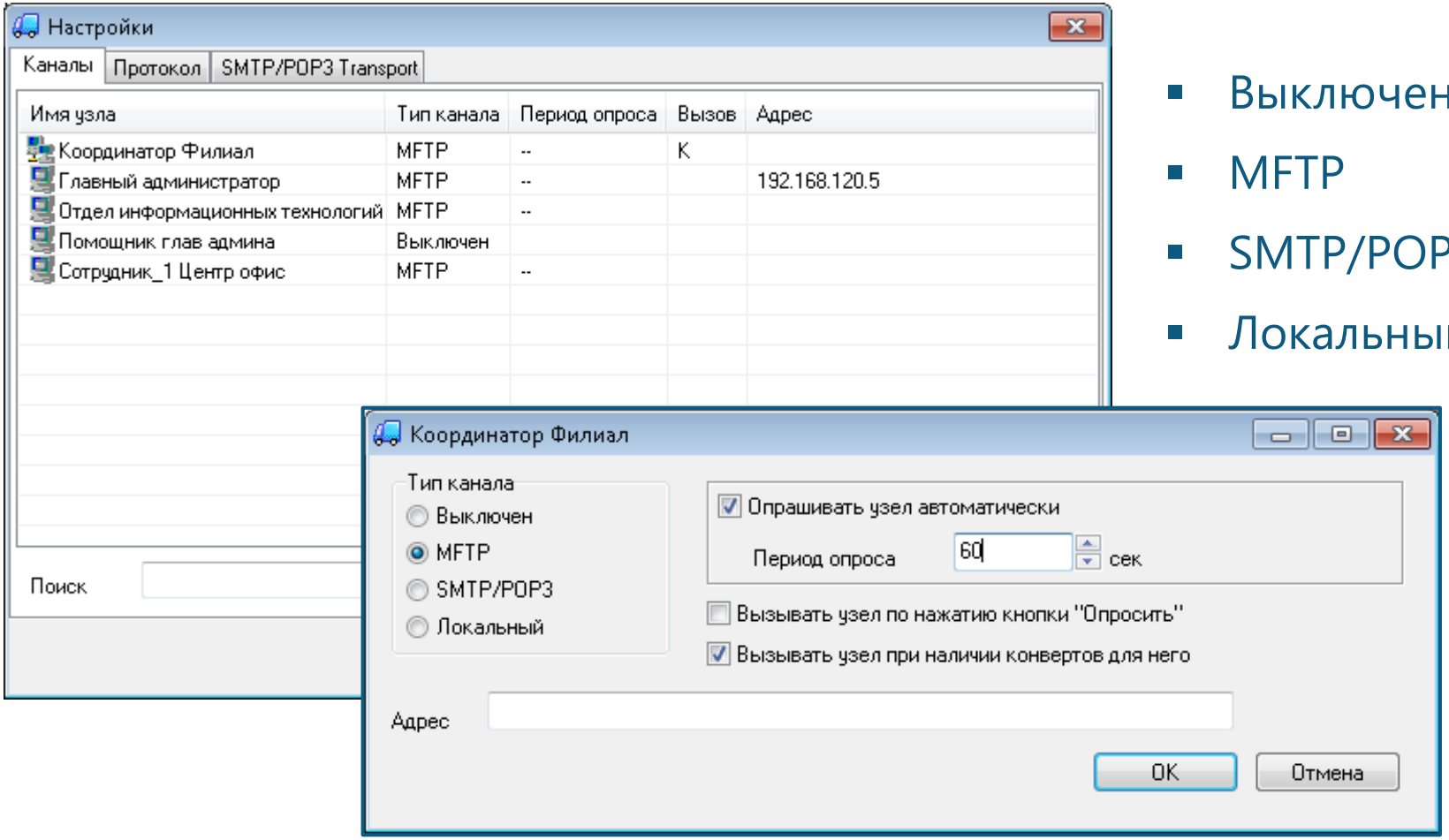
- файл, оповещающий отправителя о невозможности доставки конверта

служебный конверт

- файл, который содержит обновление справочников и ключей или обновление программного обеспечения ViPNet; предназначен для задач администрирования и формируется в программе ViPNet Центр управления сетью

Настройка ViPNet MFTP

Настройка каналов передачи конвертов

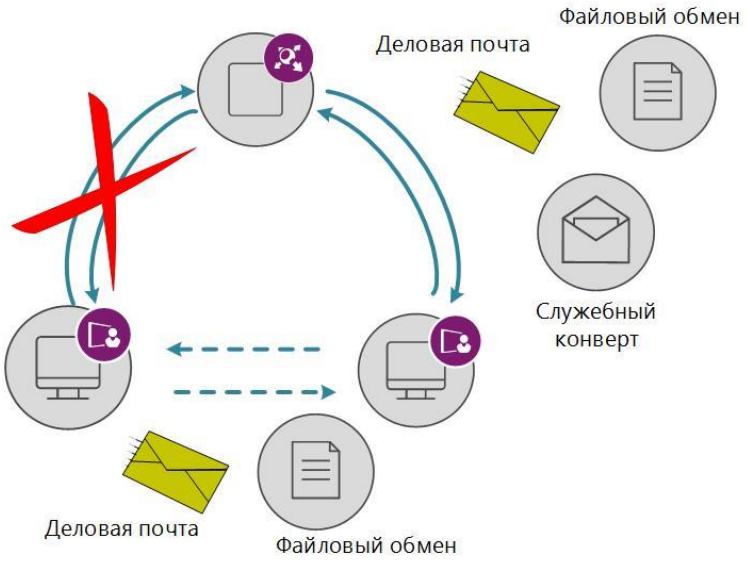


- Выключен
- MFTP
- SMTP/POP3
- Локальный

Настройка ViPNet MFTP

тип канала «Выключен»

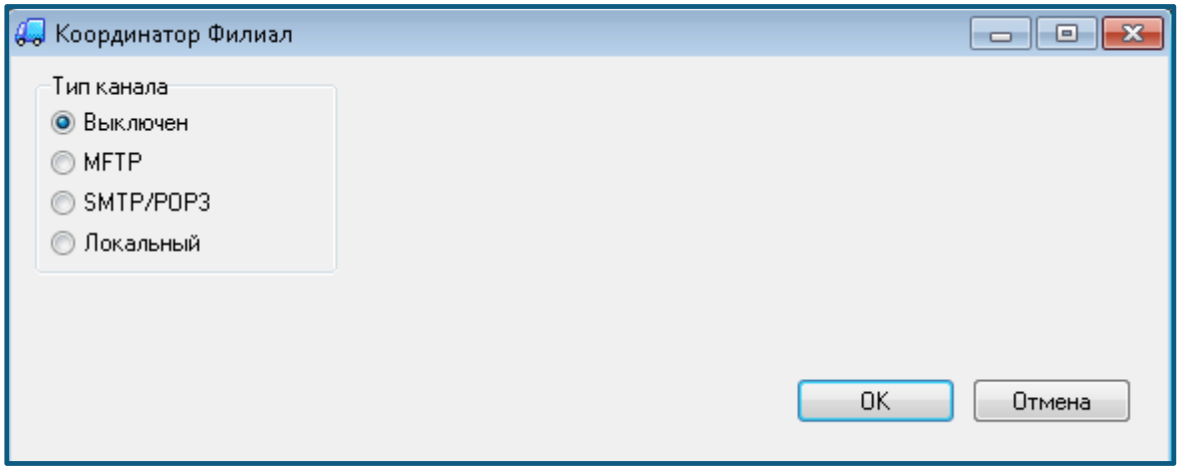
- при выборе режима "Выключен" координатор не будет пытаться соединиться с узлом ViPNet
- в зависимости от настроек все поступающие конверты будут удаляться или ожидать отправки
- может использоваться, когда нужно ограничить трафик между клиентом и координатором, например, при сбое



Настройка ViPNet MFTP

тип канала «Выключен»

- при выборе режима "Выключен" координатор не будет пытаться соединиться с узлом ViPNet
- в зависимости от настроек все поступающие конверты будут удаляться или ожидать отправки
- может использоваться, когда нужно ограничить трафик между клиентом и координатором, например, при сбое



Настройка ViPNet MFTP

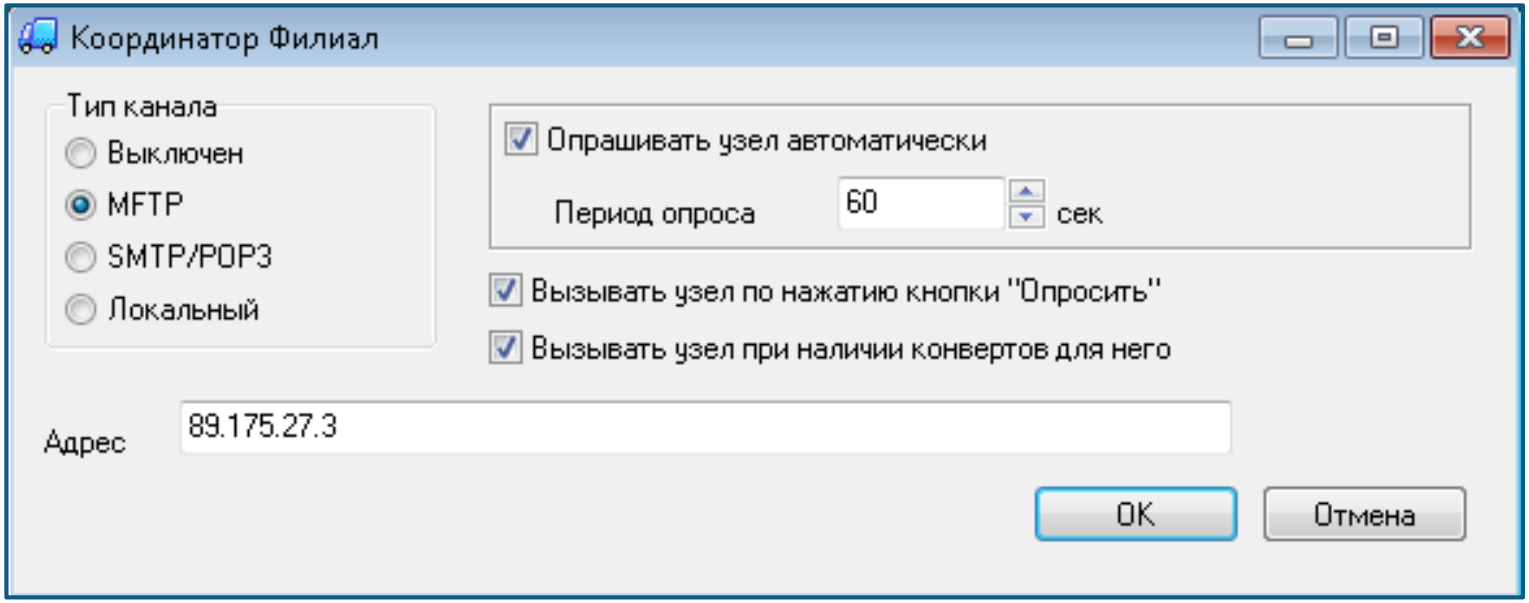
тип канала «MFTP»

- позволяет узлам ViPNet обмениваться данными напрямую друг с другом
- при восстановлении соединения после разрыва транспортный модуль MFTP продолжает передачу конвертов с того же места
- рекомендуется использовать при переносе клиента за другой сервер-маршрутизатор или при компрометации в сети ViPNet

Настройка ViPNet MFTP

тип канала «MFTP»

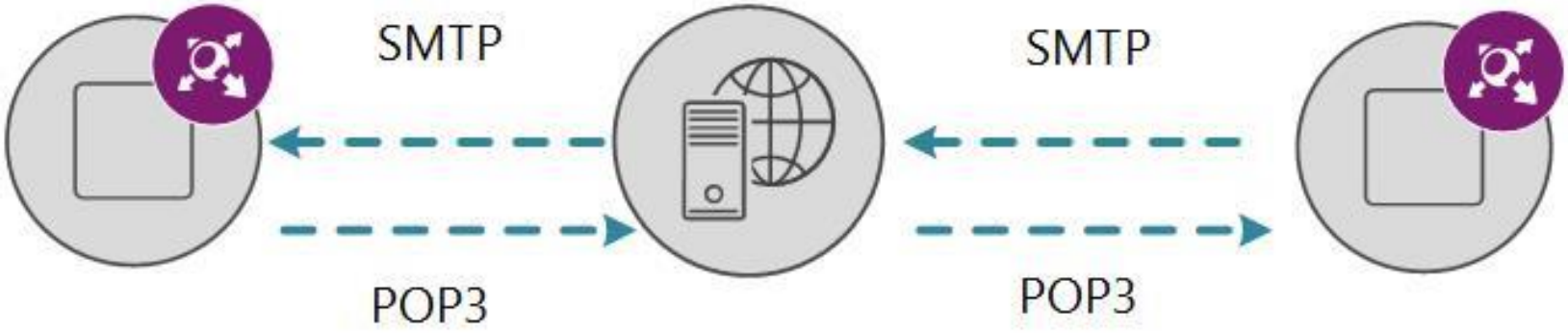
- позволяет узлам ViPNet обмениваться данными напрямую друг с другом
- при восстановлении соединения после разрыва транспортный модуль MFTP продолжает передачу конвертов с того же места
- рекомендуется использовать при переносе клиента за другой сервер-маршрутизатор или при компрометации в сети ViPNet



Настройка ViPNet MFTP

тип канала «SMTP/POP3»

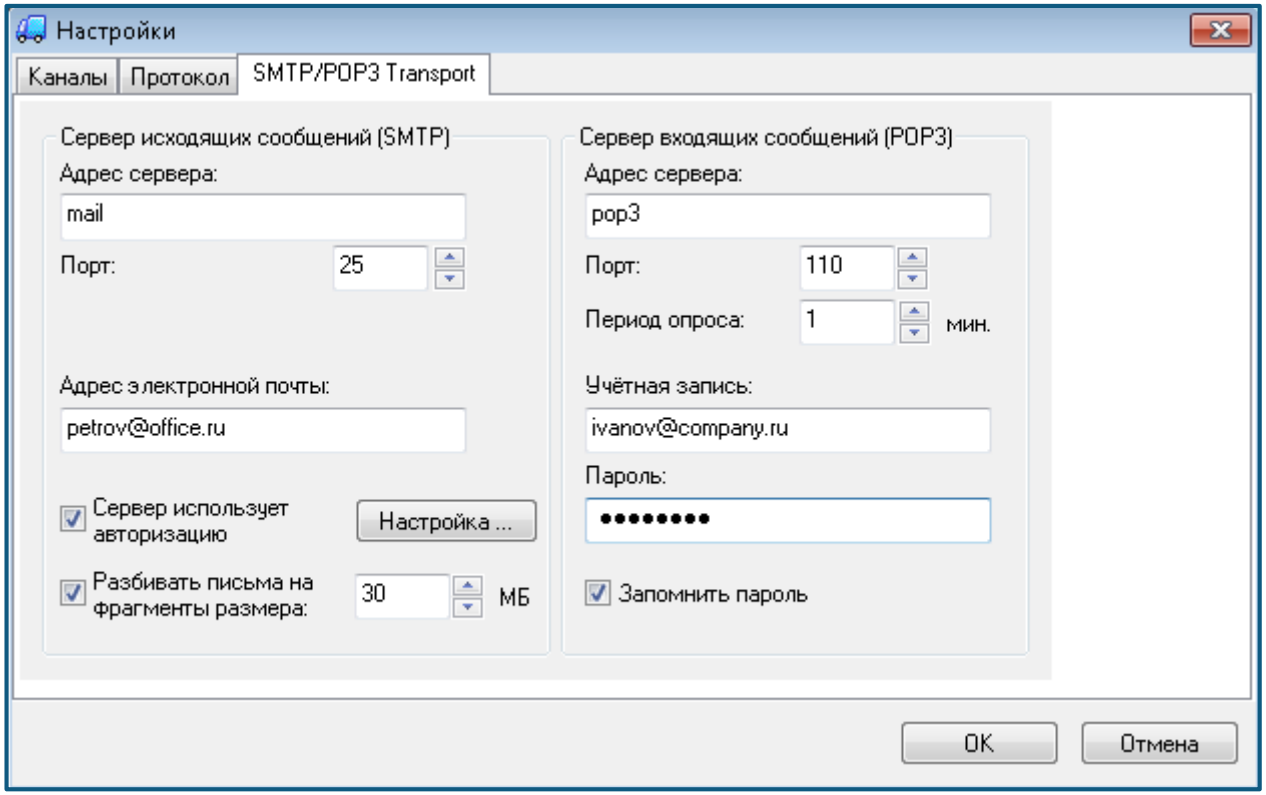
- использует почтовые сервера для обмена конвертами ViPNet
- рекомендуется использовать в сетях компаний, в которых невозможен доступ к внешним сетям по TCP-каналам



Настройка ViPNet MFTP

тип канала «SMTP/POP3»

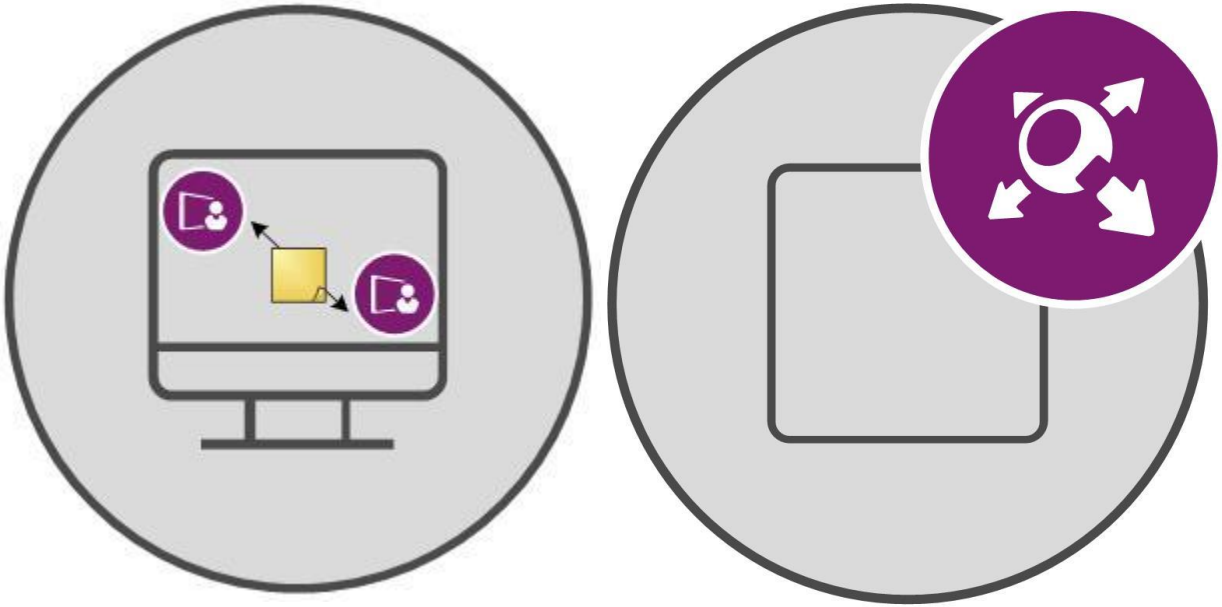
- использует почтовые сервера для обмена конвертами ViPNet
- рекомендуется использовать в сетях компаний, в которых невозможен доступ к внешним сетям по TCP-каналам



Настройка ViPNet MFTP

тип канала «Локальный»

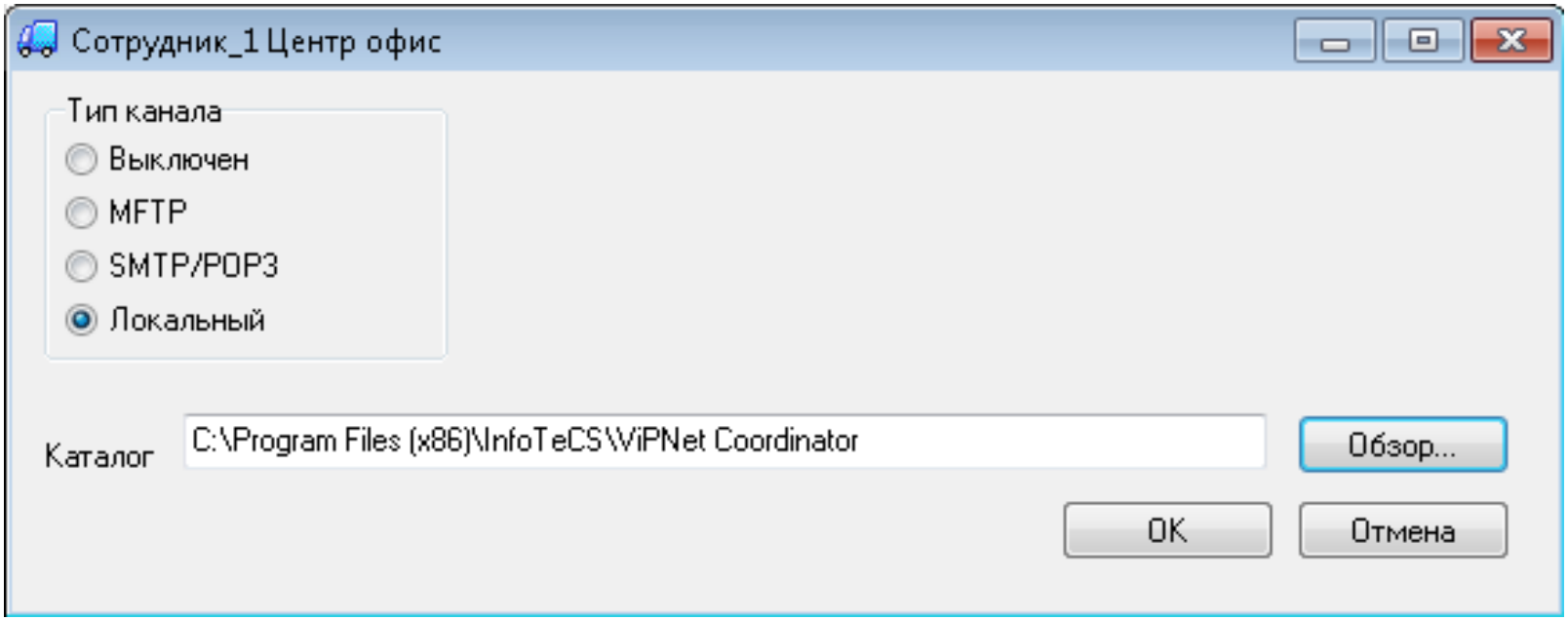
- конверты передаются через папку на диске
- рекомендуется использовать для обмена данными между узлами ViPNet, установленными на одном компьютере



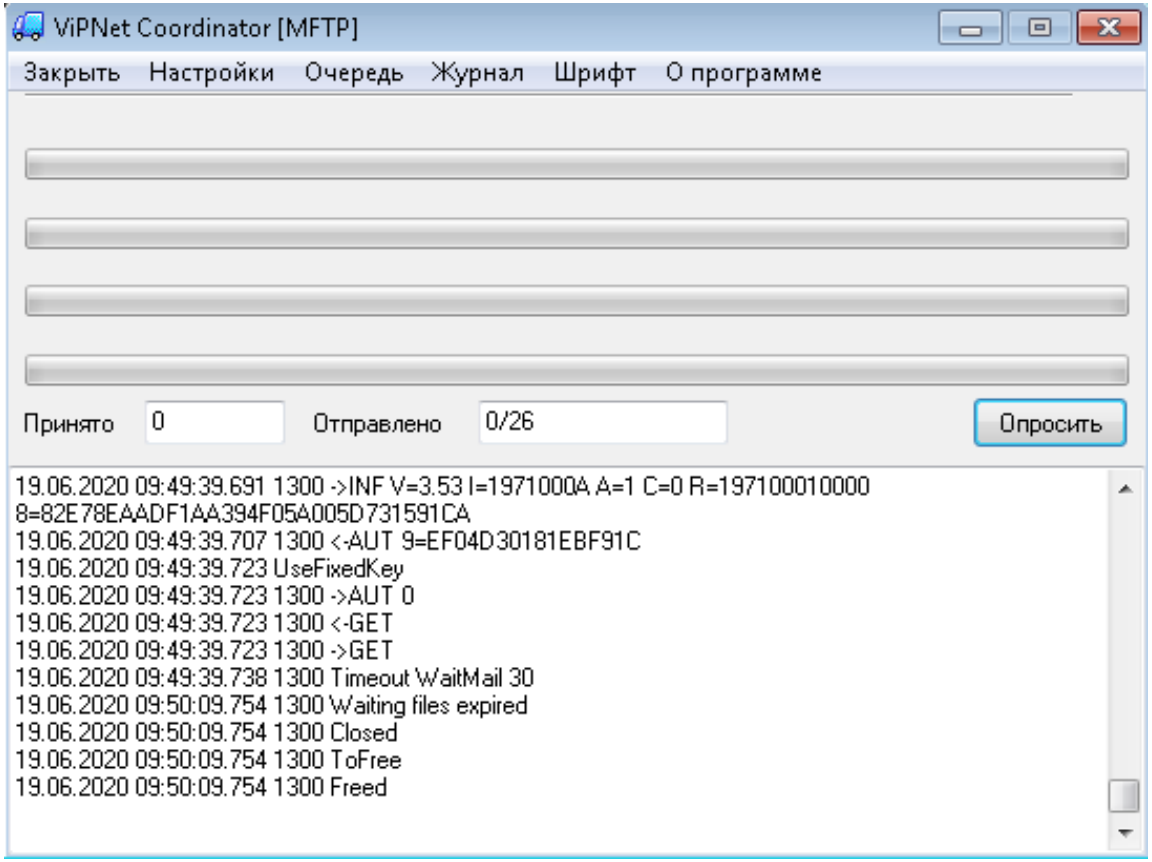
Настройка ViPNet MFTP

тип канала «Локальный»

- конверты передаются через папку на диске
- рекомендуется использовать для обмена данными между узлами ViPNet, установленными на одном компьютере

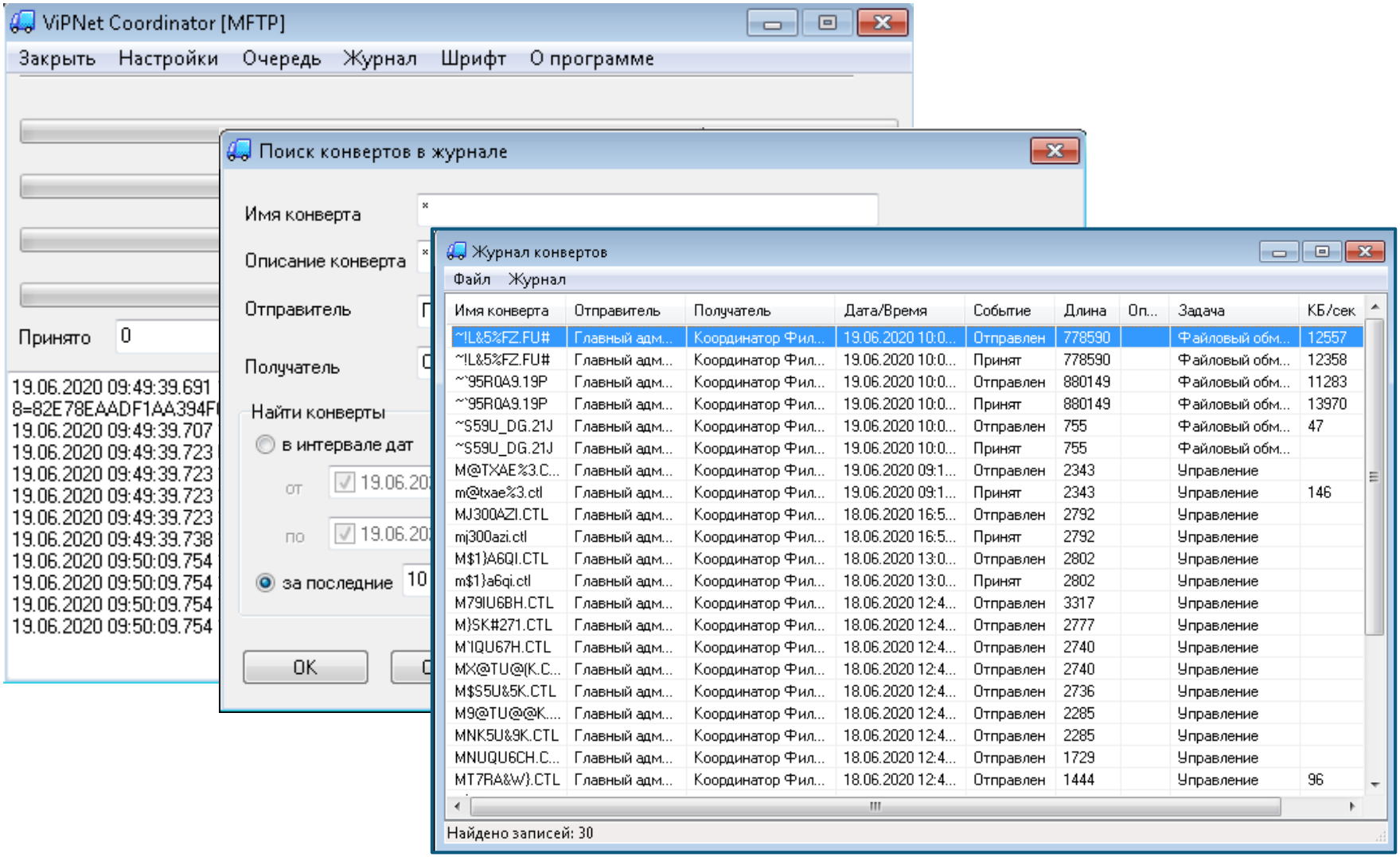


Работа с очередью и журналом конвертов



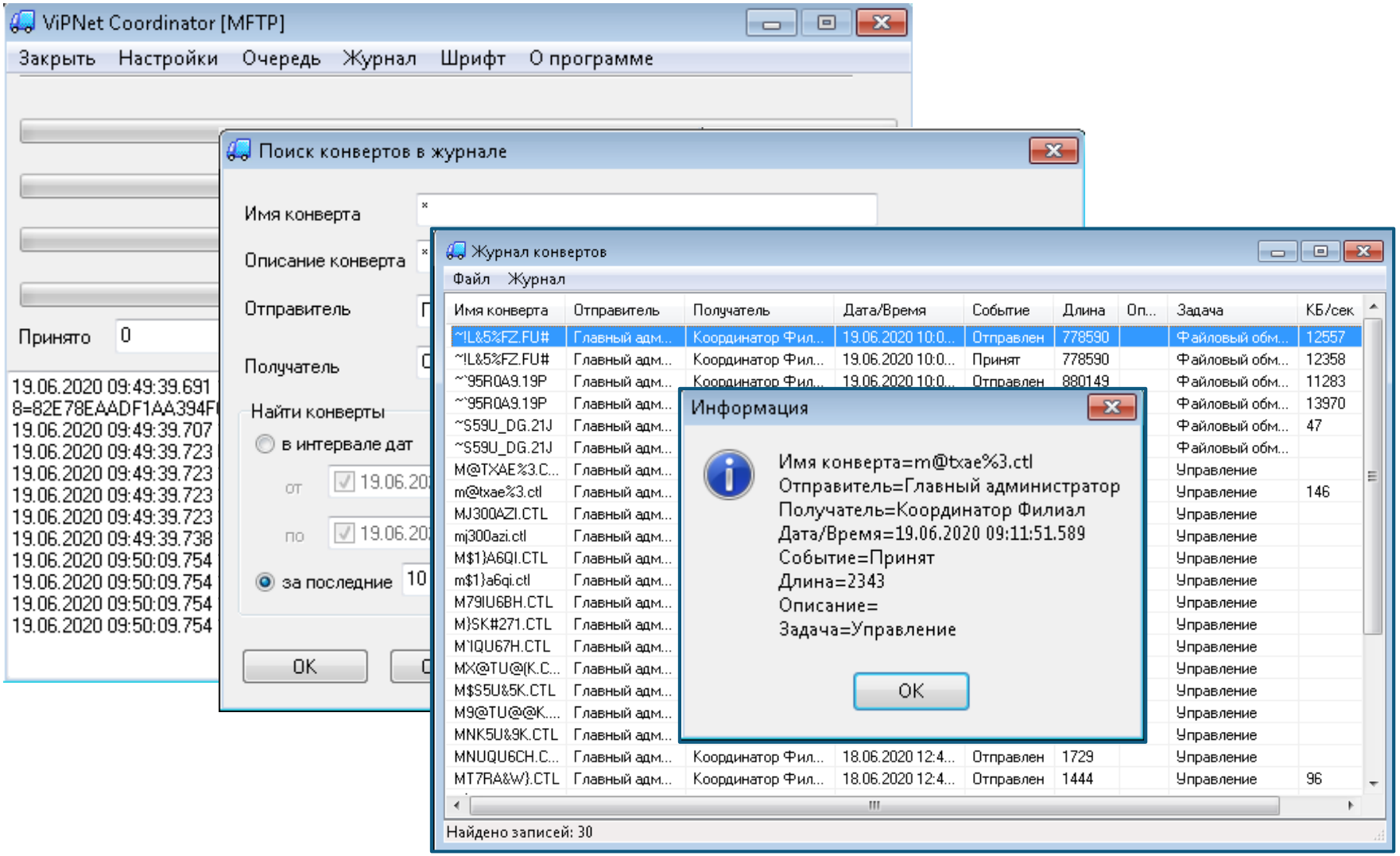
Настройка ViPNet MFTP

Работа с очередью и журналом конвертов

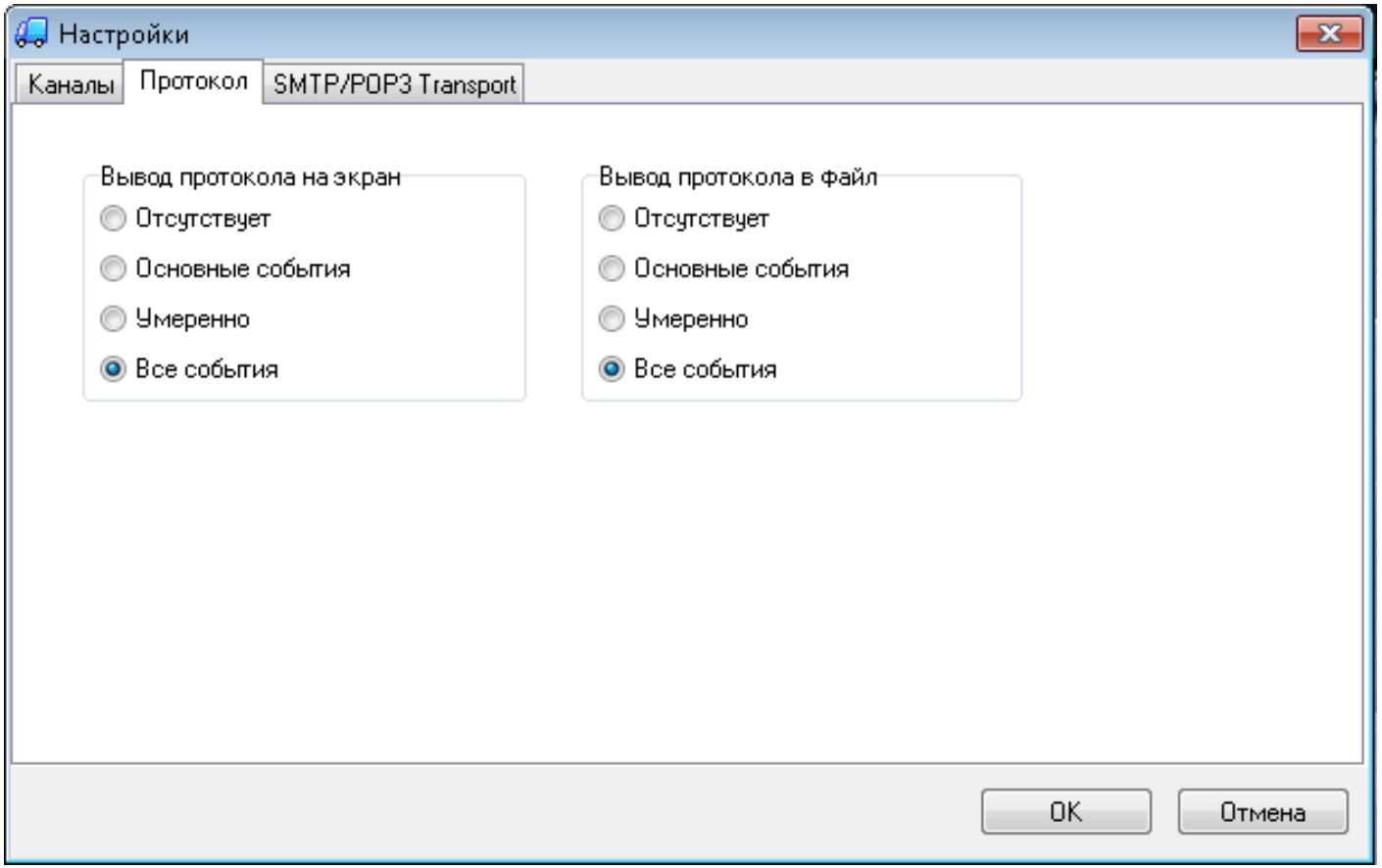


Настройка ViPNet MFTP

Работа с очередью и журналом конвертов



Настройка отображения журнала событий



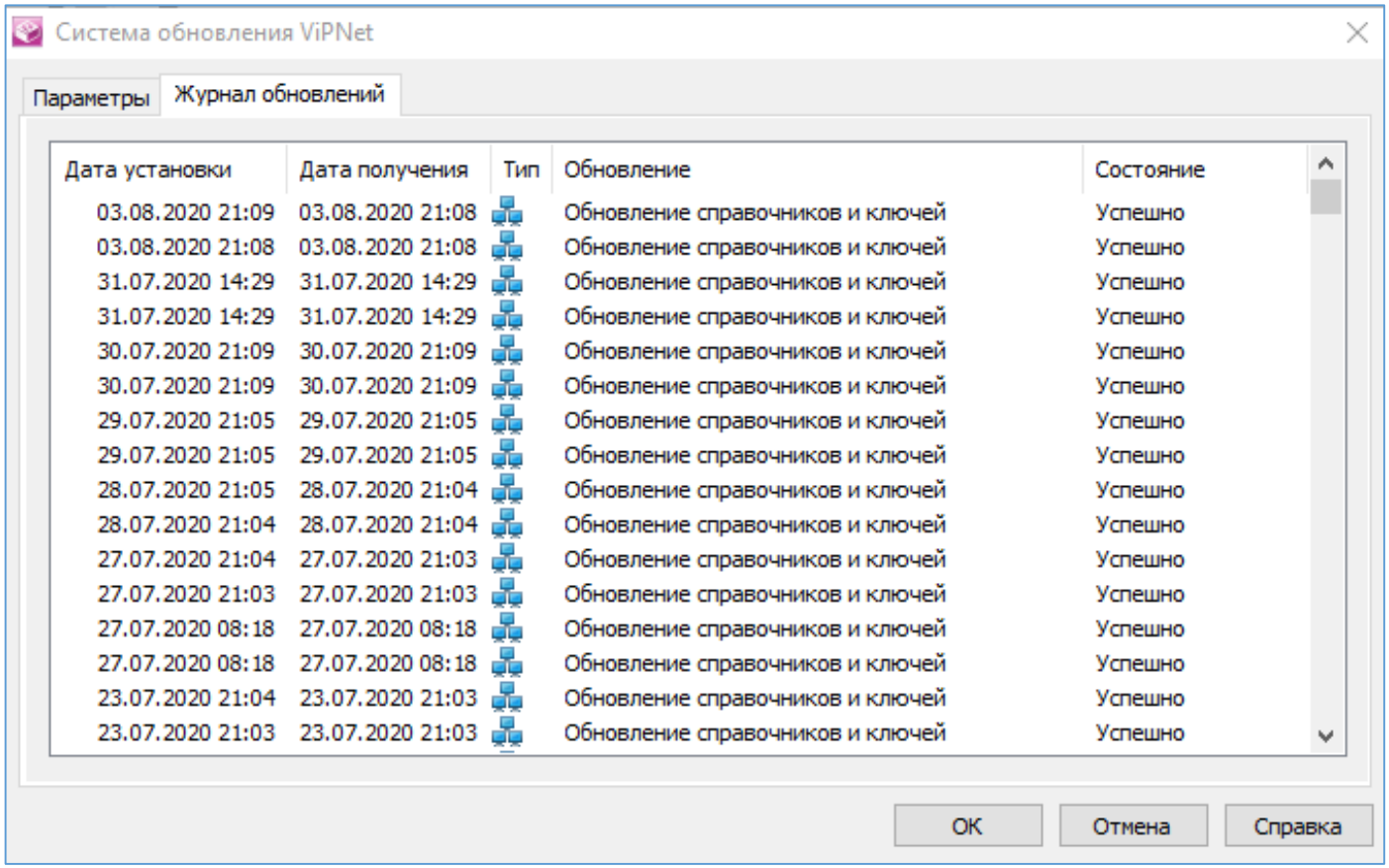
Система обновлений ViPNet

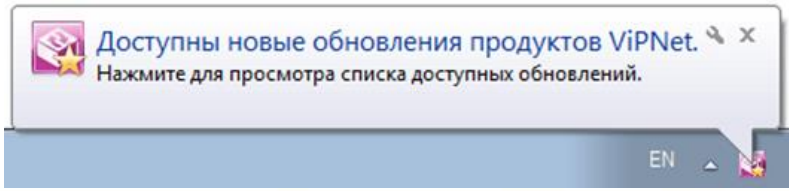
Система обновлений ViPNet

Система обновления ViPNet :

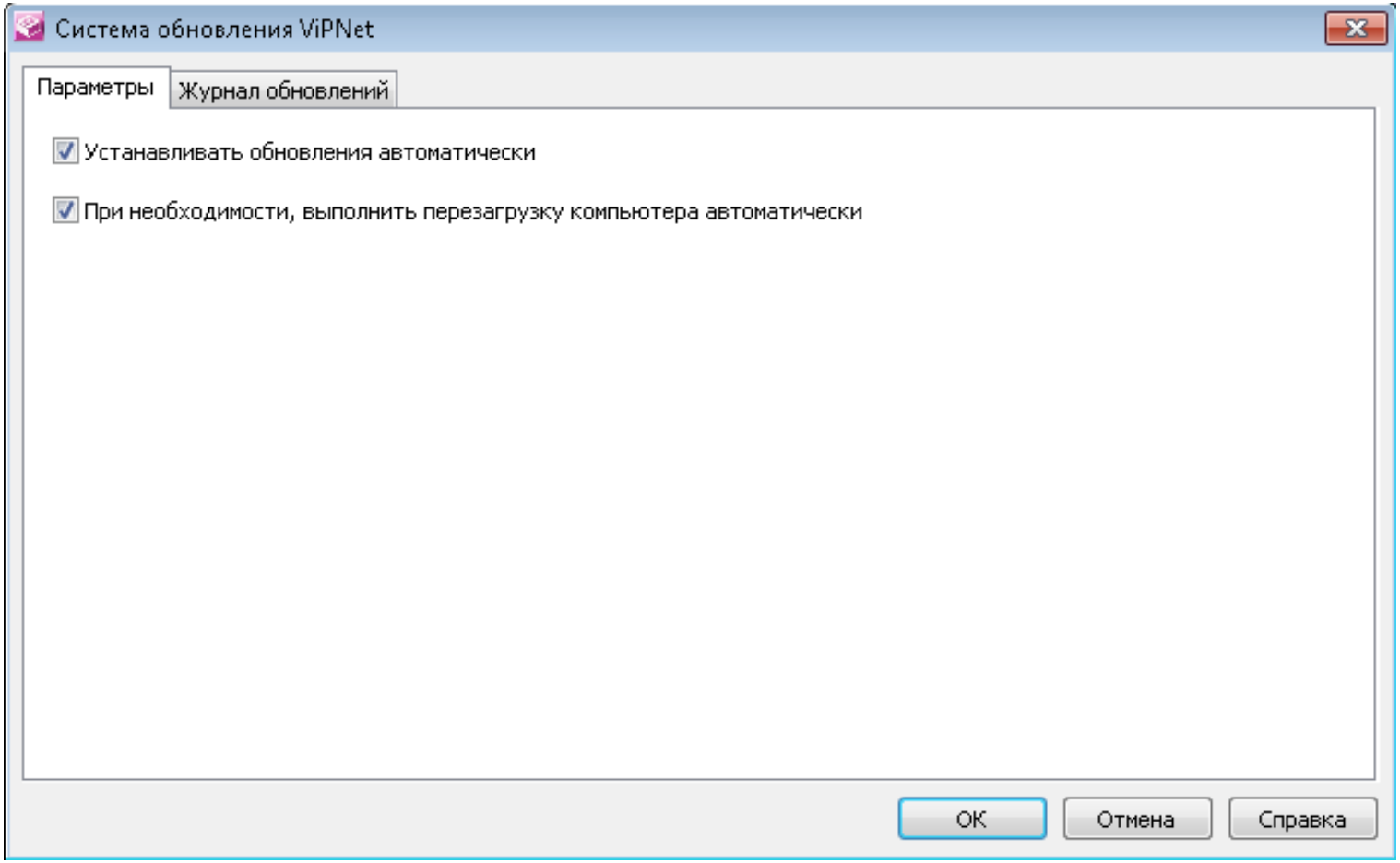
- **отвечает за получение и установку обновлений следующих типов:**
  - обновления ПО ViPNet Coordinator, полученные из программы ViPNet Administrator
  - обновления справочников и ключей, полученные из программы ViPNet Administrator
  - обновления политик безопасности, полученные из программы ViPNet Policy Manager

Настройка системы обновлений





Настройка системы обновлений



ViPNet StateWatcher

ViPNet StateWatcher

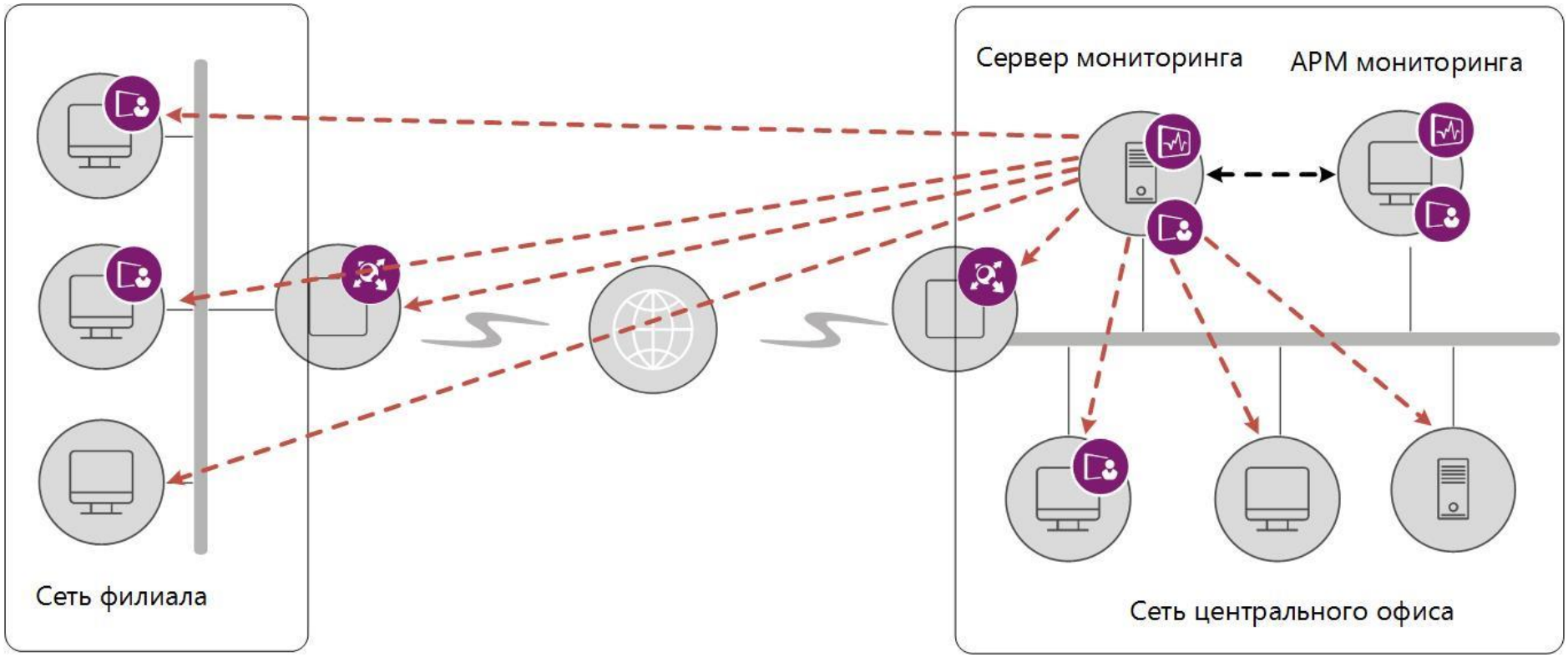
ViPNet StateWatcher:

предназначен для наблюдения за состоянием узлов сетей ViPNet, мониторинга событий безопасности, происходящих на сетевых узлах, своевременного выявления неполадок в работе узлов и оперативного оповещения пользователей о возникающих проблемах

Функции ViPNet StateWatcher

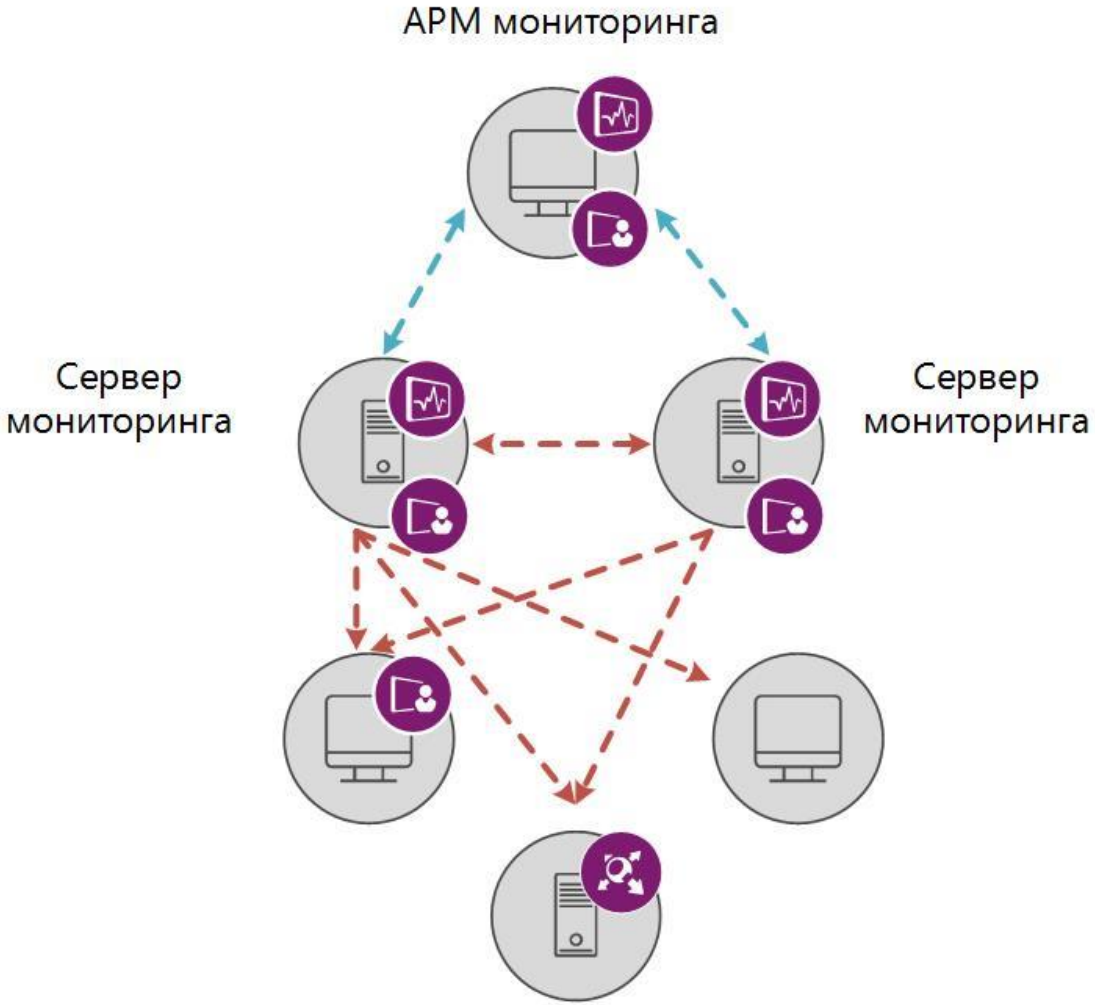
- сбор информации о текущем состоянии открытых и защищенных узлов сети ViPNet. Сбор информации осуществляется в соответствии с параметрами мониторинга, установленными администратором;
- хранение в базе данных информации, полученной при опросе узлов;
- определение правильности функционирования узлов на основании полученной информации.
- предоставление пользователям альтернативных способов наблюдения за состоянием узлов – в виде списка, на географической карте и в виде графиков;
- оповещение пользователей о сбоях в работе узлов и критических событиях на них различными способами: выделением узлов цветом в списке и на карте, отображением текстовых сообщений, проигрыванием звуковых файлов, SMS-сообщений и др.;
- и др.

Архитектура ViPNet StateWatcher

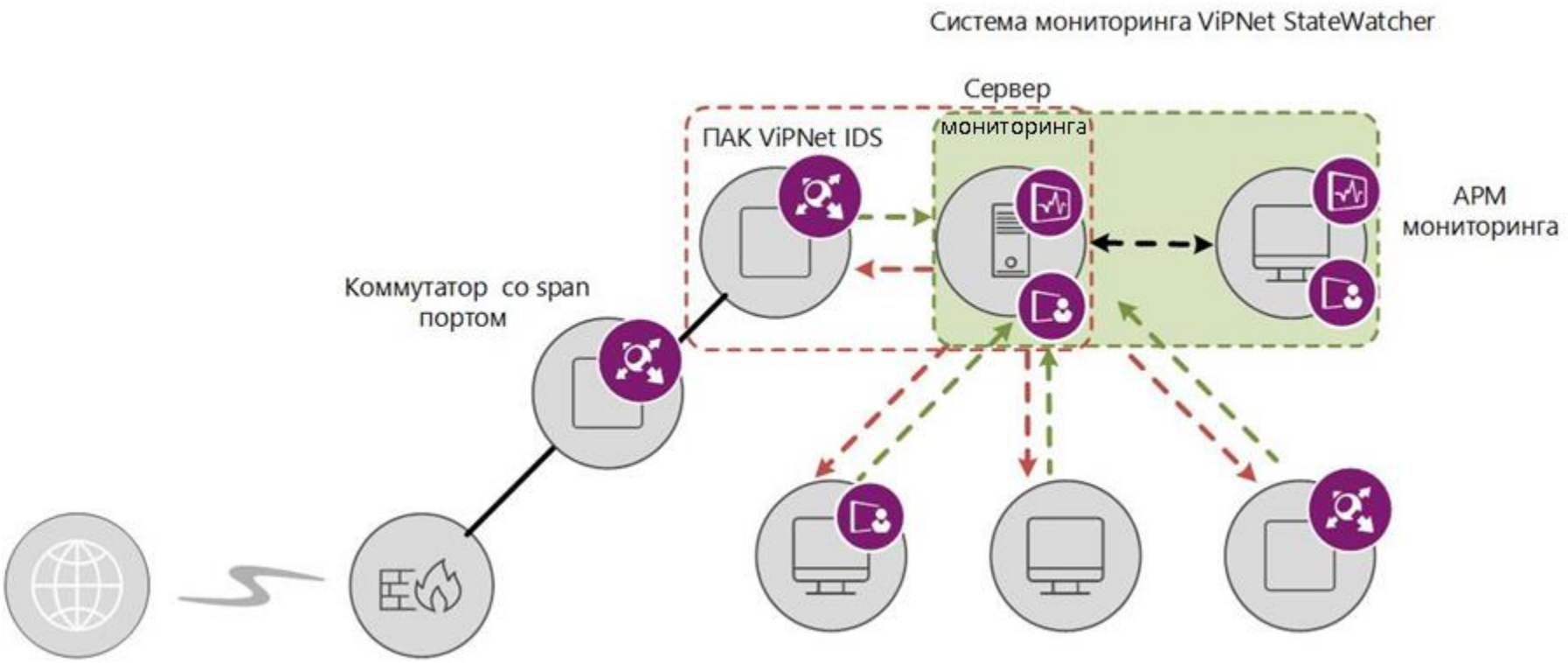


Архитектура ViPNet StateWatcher

- ***организация перекрестного мониторинга***



Взаимодействие с ViPNet IDS



Программно-аппаратные комплексы ViPNet

ПАК ViPNet

Серверные компоненты

- 1. **ViPNet Coordinator HW** — семейство шлюзов безопасности, входящих в состав продуктовой линейки ViPNet Network Security
- 2. **ViPNet Coordinator KB** - модельный ряд шлюзов безопасности ViPNet, удовлетворяющий требованиям к средствам криптографической защиты информации по классу КВ.
- 3. **ПАК ViPNet xFirewall** — это шлюз безопасности — межсетевой экран следующего поколения, который устанавливается на границе сети, обеспечивает фильтрацию трафика на всех уровнях, позволяет создать гранулированную политику безопасности на основе учетных записей пользователей и списка приложений.
- 4. **ViPNet Industrial Gateway** - индустриальные шлюзы безопасности с поддержкой промышленных протоколов, обеспечивающие защиту каналов связи и сетевое экранирование
- 5. И др.

ПАК ViPNet Coordinator HW

ViPNet Coordinator HW-VA

ViPNet Coordinator HW100

ViPNet Coordinator HW1000

ViPNet Coordinator HW2000

ViPNet Coordinator HW5000

ViPNet Coordinator HW-VPNM

ViPNet Coordinator HW

- семейство шлюзов безопасности, входящих в состав продуктовой линейки ViPNet Network Security;
- представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet;
- функционирует под управлением адаптированной операционной системы Linux;
- реализует функции межсетевого экрана, VPN-шлюза и VPN-сервера в IP-сетях, защита которых организуется совместно с программным комплексом ViPNet Network Security;
- предназначен для разграничения доступа к сетевым узлам, защиты соединений между корпоративной сетью и удаленными узлами, защиты от атак.

ViPNet Coordinator HW 50,100

- Шлюз безопасности для защиты филиалов компаний, небольших удаленных офисов и удаленных рабочих мест, а также терминалов и устройств. Благодаря поддержке каналов Ethernet, Wi-Fi, 3G и 4G, позволяет обеспечить безопасное подключение к корпоративной защищенной сети ViPNet по проводным и беспроводным каналам. Исполненный в форм-факторе miniPC, потребляет низкое количество электроэнергии, оснащен пассивной системой охлаждения и не требует каких-либо особых условий для размещения и эксплуатации.

Области применения:

- ✓ *Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site)*
- ✓ *Защищенный доступ удаленных и мобильных пользователей*
- ✓ *Взаимодействие с сетями ViPNet других организаций*
- ✓ *Защита беспроводных сетей связи*
- ✓ *Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)*
- ✓ *Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ)*
- ✓ *Защищенный контролируемый доступ в Интернет*
- ✓ *Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.*

Сертификат соответствия ФСБ России

Сертификат соответствия ФСБ России

ViPNet Coordinator HW 1000/ 2000/ 5000

- Шлюз безопасности для защиты компьютерных сетей масштаба предприятия. Позволяет организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру, и поддерживает защиту скоростных каналов связи до **1 Гбит/сек,/ до 2,7 Гбит/сек./ до 10 Гбит/сек** . Исполненный в форм-факторе 1U, потребляет низкое количество электроэнергии, обладает невысоким уровнем тепловыделения и не требует каких-либо особых условий для размещения и эксплуатации, представляя собой высокоэффективное средство сетевой защиты.

Области применения:

- ✓ *Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).*
- ✓ *Защищенный доступ удаленных и мобильных пользователей.*
- ✓ *Взаимодействие с сетями ViPNet других организаций.*
- ✓ *Защита магистральных каналов, соединяющих ЦОДы.*
- ✓ *Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).*
- ✓ *Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение DMZ).*
- ✓ *Защищенный контролируемый доступ в Интернет.*
- ✓ *Организация контролируемого доступа пользователей из публичной сети к предоставляемым организацией ресурсам и сервисам.*

Сертификат соответствия ФСБ России

Сертификат соответствия ФСБ России

ViPNet Coordinator KB

- Семейство шлюзов безопасности в составе продуктовой линейки ViPNet Network Security с повышенным уровнем безопасности класса КВ.
- Представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet.
- Функционирует под управлением адаптированной операционной системы Linux.
- Реализует функции межсетевого экрана, VPN-шлюза и VPN-сервера в IP-сетях, защита которых организуется совместно с программным комплексом ViPNet Network Security.
- Предназначен для разграничения доступа к сетевым узлам, защиты соединений между корпоративной сетью и удаленными узлами, защиты от атак.

ViPNet Coordinator KB 2 100/ 1000

- Маршрутизация и контроль целостности зашифрованных IP-пакетов, передаваемых между узлами сети ViPNet.
- Туннелирование (шифрование и имитозащита) открытых IP-пакетов, передаваемых между объектами сети ViPNet, находящимися в разных сегментах сети.
- Межсетевое экранирование — анализ, фильтрация, регистрация открытого IP-трафика и обнаружение атак на границе сегмента сети ViPNet.
- Маршрутизация почтовых сообщений, передаваемых почтовыми клиентами корпоративной электронной почты ViPNet Деловая почта.

Области применения:

✓ *Построение защищенных каналов связи между офисами компании (Site-to-Site и Multi Site-to-Site).*

✓ *Защищенный доступ удаленных и мобильных пользователей.*

✓ *Взаимодействие с сетями ViPNet других организаций.*

✓ *Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь).*

✓ *Разграничение доступа к информации в локальных сетях и сегментирование локальных сетей (например, выделение DMZ).*

✓ *Защищенный контролируемый доступ в Интернет.*

✓ *Организация контролируемого доступа пользо предоставляемым организацией ресурсам и сервисам.*

Сертификат соответствия ФСБ России

Сертификат соответствия ФСБ России

ViPNet Coordinator Industrial Gateway

- Индустриальные шлюзы безопасности с поддержкой промышленных протоколов, обеспечивающие защиту каналов связи и сетевое экранирование.
- Представляет собой интегрированное решение на базе специализированной аппаратной платформы и программного обеспечения ViPNet.
- Функционирует под управлением адаптированной операционной системы Linux.
- Реализует функции межсетевого экрана, VPN-шлюза и VPN-сервера в IP-сетях, защита которых организуется совместно с программным комплексом ViPNet Network Security.
- Предназначен для разграничения доступа к сетевым узла защиты соединений между корпоративной сетью и удаленными узлами, защиты от атак.

ViPNet Coordinator IG 10

- Сетевой шлюз безопасности в индустриальном исполнении, предназначенный для защиты каналов в промышленных системах и сегментирования их на домены безопасности. Обеспечивает эффективную защиту от сетевых атак и несанкционированного доступа путем создания защищенных каналов на основе технологии ViPNet. Легко встраивается в существующую инфраструктуру.

Области применения:

- ✓ *Защита индустриальной сети, индустриальной беспроводной локальной сети (WLAN).*
- ✓ *Защищенный удаленный мониторинг.*
- ✓ *Эшелонированная защита (использование ПАК для защиты каналов совместно со средствами защиты данных на прикладном уровне).*
- ✓ *Сегментация и защита периметра, разграничение доступа.*
- ✓ *Контроль доступа из индустриальной сети в Интернет.*
- ✓ *Защищенный удаленный доступ в индустриальную сеть, к рабочему столу оператора или инженера, а также к оборудованию. В том числе имеется возможность осуществлять мобильный удаленный доступ.*
- ✓ *Коммуникационный шлюз для взаимодействия с промышленным оборудованием по последовательным интерфейсам*

ПАК ViPNet xFirewall

Это **шлюз безопасности** — межсетевой экран следующего поколения, который устанавливается на границе сети, обеспечивает фильтрацию трафика на всех уровнях, позволяет создать гранулированную политику безопасности на основе учетных записей пользователей и списка приложений.

Области применения:

- ✓*Гранулированная политика безопасности, которая строится в терминах «Пользователь» — «Приложение» — разрешить/запретить*
- ✓*Обеспечение безопасного использования персональных устройств в рабочих целях с полным соблюдением политик безопасности компании – BOYB (Bring Your Own Device)*
- ✓*Выявление и блокировка более 2000 прикладных протоколов и приложений: игры, социальные сети, torrent и т.д.*
  - *Снижение расходов на потребление Интернет-трафика*
  - *Минимизация поверхности атак*

Сертификат соответствия ФСТЭК России.

infotecs

Спасибо за внимание!

Вопросы?

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»
education@infotecs.ru

ОАО «ИнфоТеКС», Москва
(495) 737-61-92
www.infotecs.ru