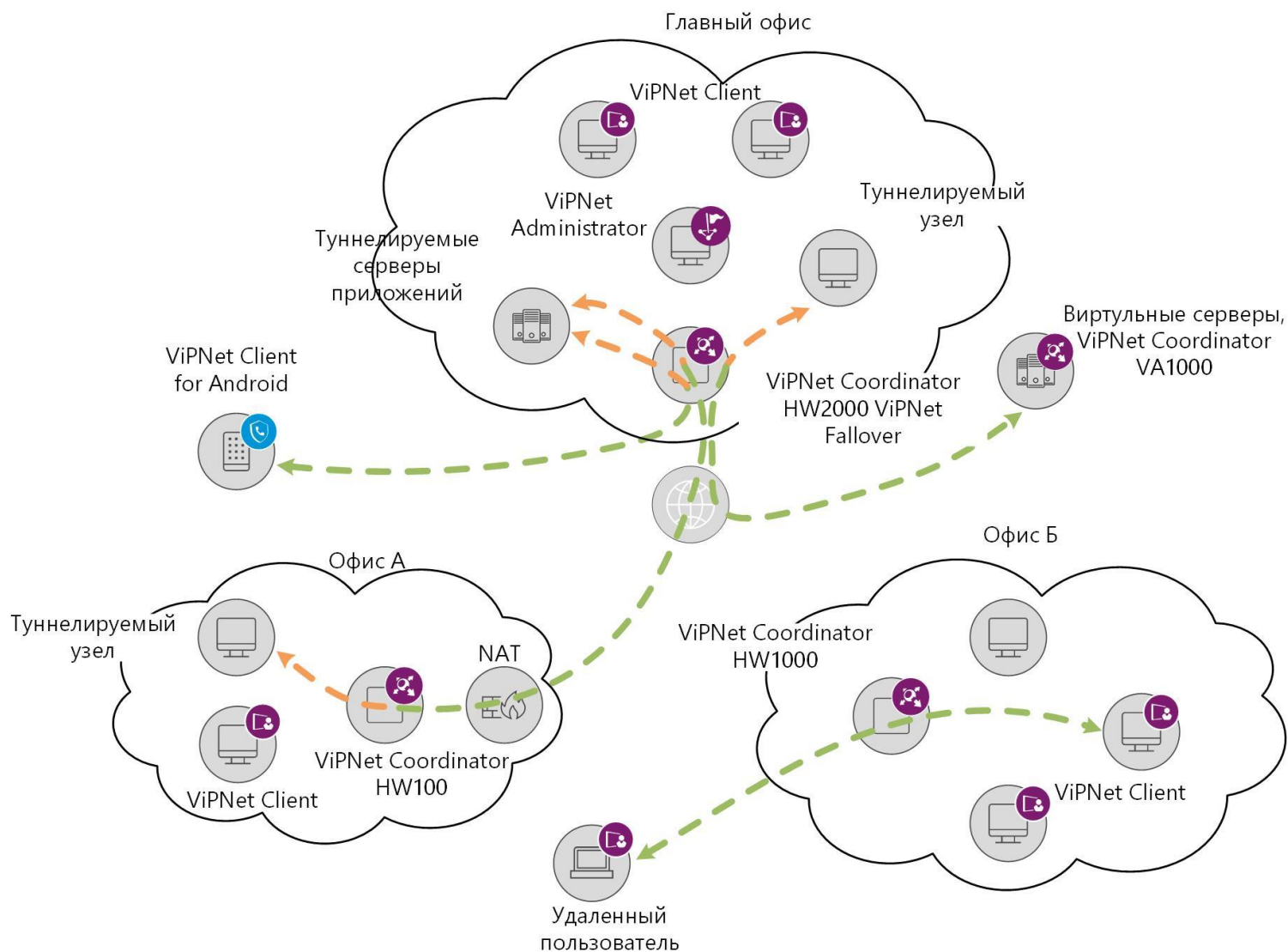


# ViPNet Coordinator 4.x

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»  
[education@infotecs.ru](mailto:education@infotecs.ru)

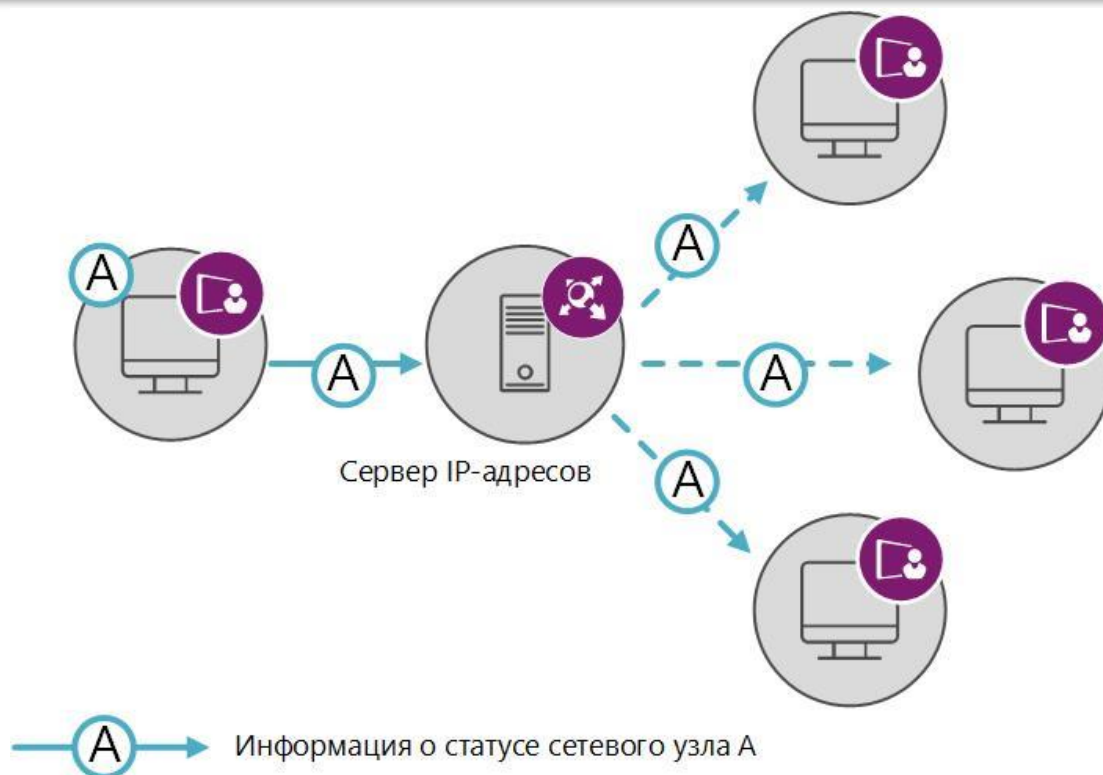
ОАО «ИнфоТеКС», Москва  
(495) 737-61-92  
[www.infotecs.ru](http://www.infotecs.ru)

# Пример использования компонентов сети ViPNet в крупной компании



## Сервер IP-адресов

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



## 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.



## 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.



## VPN-шлюз

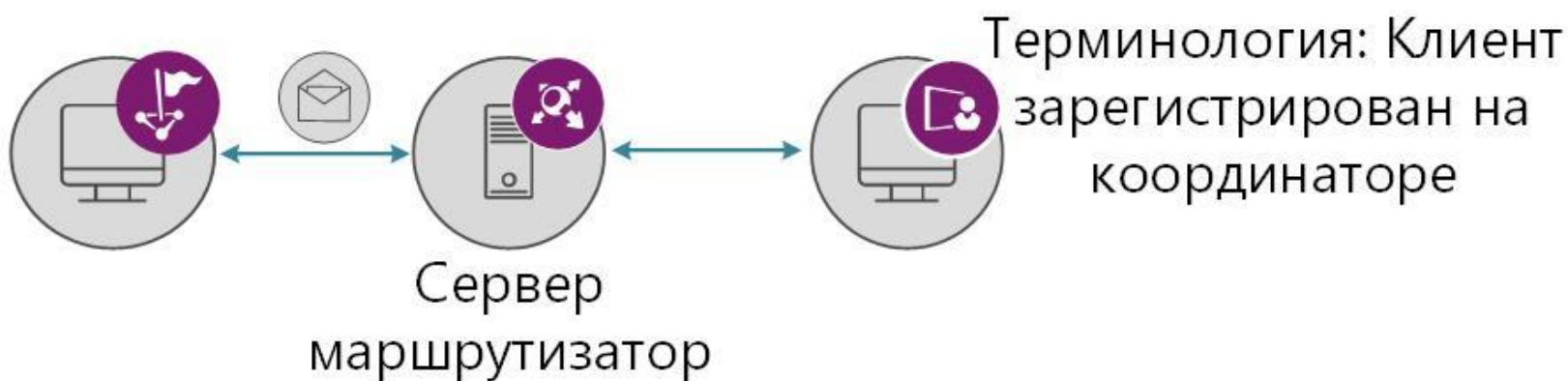
- позволяет создавать защищенные каналы (туннели) посредством шифрования трафика открытых узлов, размещенных за координатором, и передачи этого трафика на другие VPN-шлюзы или защищенные клиенты;
- VPN-шлюз интегрирован с межсетевым экраном для защищенных и открытых соединений, осуществляющим фильтрацию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





### 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.



## Межсетевой экран

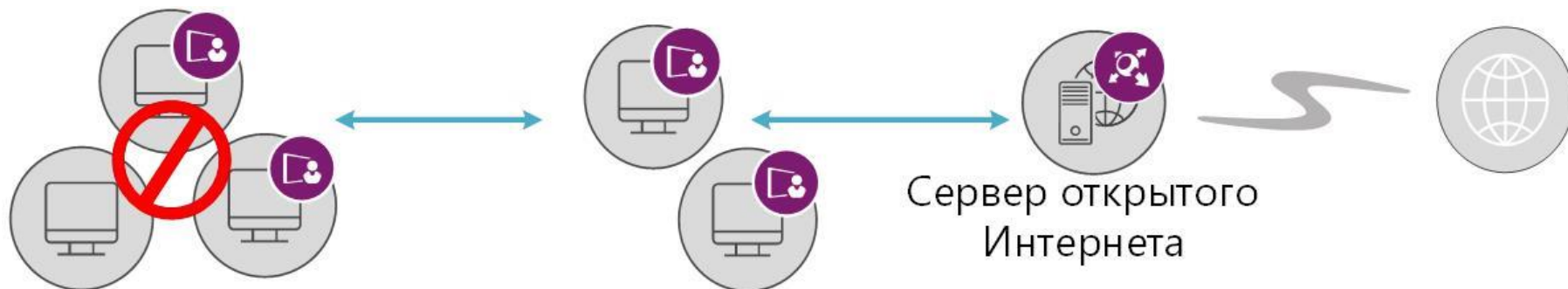
- выполняет фильтрацию открытых, транзитных и локальных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил;
- осуществляет трансляцию адресов (NAT) для проходящего через координатор открытого трафика. Позволяет задать правила 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.





### Сервер открытого Интернета

- позволяет обеспечить отдельный 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.



### ТСР-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 ТСР-туннель, он автоматически начинает устанавливать с узлами соединение через ТСР-туннель сервера соединений. На сервере соединений полученные IP-пакеты извлекаются из ТСР-туннеля и передаются дальше на узлы назначения по UDP-протоколу.



## Новые возможности ViPNet Coordinator 4.x



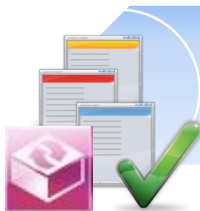
реализована установка ViPNet Coordinator с помощью установочного пакета MSI и сценария входа в систему logon script;



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;

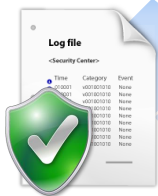


обеспечена интеграция с программой ViPNet SafeDisk-V;

## 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.

### 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.

### 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.



### 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.

### ViPNet Контроль приложений:

- отслеживает сетевую активность 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.

## 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**

## 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;

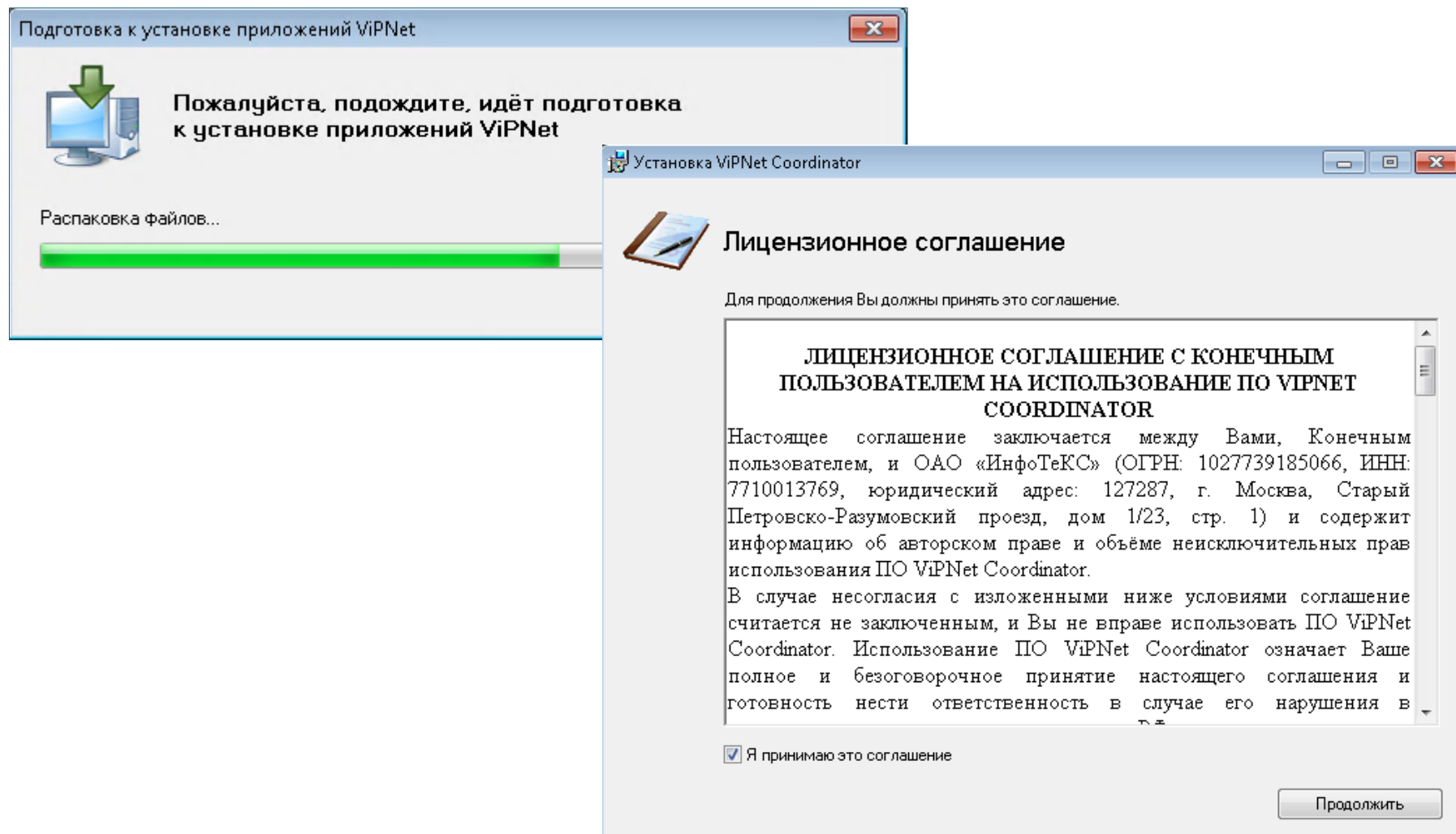


отключить сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT);

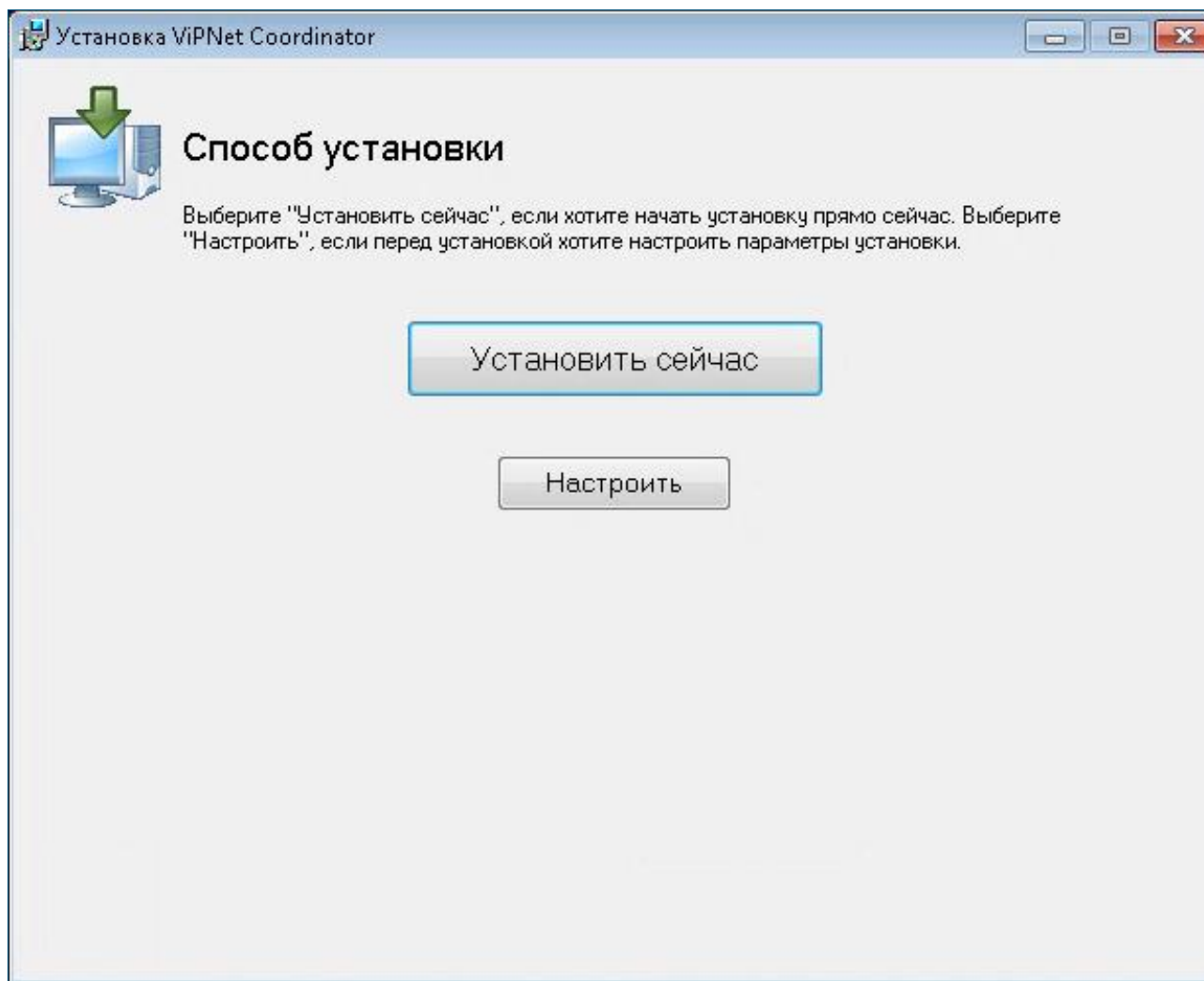


убедиться, что на компьютере правильно заданы часовой пояс, дата и время.

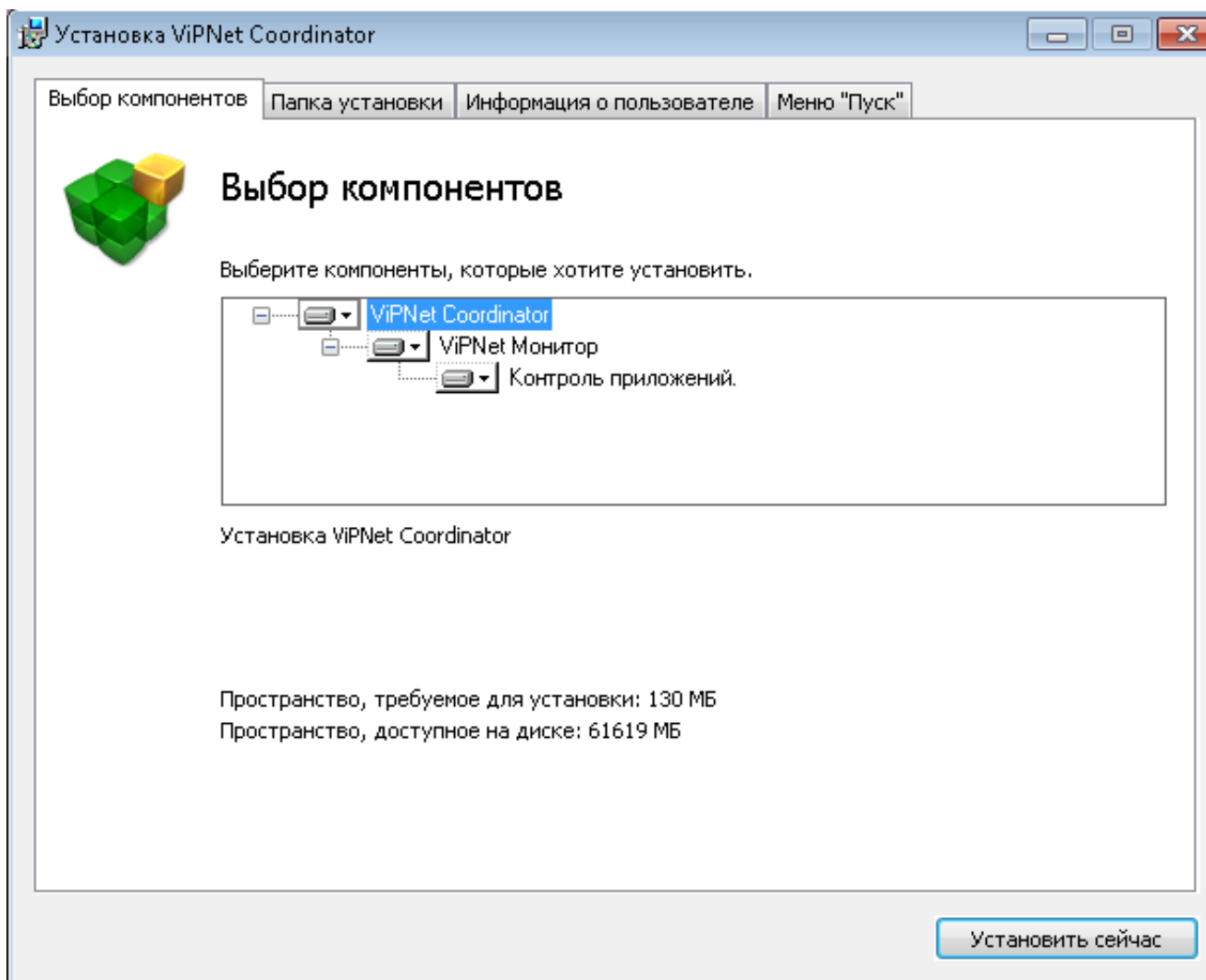
## Установка в интерактивном режиме



## Установка в интерактивном режиме

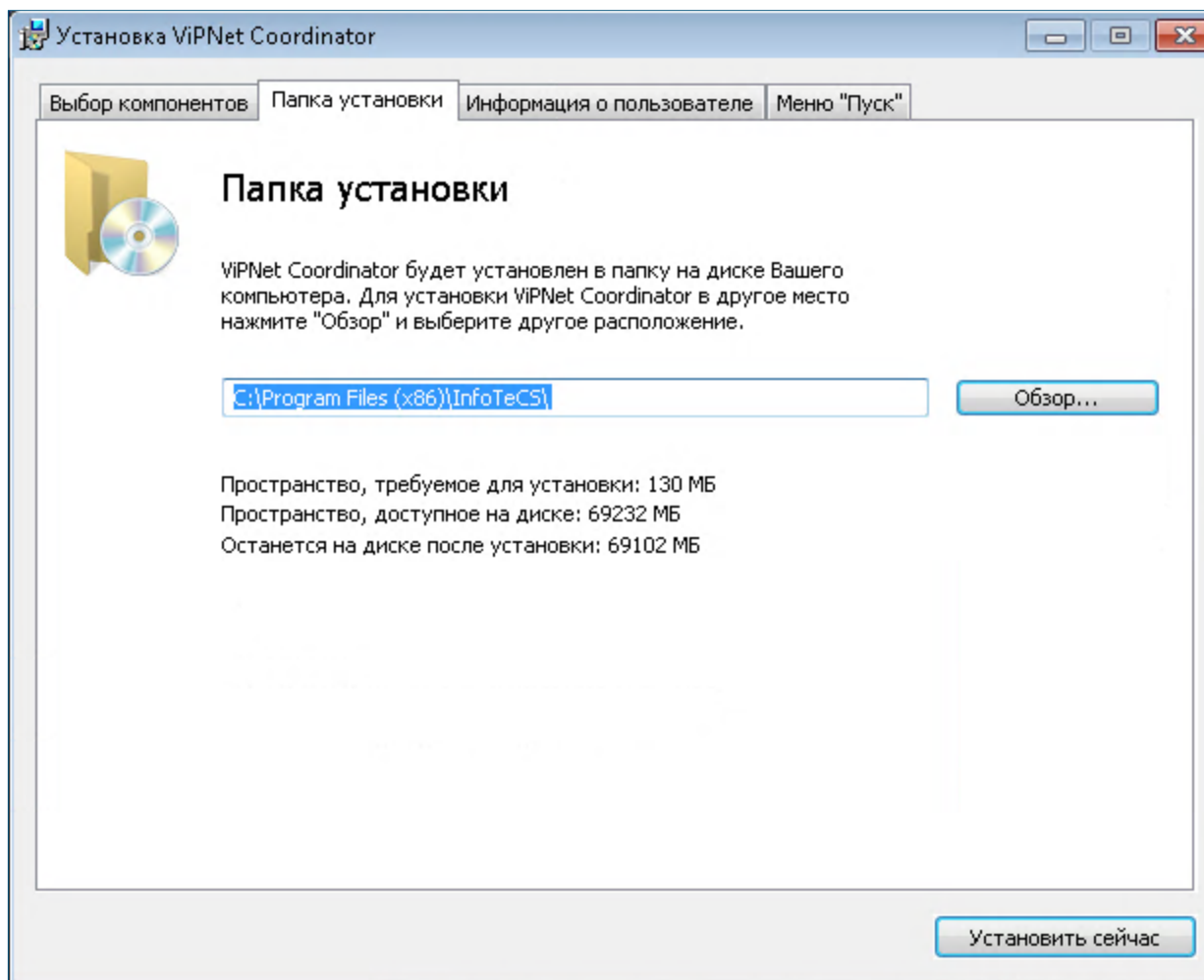


## Дополнительные параметры установки

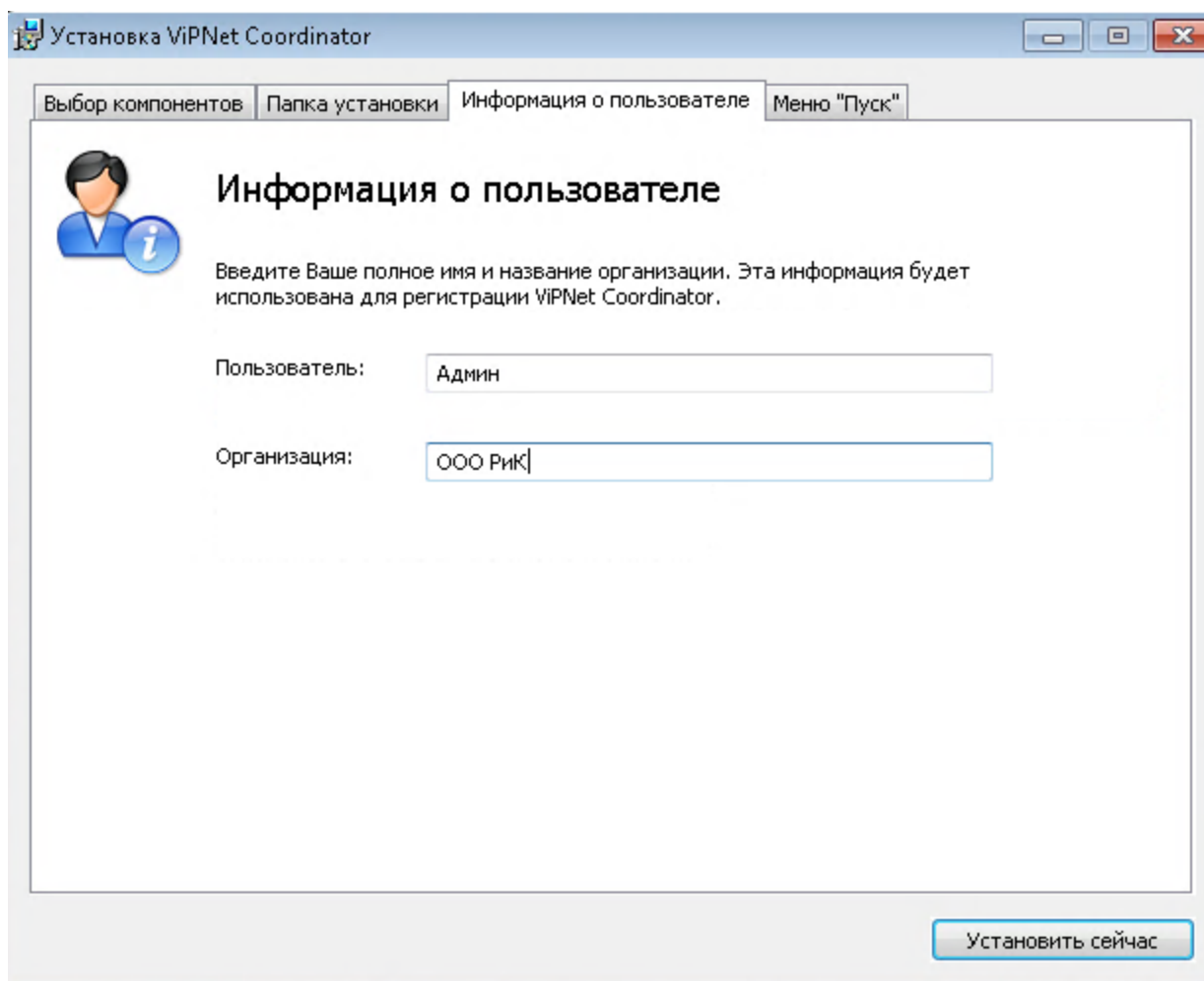




## Дополнительные параметры установки





## Дополнительные параметры установки



The screenshot shows the 'Установка ViPNet Coordinator' window with the 'Информация о пользователе' tab selected. The window has a title bar with standard Windows controls. Below the title bar are four tabs: 'Выбор компонентов', 'Папка установки', 'Информация о пользователе', and 'Меню "Пуск"'. The 'Информация о пользователе' tab is active, displaying a user icon and an information icon. The text instructs the user to enter their full name and organization name for registration. Two text input fields are provided: 'Пользователь:' with the value 'Админ' and 'Организация:' with the value 'ООО РИК'. A 'Установить сейчас' button is located at the bottom right of the window.

Установка ViPNet Coordinator

Выбор компонентов | Папка установки | **Информация о пользователе** | Меню "Пуск"

  **Информация о пользователе**

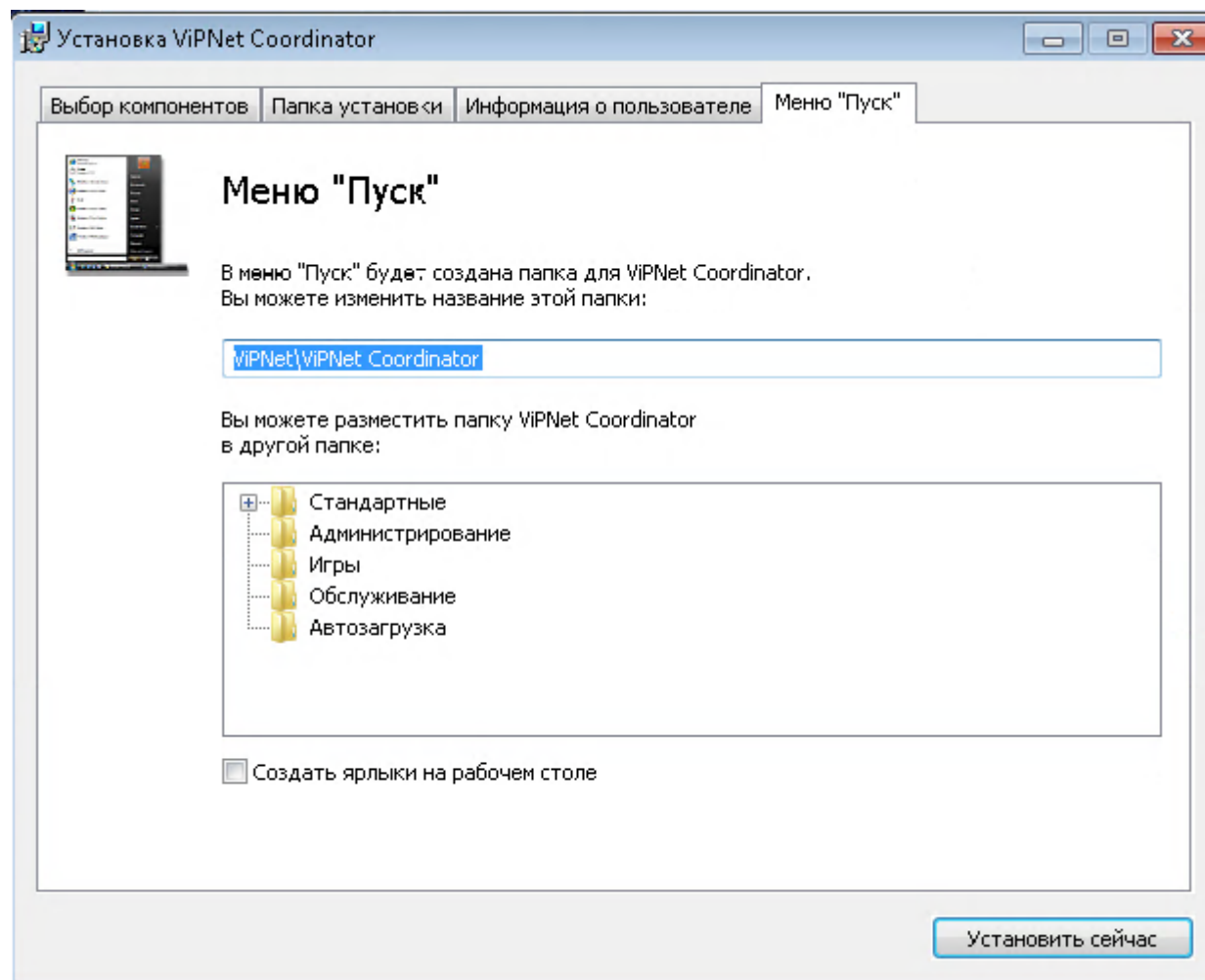
Введите Ваше полное имя и название организации. Эта информация будет использована для регистрации ViPNet Coordinator.

Пользователь:

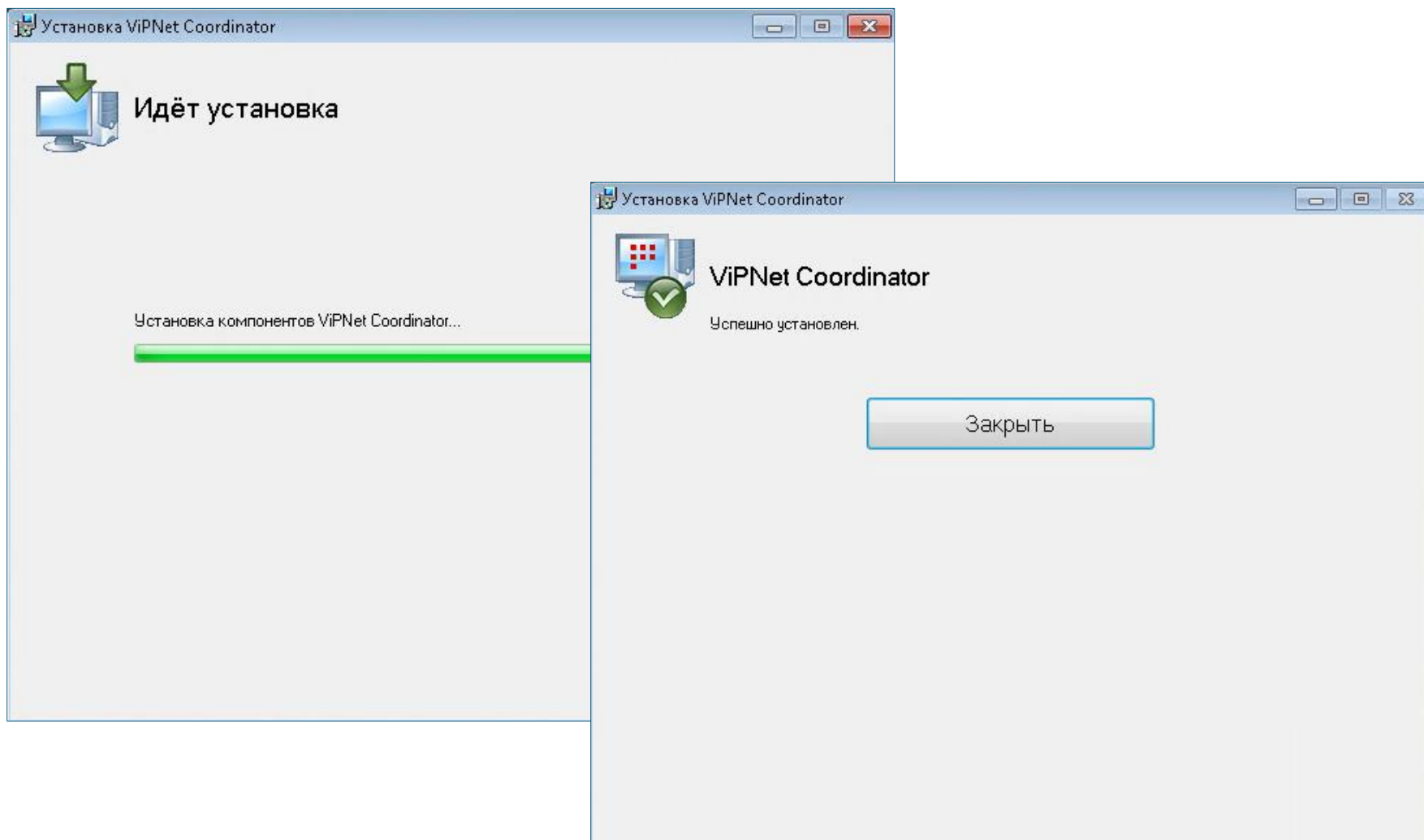
Организация:

Установить сейчас

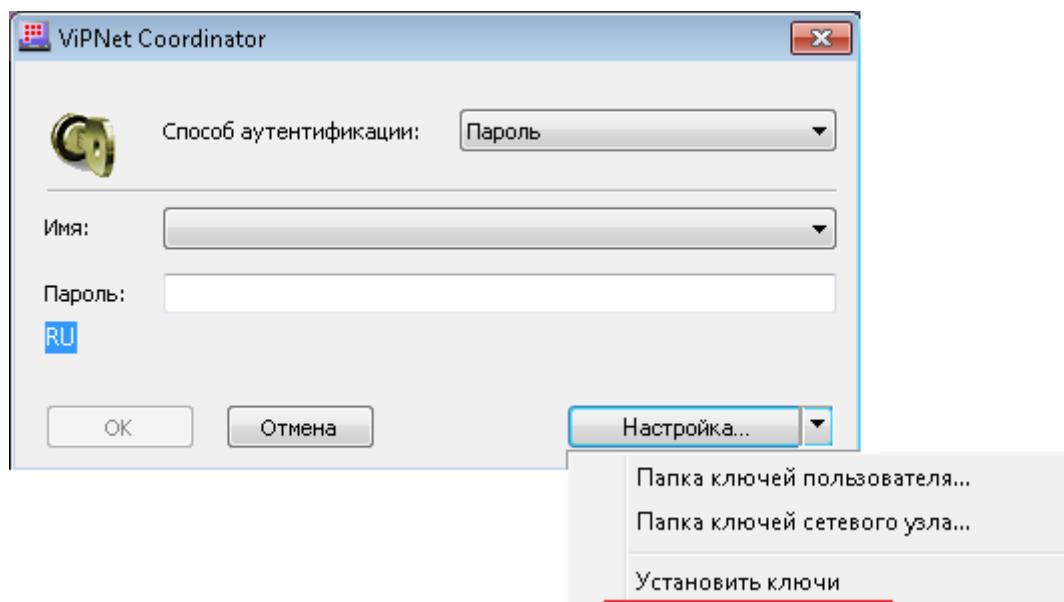
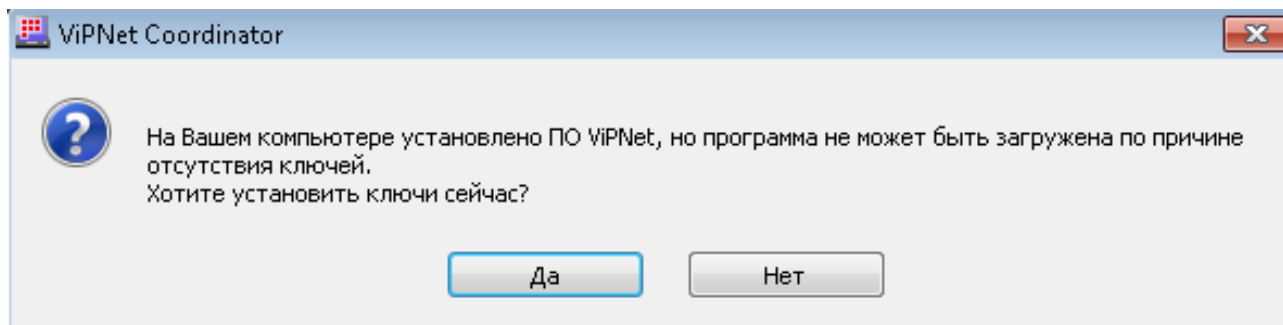
## Дополнительные параметры установки



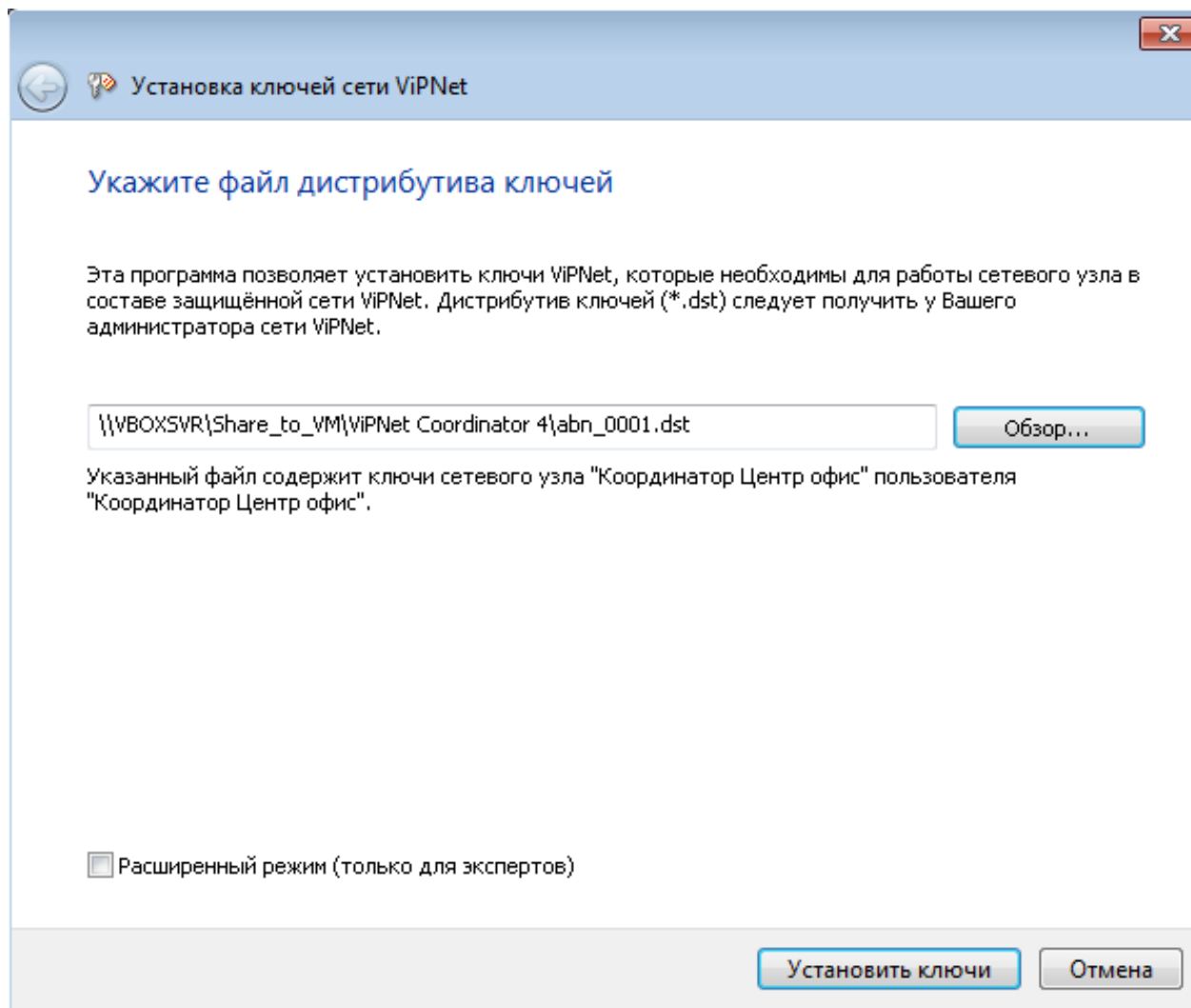
## Установка в интерактивном режиме



## Установка справочников и ключей



## Установка справочников и ключей



Установка ключей сети ViPNet

**Укажите файл дистрибутива ключей**

Эта программа позволяет установить ключи ViPNet, которые необходимы для работы сетевого узла в составе защищённой сети ViPNet. Дистрибутив ключей (\*.dst) следует получить у Вашего администратора сети ViPNet.

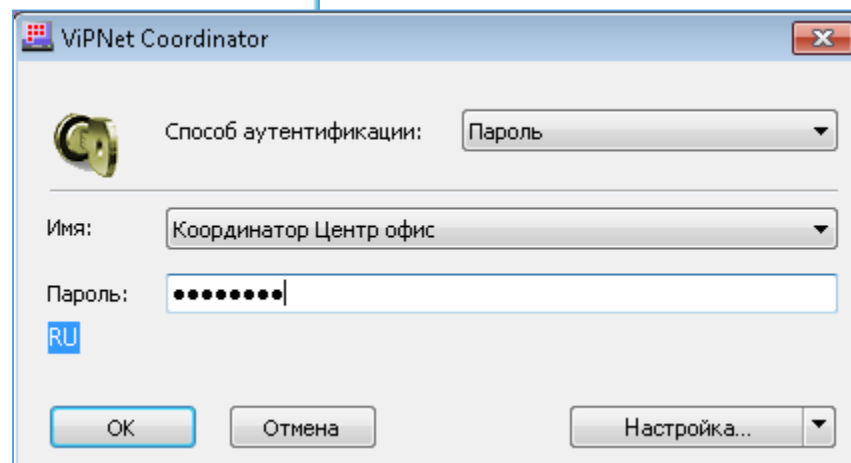
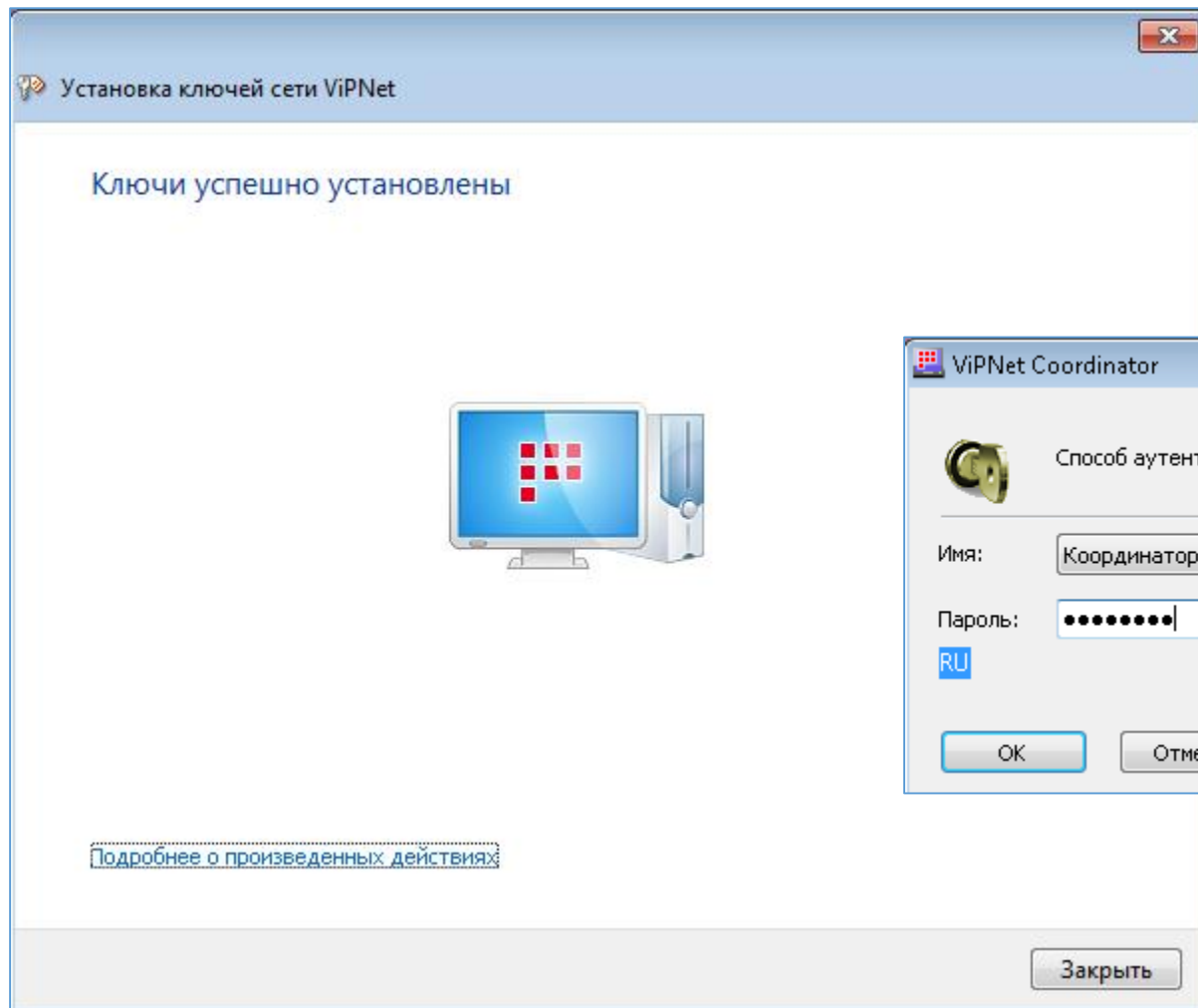
\\VBOXSVR\Share\_to\_VM\ViPNet Coordinator 4\abn\_0001.dst    Обзор...

Указанный файл содержит ключи сетевого узла "Координатор Центр офис" пользователя "Координатор Центр офис".

☐ Расширенный режим (только для экспертов)

Установить ключи    Отмена

## 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

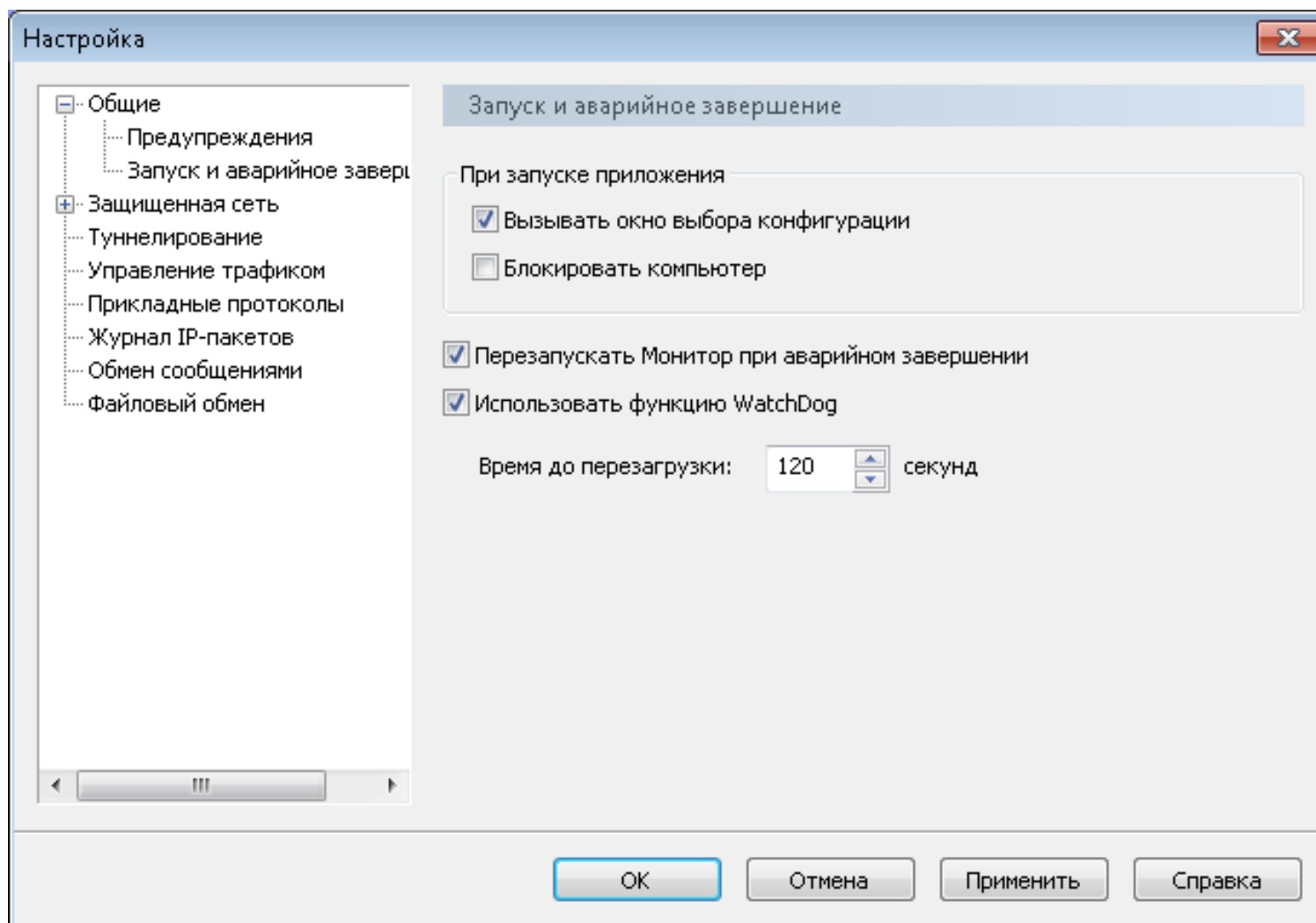


## Пароль на устройстве

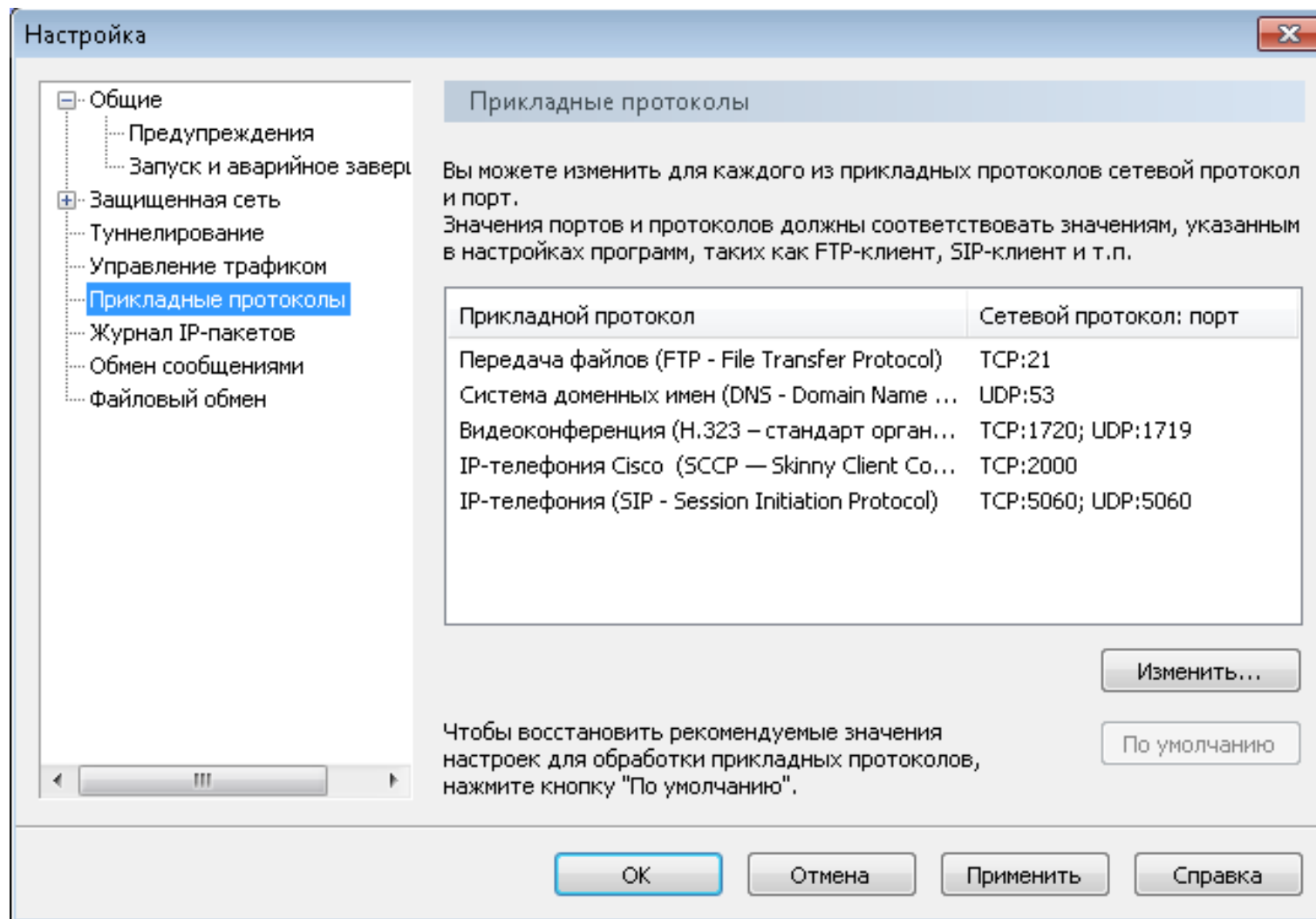
- Для входа в программу нужно подключить устройство и ввести ПИН-код
- Пароль хранится на устройстве
- **Внимание! Способ аутентификации Пароль на устройстве не отвечает требованиям безопасности. Возможность его использования оставлена для совместимости с ПО ViPNet более ранних версий**



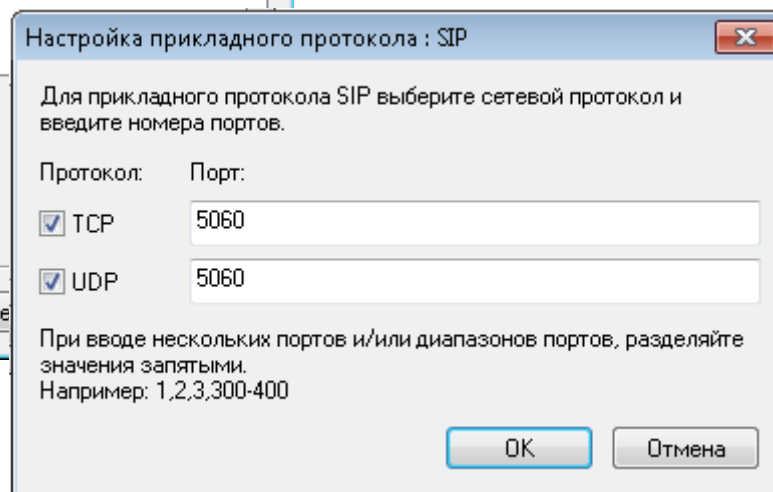
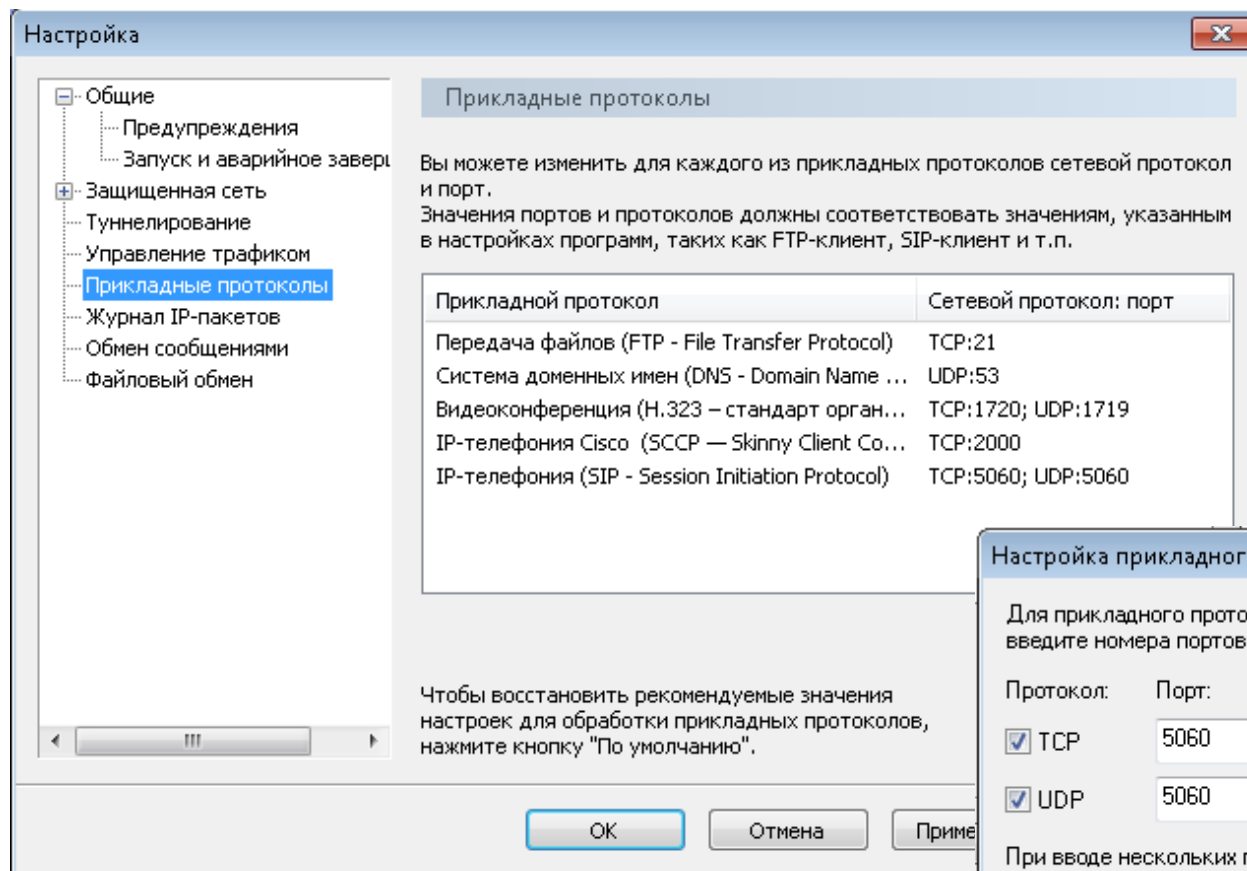
## Общие настройки



## Настройка обработки прикладных протоколов



## Настройка обработки прикладных протоколов

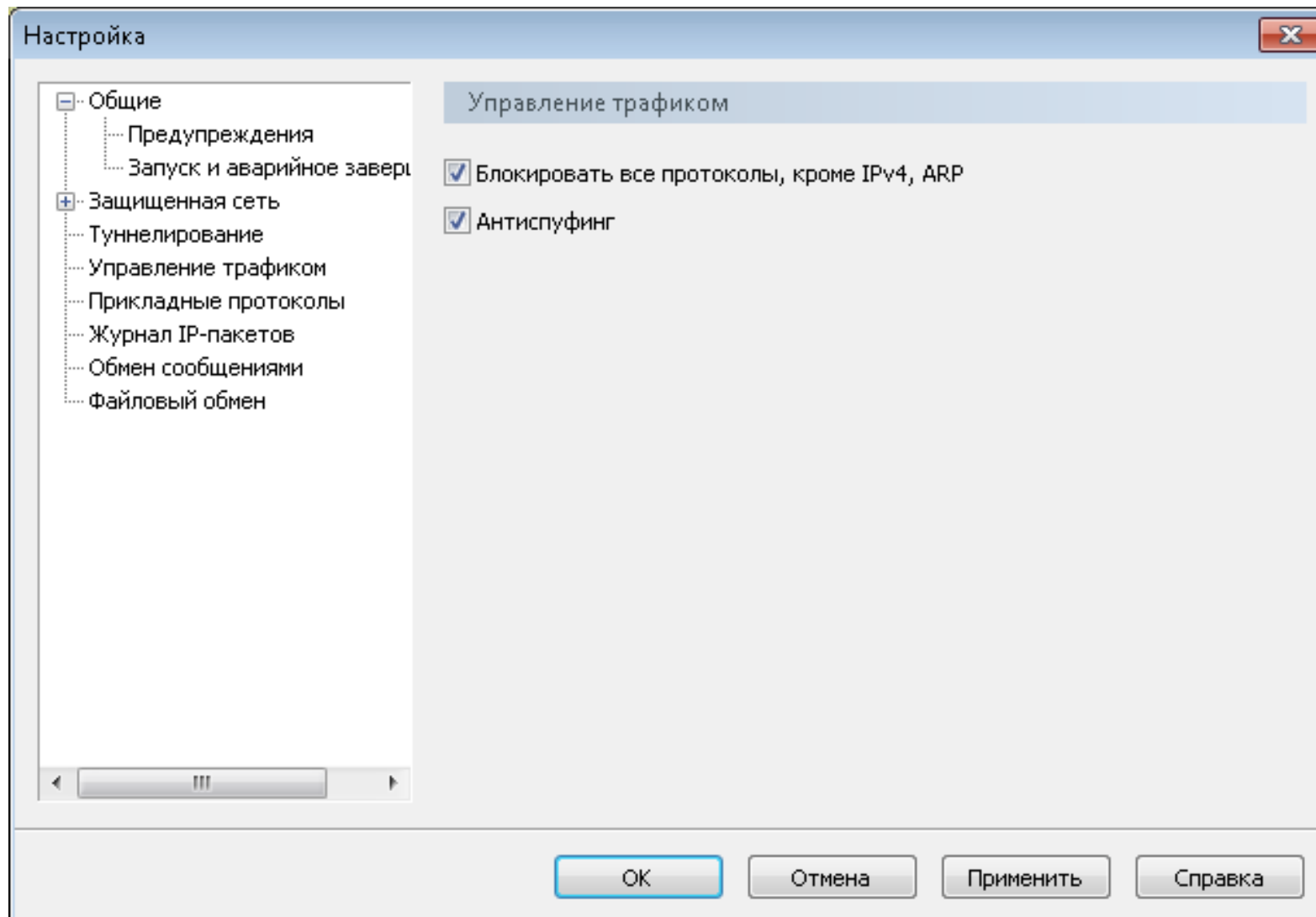


## Антиспуфинг:

- 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



- 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

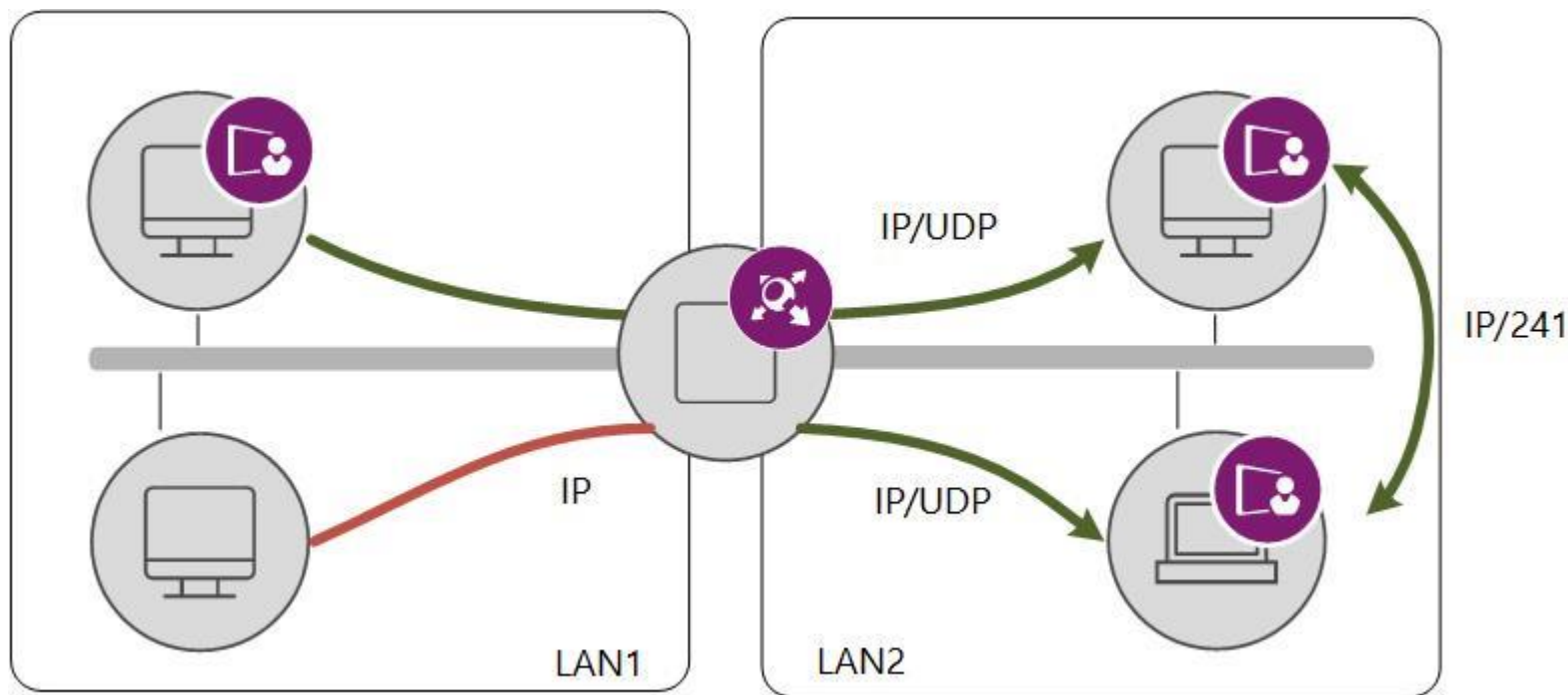


- подключение без использования межсетевого экрана
- подключение через координатор
- подключение через межсетевой экран с динамической трансляцией адресов
- подключение через межсетевой экран со статической трансляцией адресов



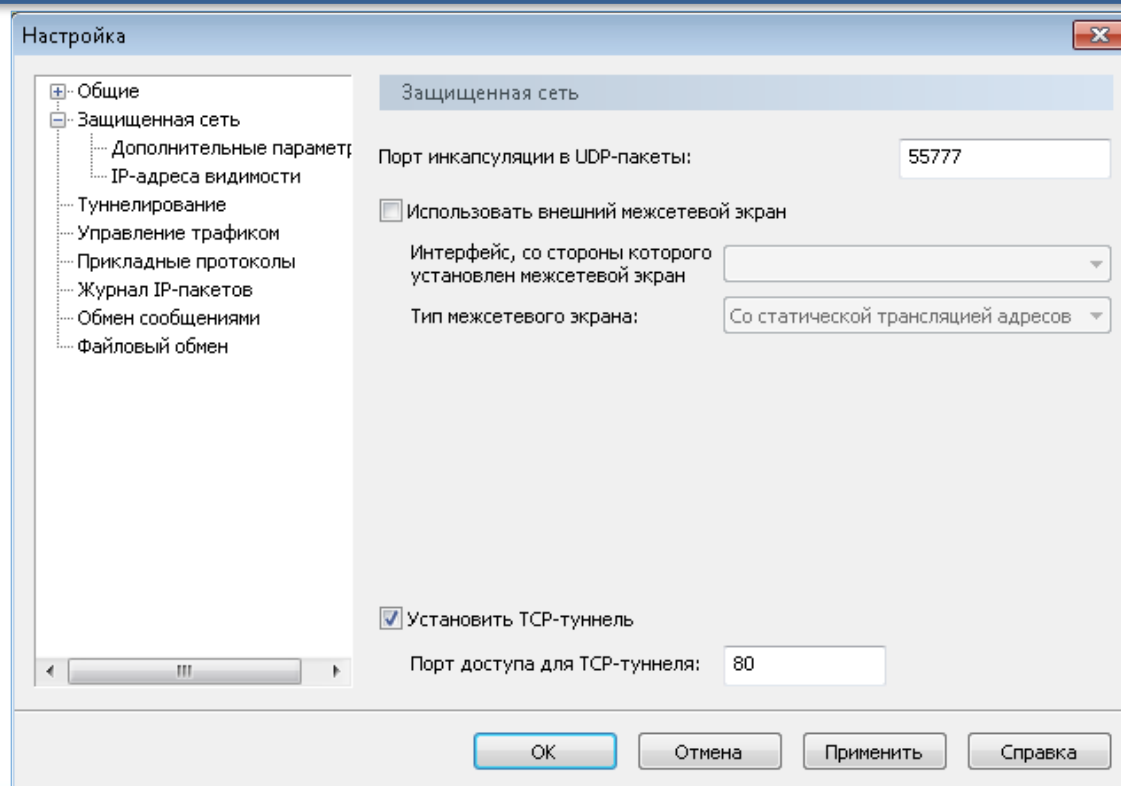
## ■ без использования межсетевого экрана:

- 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;



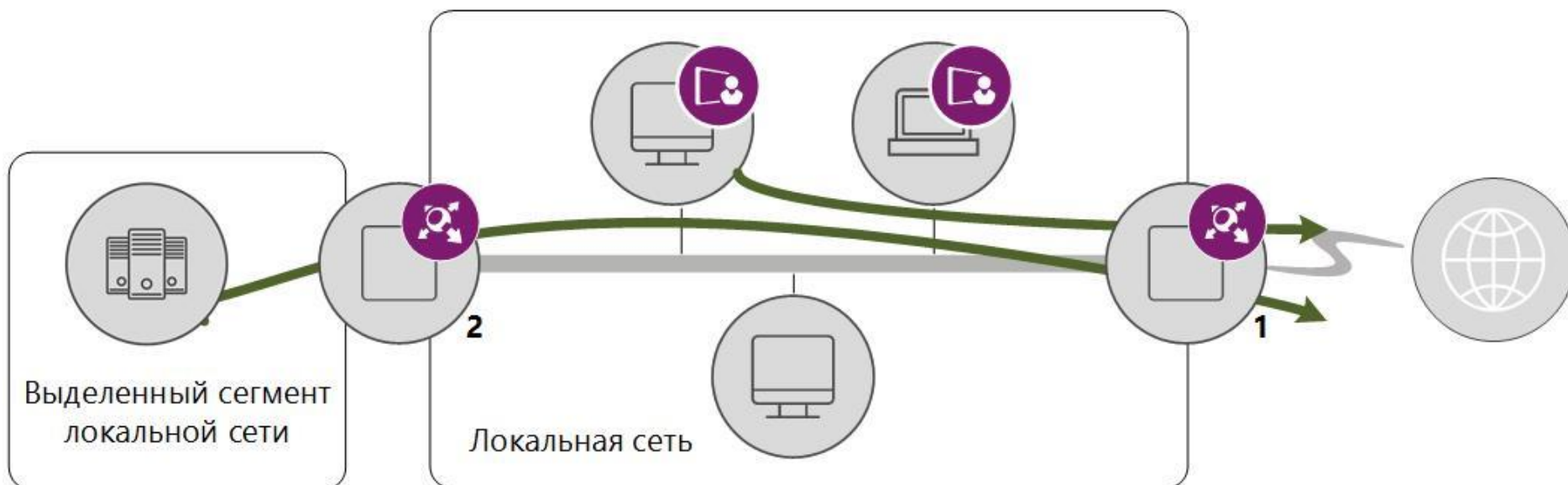
- **без использования межсетевого экрана:**

- 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;



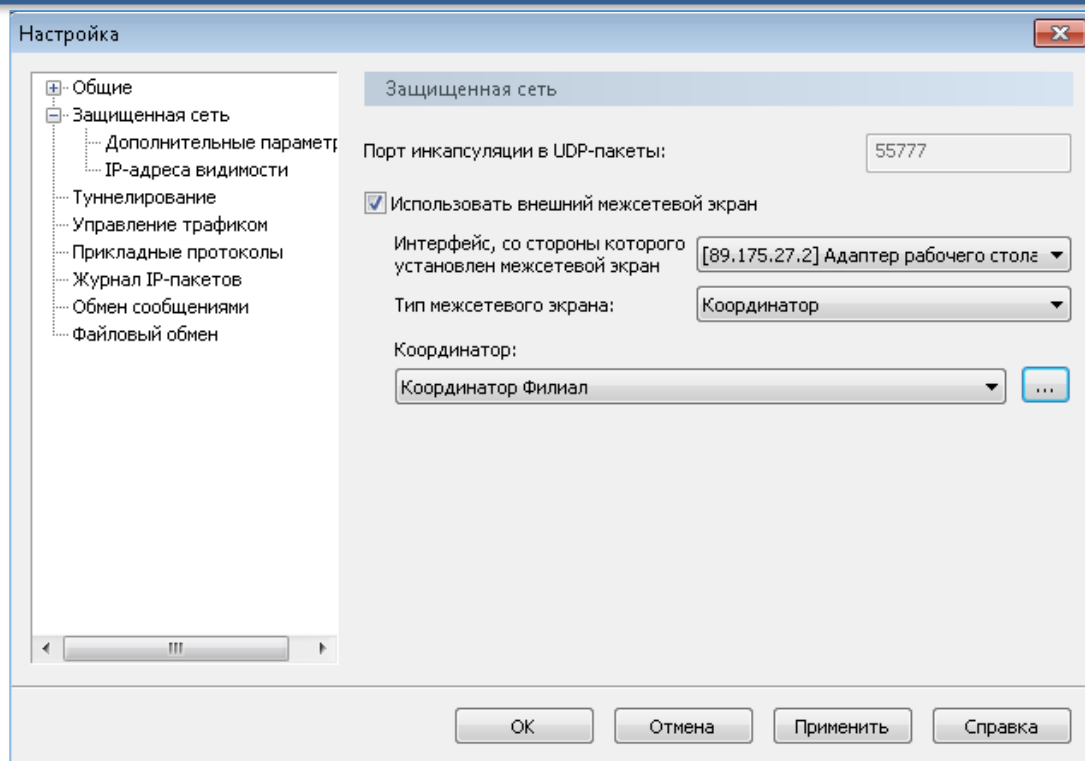
## ■ через координатор:

- 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;



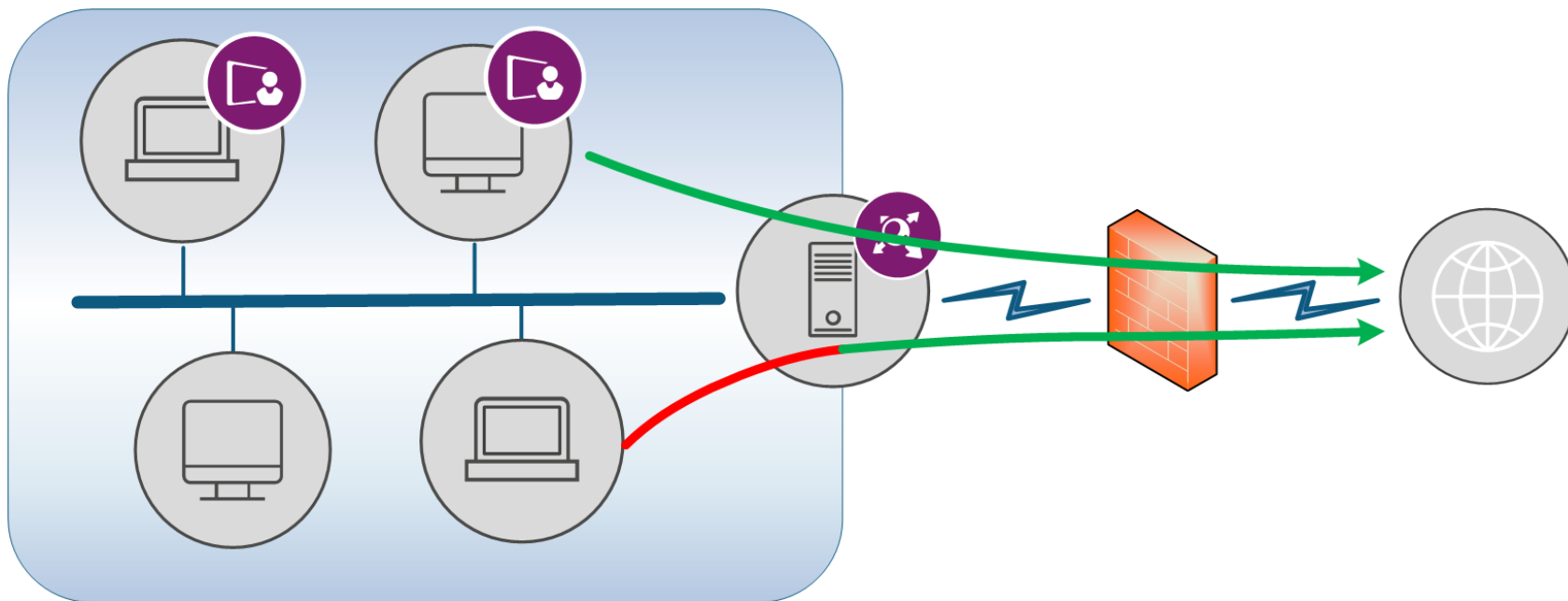
## ■ через координатор:

- 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;

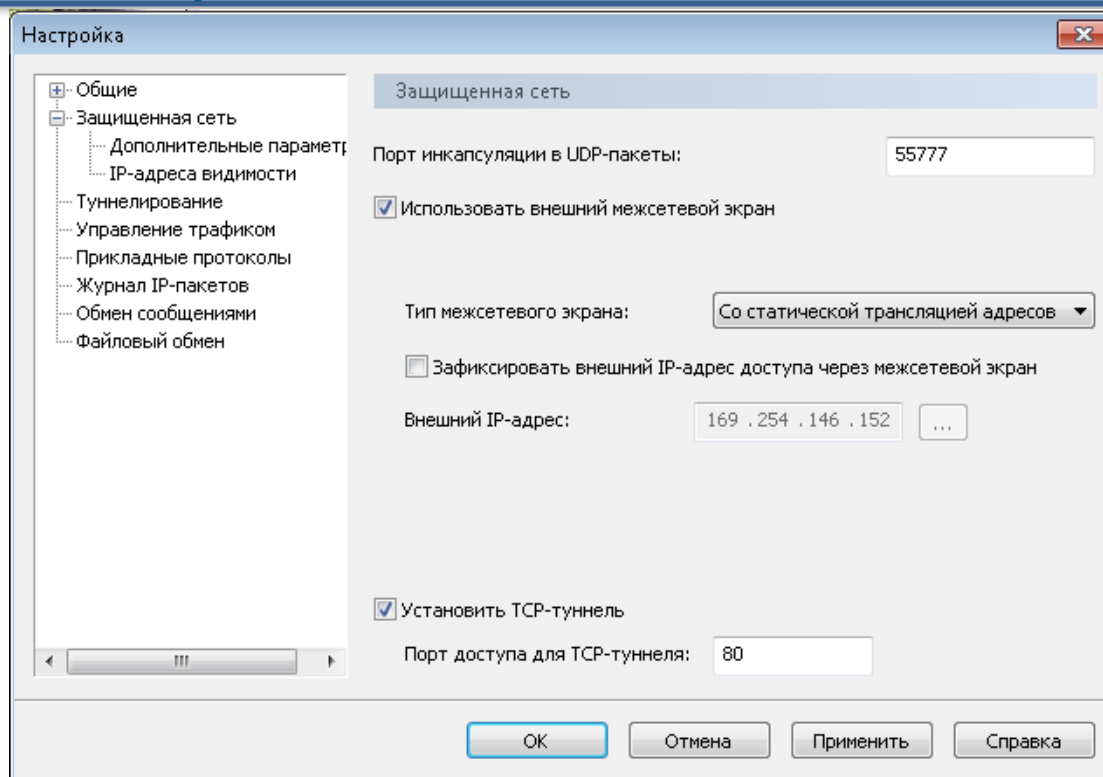


- **через межсетевой экран со статической трансляцией адресов:**

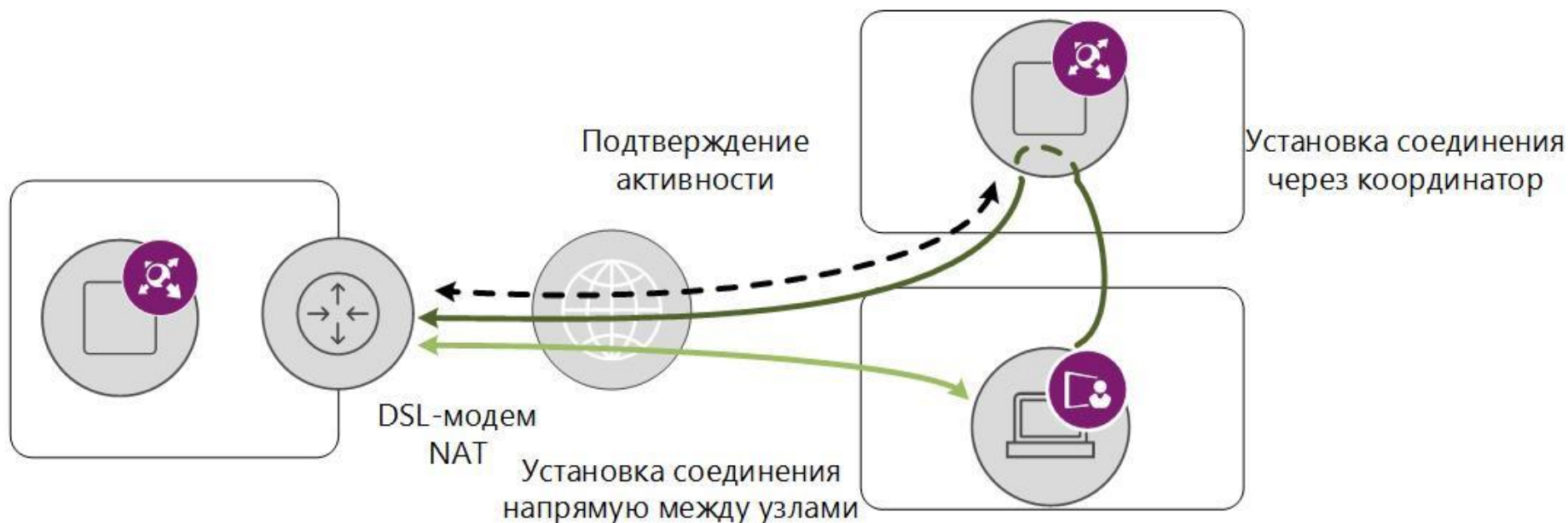
- используется, если соединение с внешней сетью происходит через межсетевой экран, на котором можно настроить статические правила трансляции адресов;
- для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию;



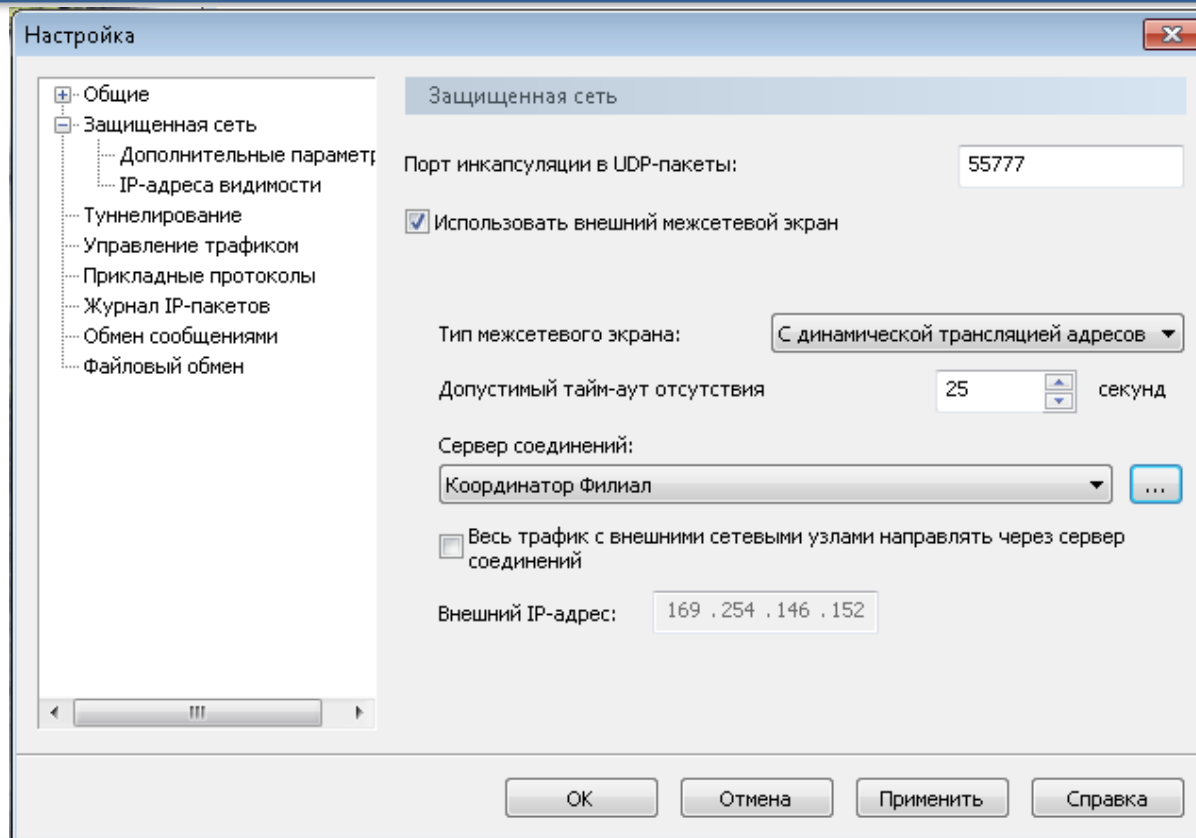
- через межсетевой экран со статической трансляцией адресов:
- используется, если соединение с внешней сетью происходит через межсетевой экран, на котором можно настроить статические правила трансляции адресов;
- для правильной работы адрес межсетевого экрана должен быть указан в качестве шлюза по умолчанию;



- **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.



- **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.

## Виртуальные IP-адреса



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.

## 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;



## 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 доступа к защищенным узлам

Свойства узла (Координатор Филиал)

Общие IP-адреса Межсетевой экран Туннель

**1971000B Координатор Филиал**

Имя компьютера: arm1  
Версия ПО: 4.3(3.51461) RUS  
Версия ОС: Microsoft Windows 7 Ultimate Edition, 64-bit Service Pack 1 (build 7601.win7sp1\_gdr.150202-1526)

Реальные IP-адреса видимости:  
• 89.175.27.5, 192.168.80.3

Виртуальные IP-адреса видимости:  
• 11.0.0.2, 11.1.0.2

Доступен по реальным IP-адресам  
Доступен по Broadcast

Информация о типе межсетевого экрана:  
• IP-адреса доступа через межсетевого экран: 89.175.27.5 [2,2]  
• Порт UDP: 55777  
• Тип межсетевого экрана:  
• Со статической трансляцией адресов

Текущая точка доступа:  
• 1971000B Координатор Филиал  
• 89.175.27.5: 55777  
• Установлено прямое соединение с данным узлом

Туннели (доступны по реальным IP-адресам):  
192.168.80.4-192.168.80.20 (12.0.0.1-12.0.0.17)

Псевдоним:

OK Отмена Применить Справка

Свойства узла (Координатор Филиал)

Общие IP-адреса Межсетевой экран Туннель

IP-адреса:

Реальные IP-адреса	Виртуальные IP-адреса
89.175.27.5	11.0.0.2
192.168.80.3	11.1.0.2
10.2.0.30	11.1.0.3
212.134.1.5	11.1.0.4

Введите IP-адрес для поиска

☒ ☐ ☐ Добавить... Изменить... Удалить

IP-адреса видимости узла:

☒ Использовать DNS-имя:

DNS-имя

db.company.ru

Введите DNS-имя для поиска

☒ ☐ ☐ Добавить... Изменить... Удалить

OK Отмена Применить Справка

## Настройка доступа к защищенным узлам

The image displays three overlapping screenshots of the ViPNet Coordinator software interface, specifically the 'Свойства узла (Координатор Филиал)' (Node Properties - Branch Coordinator) dialog box.

**Leftmost screenshot (General tab):** Shows the 'Общие' (General) tab. It displays the node name '1971000В Координатор Филиал' and various system information including the computer name 'arm1', OS version 'Microsoft Windows 7 Ultimate', and IP address visibility settings. It lists real IP addresses (89.175.27.5, 192.168.80.3) and virtual IP addresses (11.0.0.2, 11.1.0.2). It also shows the current access point and tunnel status.

**Middle screenshot (IP Address tab):** Shows the 'IP-адреса' (IP Addresses) tab. It displays a table of IP addresses:

Реальные IP-адреса	Виртуальные IP-адреса
89.175.27.5	11.0.0.2
192.168.80.3	11.1.0.2
10.2.0.30	11.1.0.3
212.134.1.5	11.1.0.4

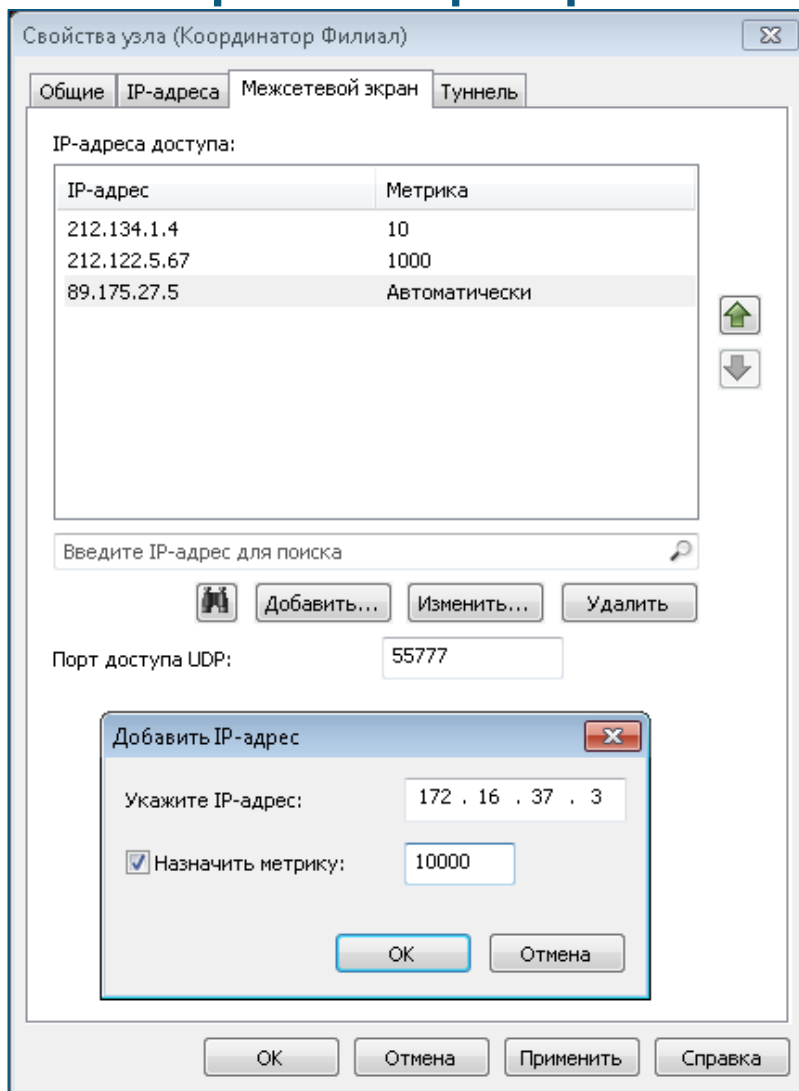
Below the table, there is a search field for IP addresses and buttons for 'Добавить...' (Add...), 'Изменить...' (Edit...), and 'Удалить' (Delete). The 'IP-адреса видимости узла' (Node visibility IP addresses) are set to 'Автоматически' (Automatic).

**Rightmost screenshot (Access tab):** Shows the 'IP-адреса доступа' (Access IP addresses) tab. It displays a table of access IP addresses:

IP-адрес	Метрика
212.134.1.4	10
212.122.5.67	1000
89.175.27.5	Автоматически

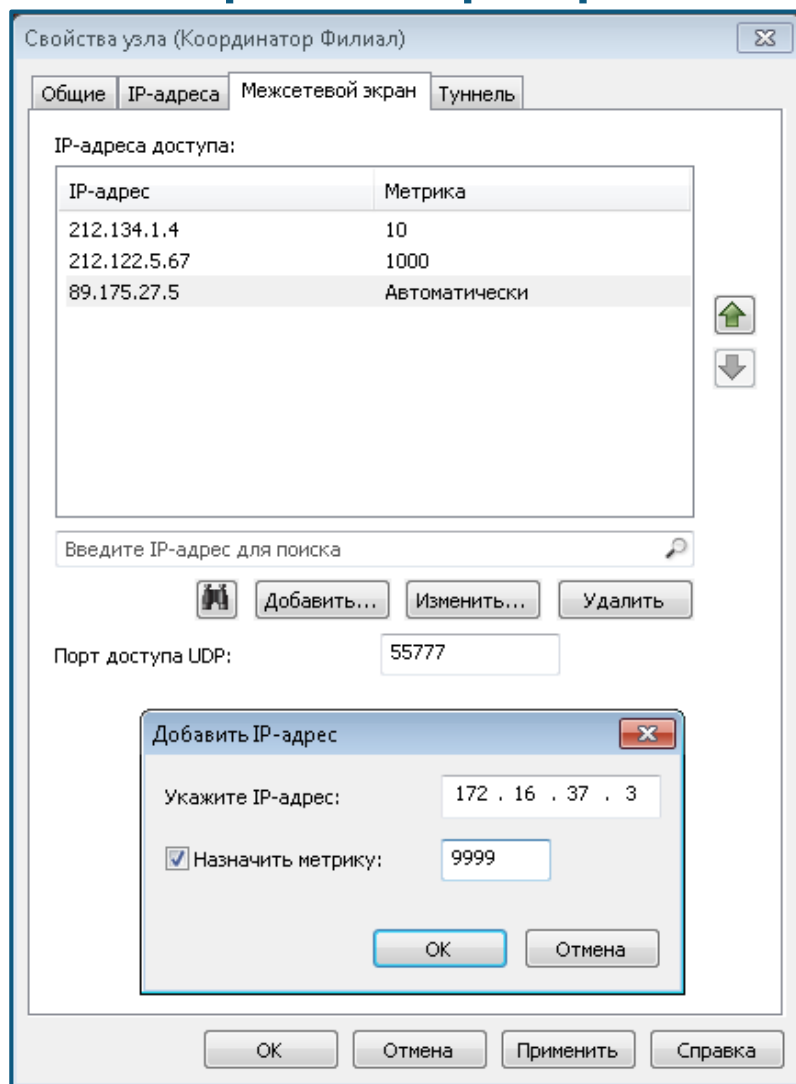
Below the table, there is a search field for IP addresses and buttons for 'Добавить...' (Add...), 'Изменить...' (Edit...), and 'Удалить' (Delete). The 'Порт доступа UDP' (UDP access port) is set to 55777.

## 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;

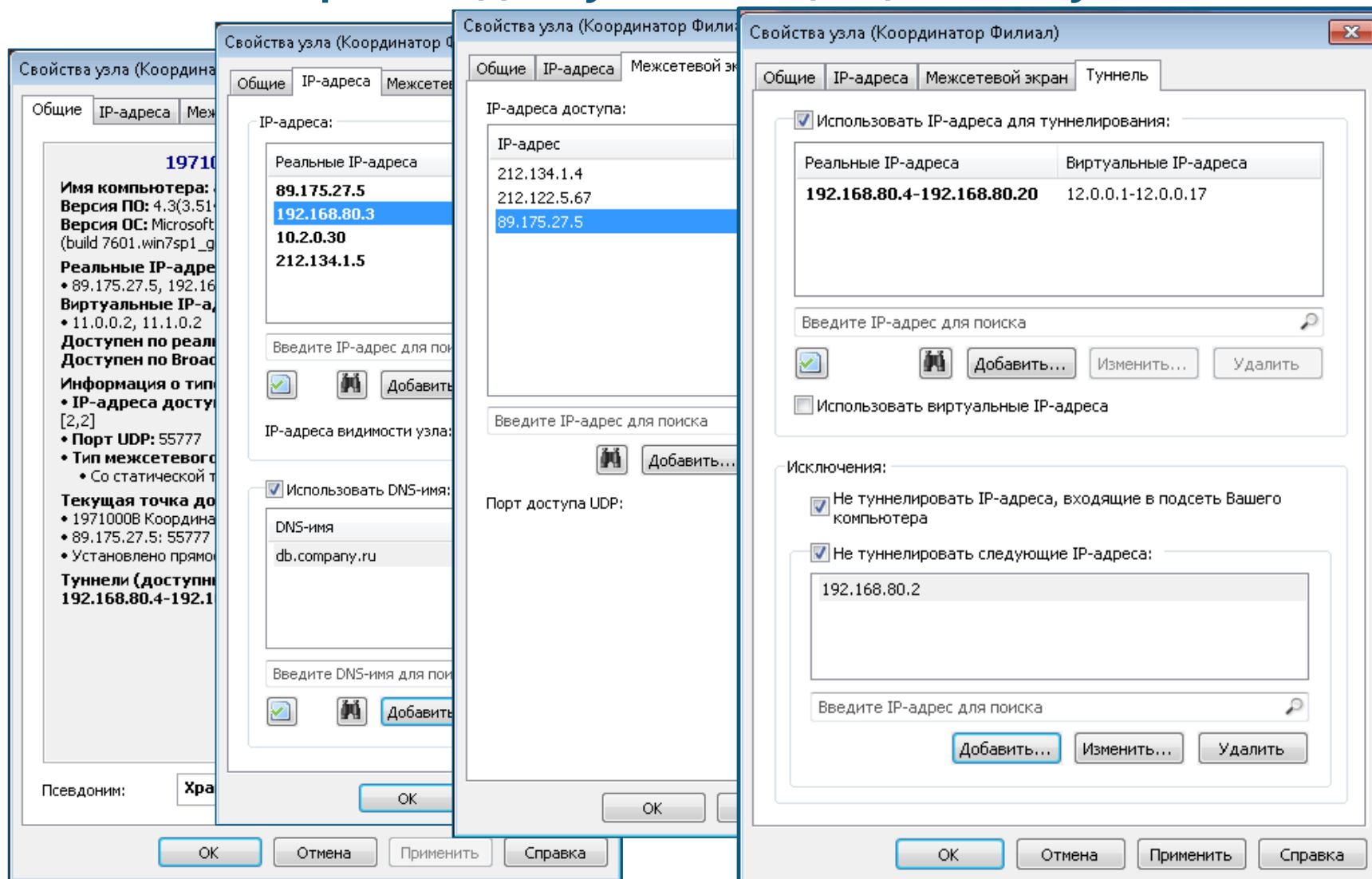
## Настройка приоритета IP-адресов доступа (метрики):



- 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 доступа к защищенным узлам



## 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;



## Туннелирование IP-трафика

Туннелирование предполагает защиту трафика по следующим правилам:

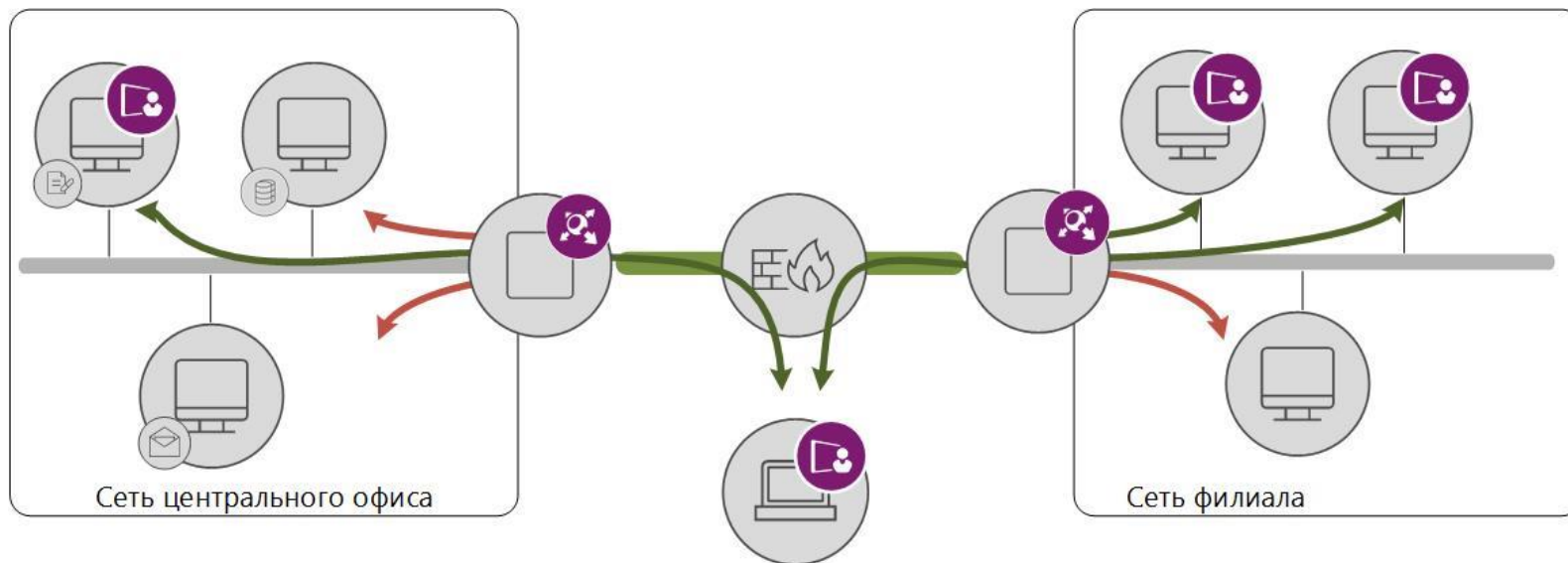
- от открытого узла до туннелирующего координатора трафик передается в открытом виде;
- на координаторе трафик подвергается фильтрации и шифрованию, после чего передается дальше в зашифрованном виде;
- на координаторе, туннелирующем узел получателя, трафик расшифровывается и передается на узел в открытом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



## Туннелирование IP-трафика

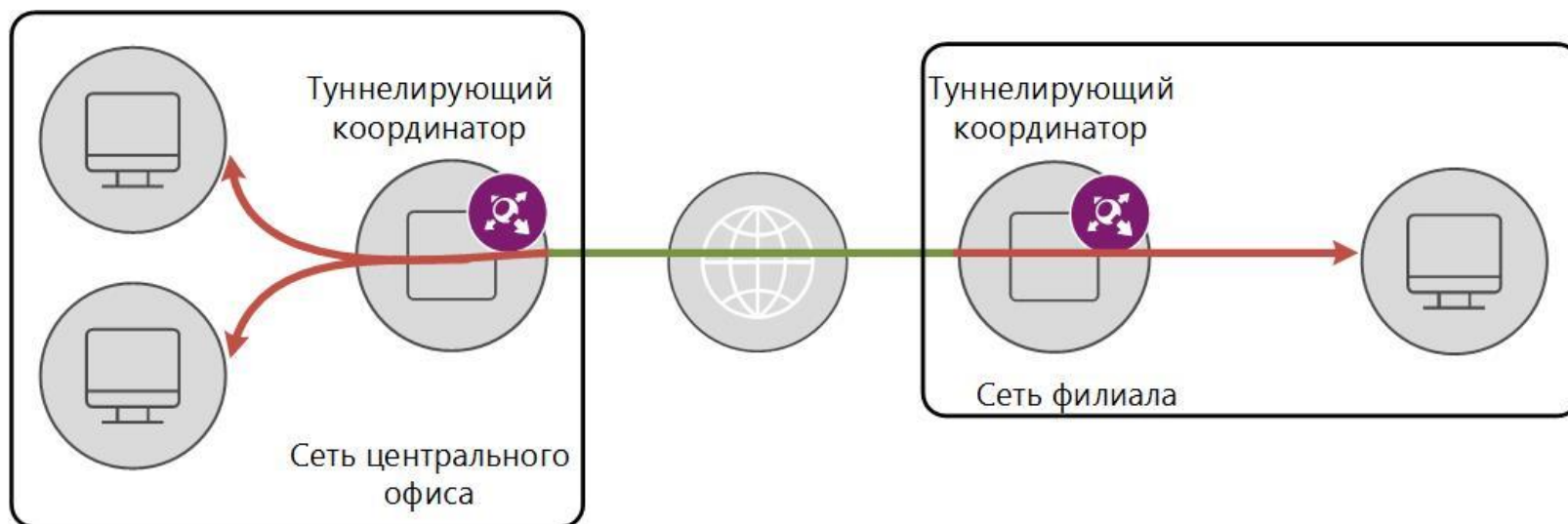
Туннелирующий координатор – координатор, за которым находится открытый узел и который с помощью туннелирования защищает трафик открытого узла.

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



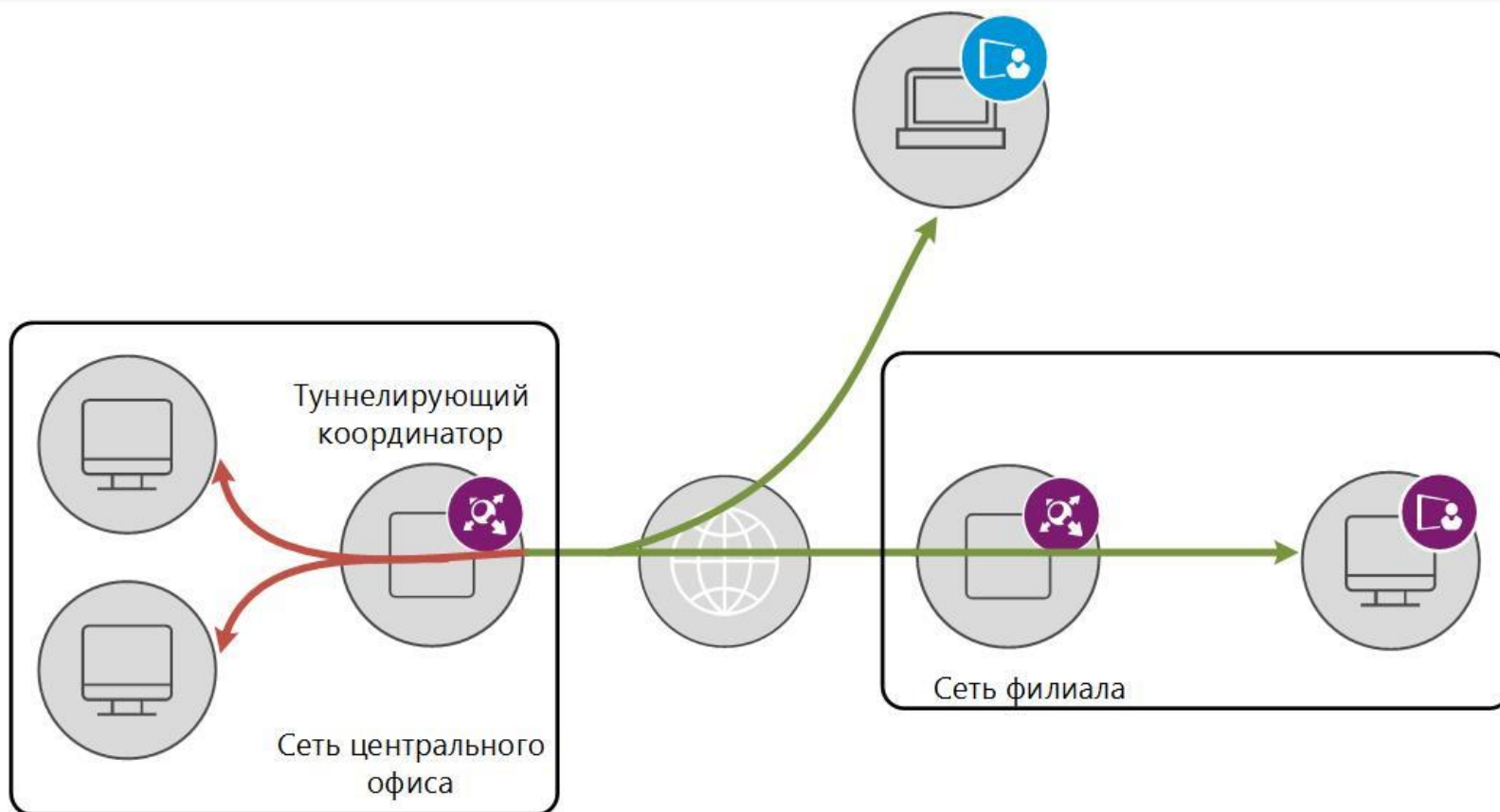
## Туннелирование IP-трафика

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



## 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.



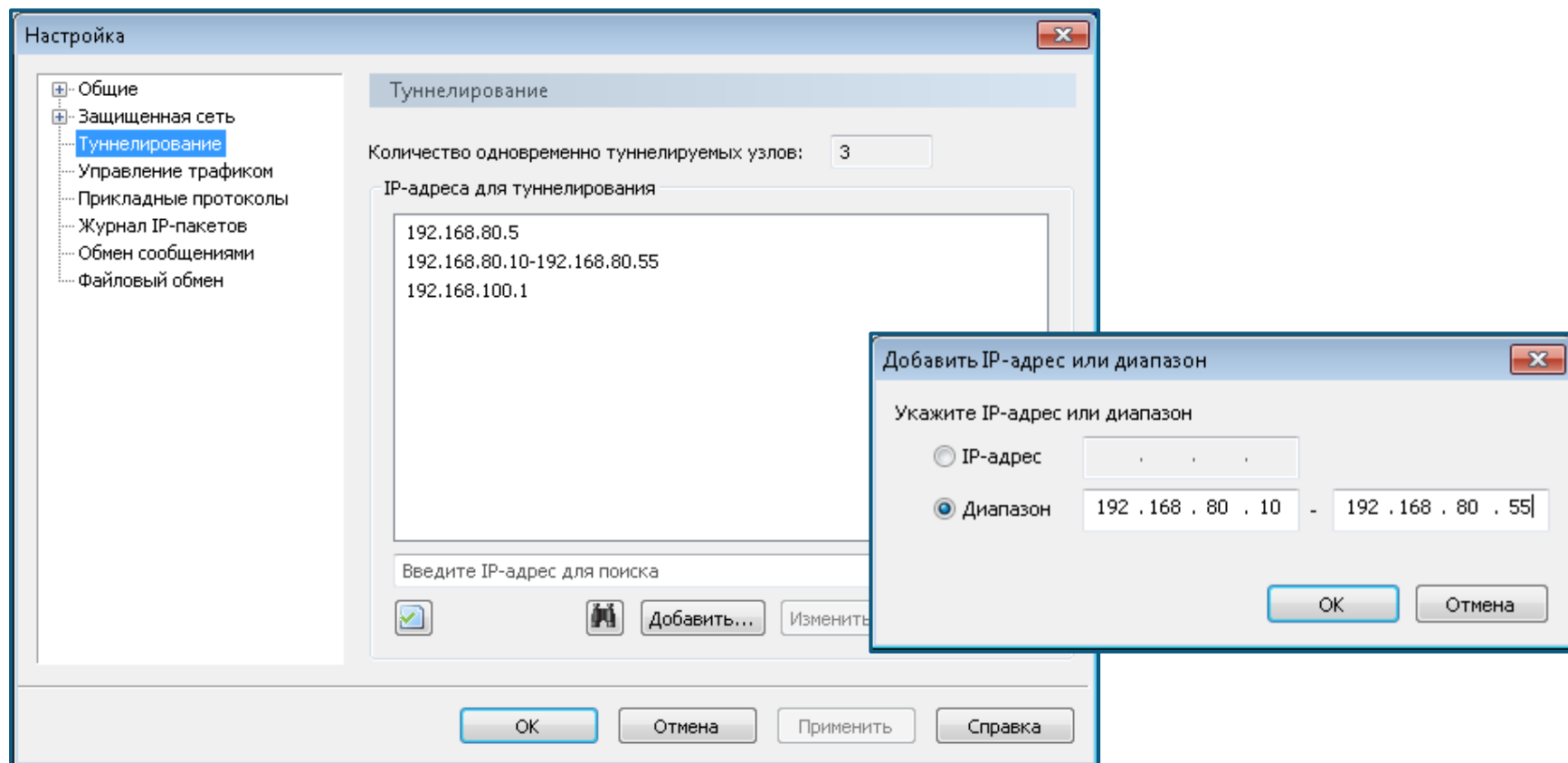
## Способы задания узлов для туннелирования

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.

## Задание узлов для туннелирования



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



## 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.



## 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.

## Виды групп объектов

### Пользовательские:

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



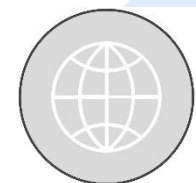
# Настройка сетевого экрана

## 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

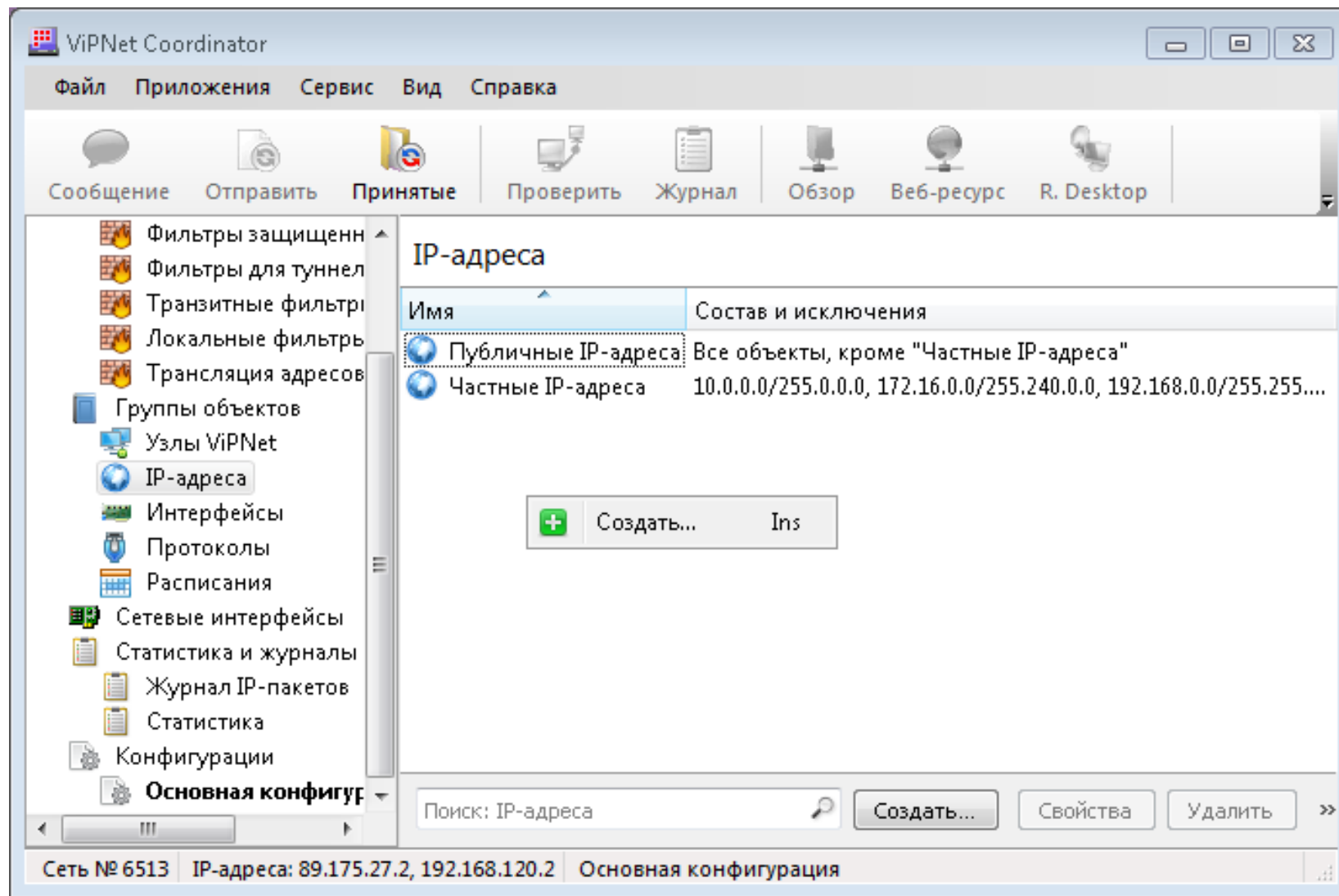
- любая комбинация условий применения сетевых фильтров по времени и дням недели. Используется во всех фильтрах.



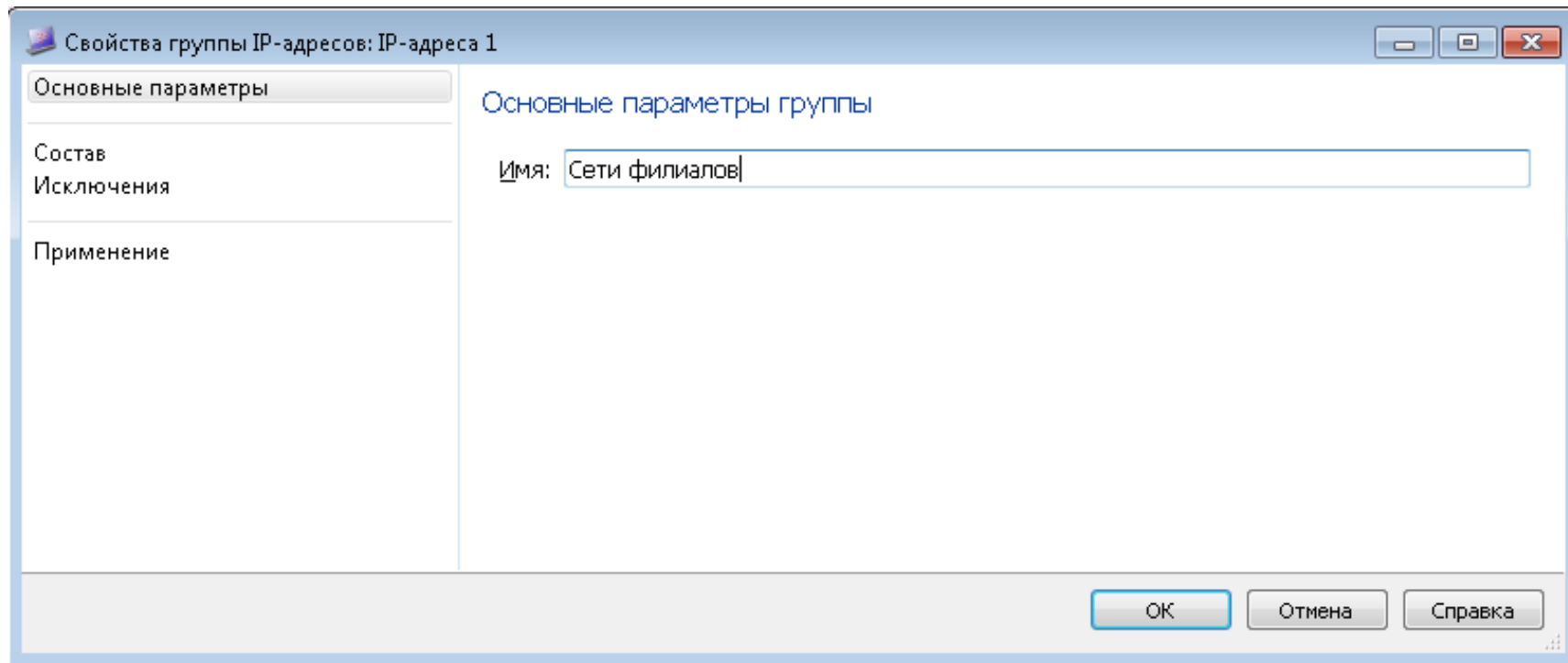
### Интерфейсы

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

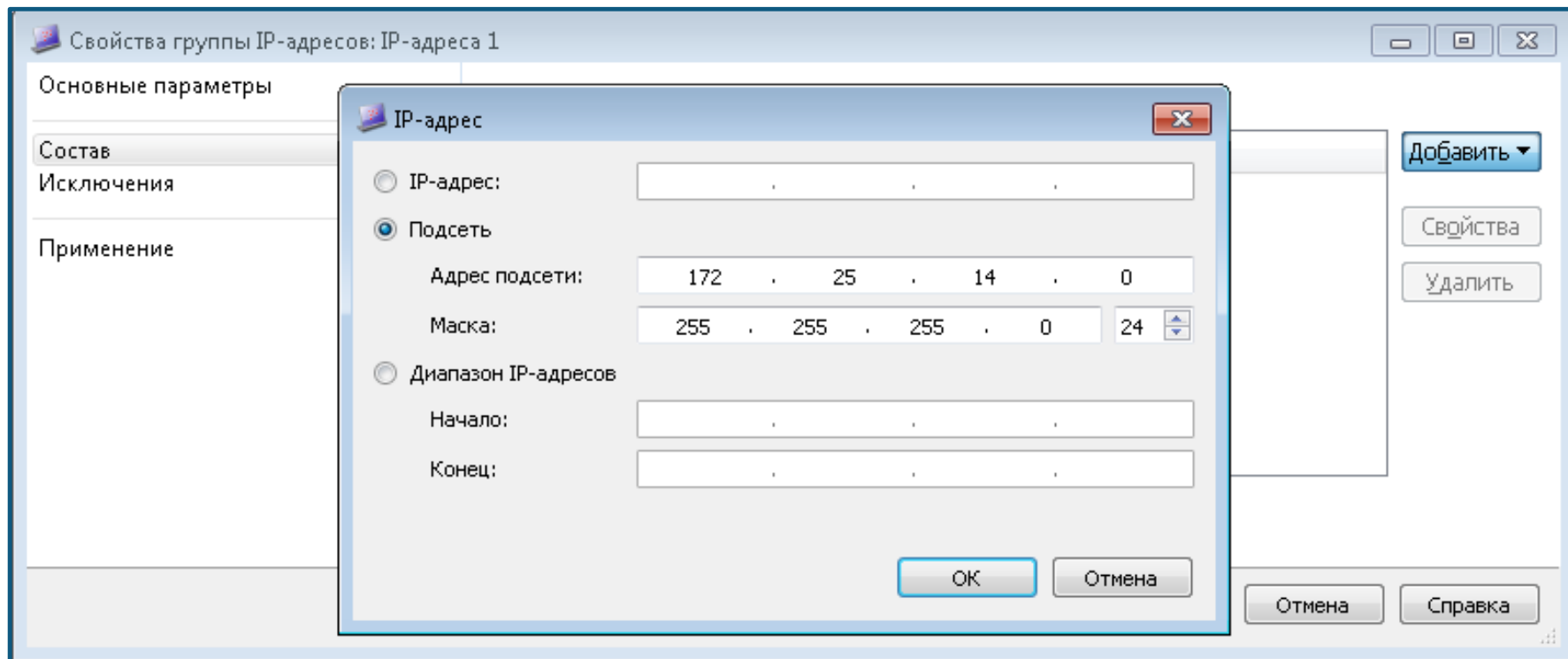
## Создание группы объектов



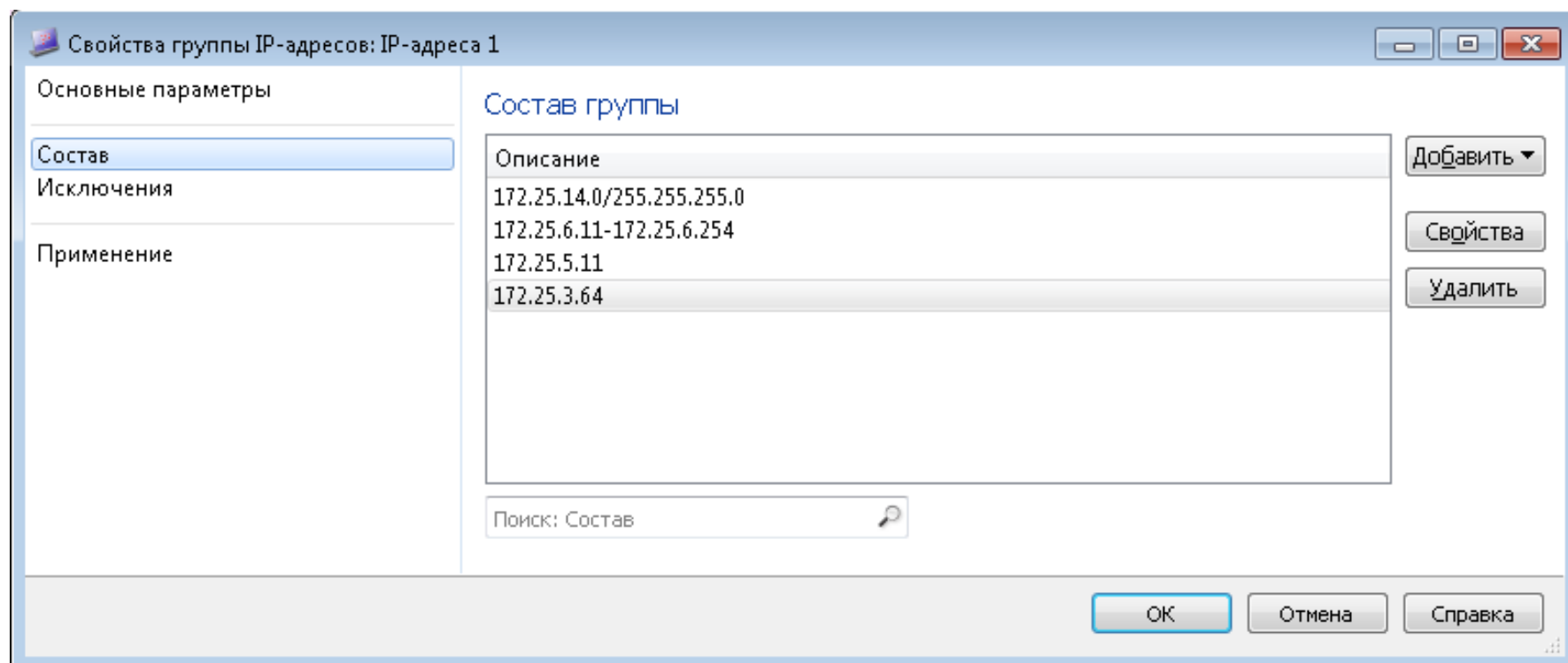
## Создание группы объектов



## Создание группы объектов

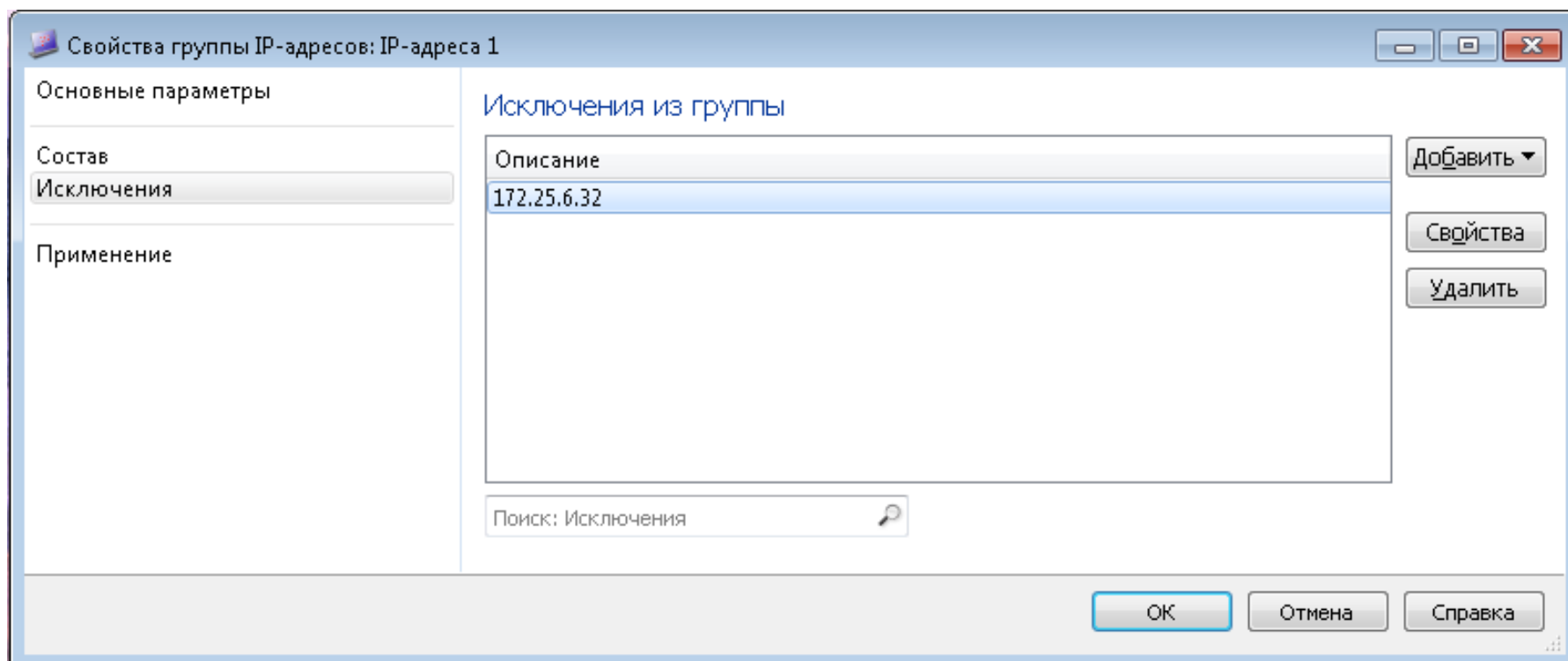


## Создание группы объектов

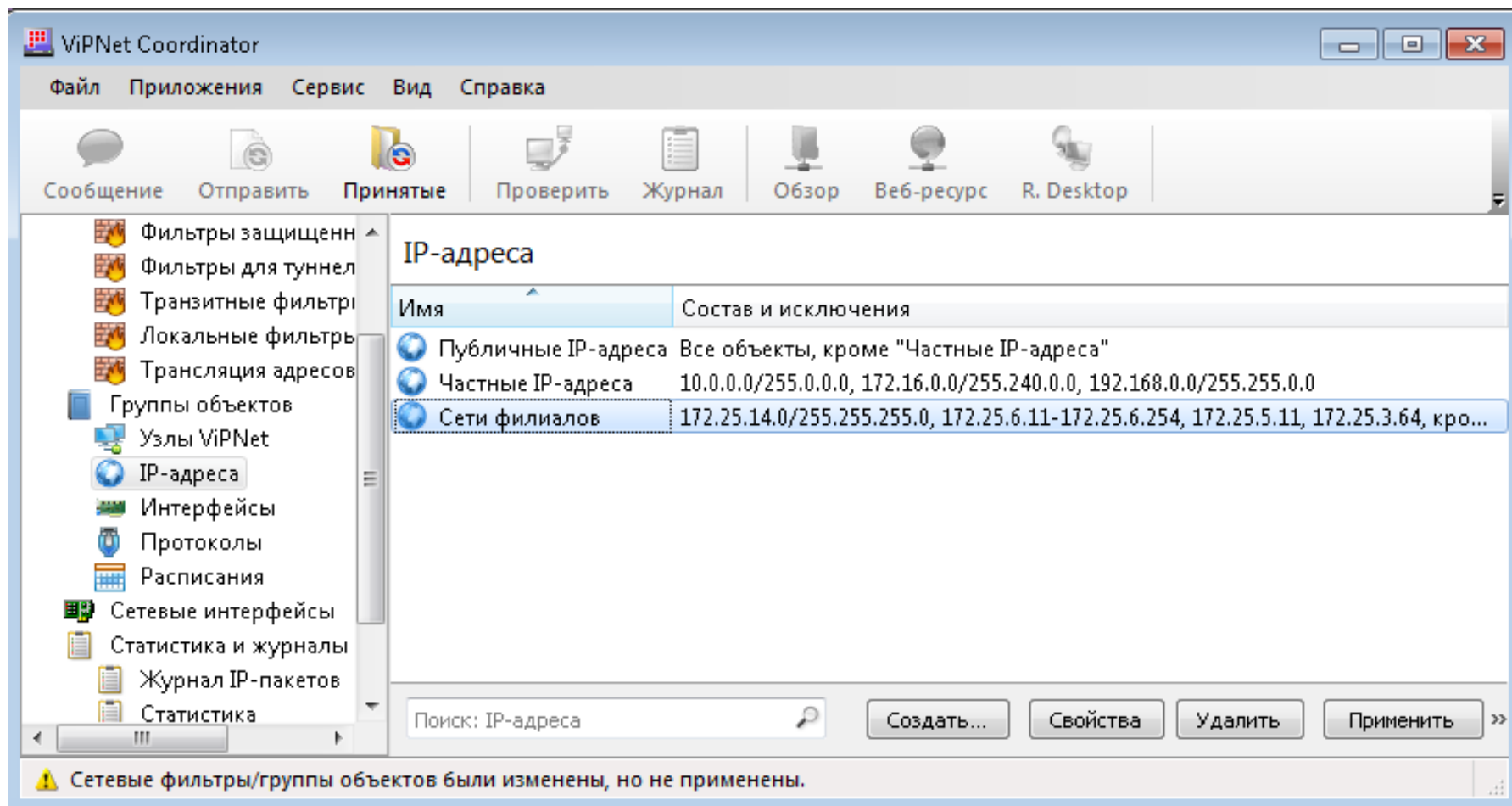




## Создание группы объектов

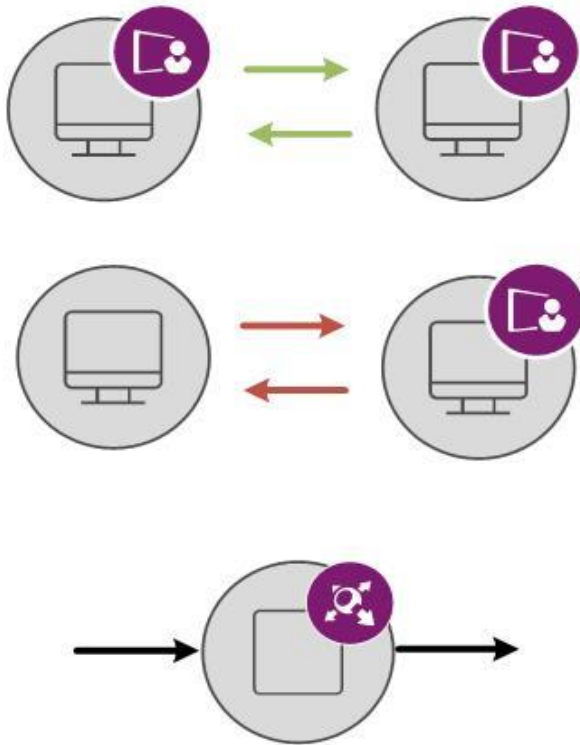


## Создание группы объектов



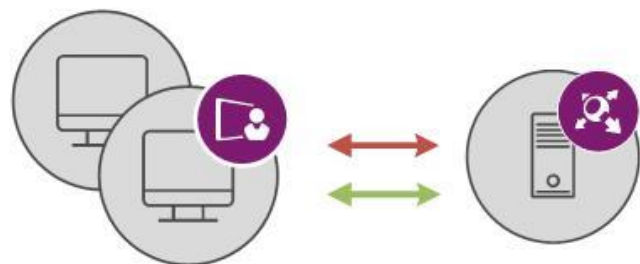
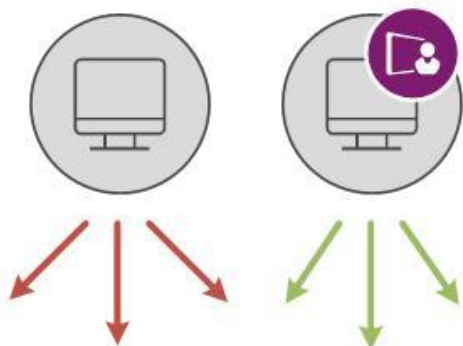
## Фильтрация трафика

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).

## 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.

## 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.

## 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						
<input checked="" type="checkbox"/>	✓ Разрешить	DHCP-тра...	Все	Все	DHCP	Все
<input checked="" type="checkbox"/>	✓ Разрешить	NetBIOS- и...	Все	Все	NetBIOS-DGM	Все
<input checked="" type="checkbox"/>	✓ Разрешить	IGMP-траф...	Все	Все	IGMP	Все
<input checked="" type="checkbox"/>	✓ Разрешить	PING	Все	Все	PING	Все
Фильтры по умолчанию						
<input checked="" type="checkbox"/>	✗ Блокировать	Прочий тр...	Все	Все	Все	Все

Транзитные фильтры открытой сети						
Вкл.	Действие	Имя	Источник	Назначение	Протокол	Расписание
Настраиваемые фильтры						
Фильтры по умолчанию						
<input checked="" type="checkbox"/>	✗ Блокировать	Прочий тр...	Все	Все	Все	Все

## 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						
<input checked="" type="checkbox"/>	 Разрешить	Трафик от ...	Все	Туннелируемые IP-адреса	Все	Все
<input checked="" type="checkbox"/>	 Разрешить	Трафик от ...	Туннелируемые IP-адреса	Все	Все	Все
Фильтры по умолчанию						
<input checked="" type="checkbox"/>	 Блокировать	 Прочий тр...	Все	Все	Все	Все

## 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**

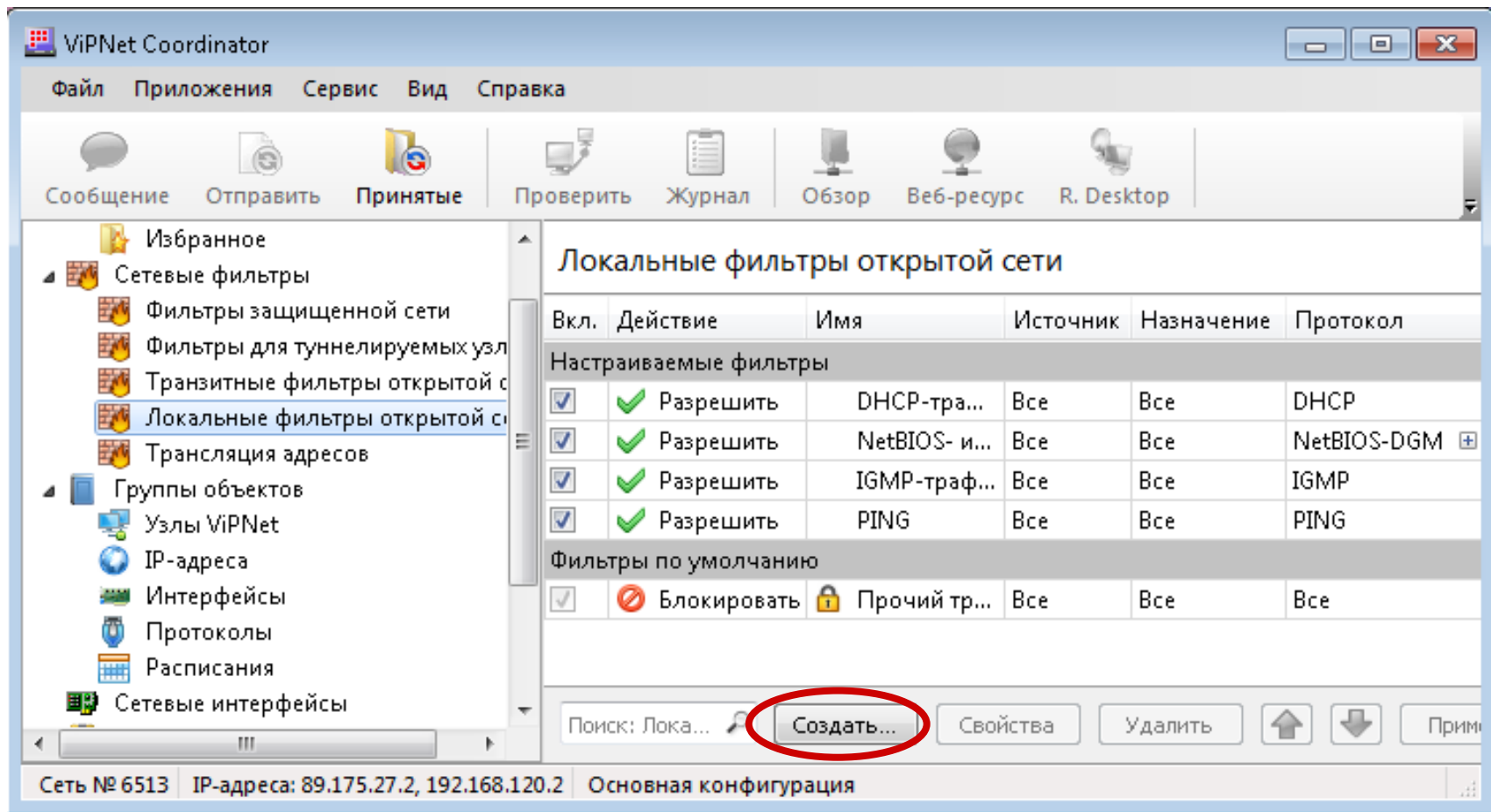
### Фильтры, настроенные по умолчанию:

- недоступны для редактирования;
- создаются программой автоматически.

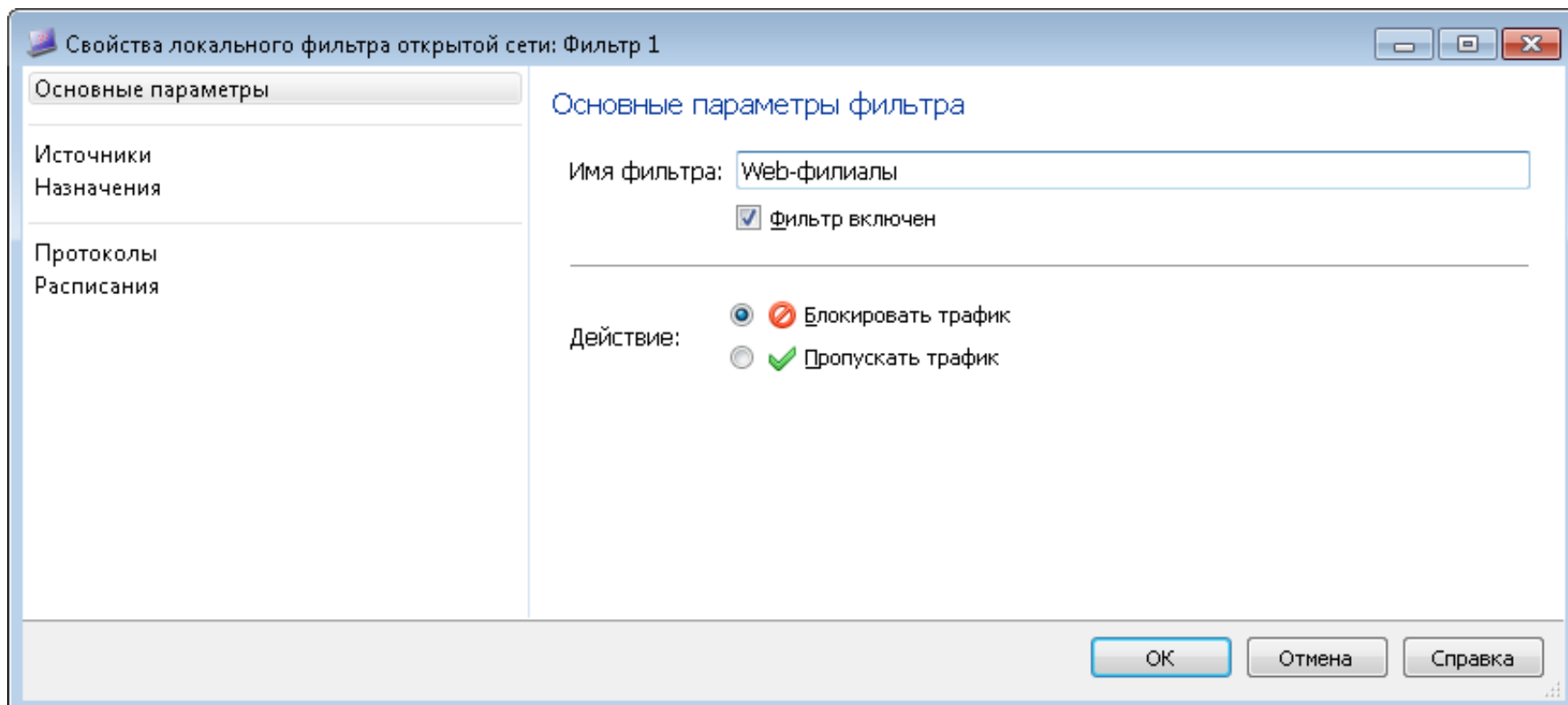
**4**



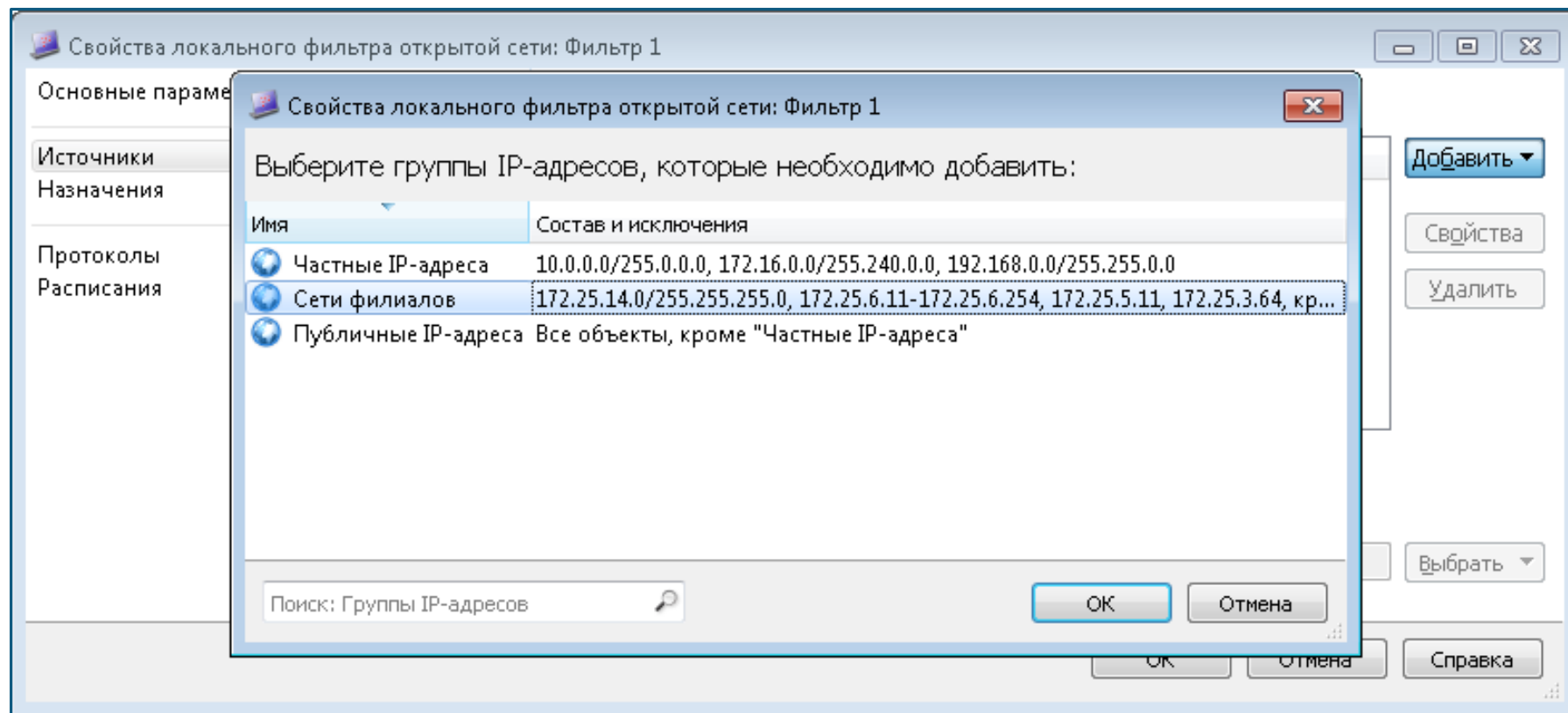
## Создание сетевого фильтра



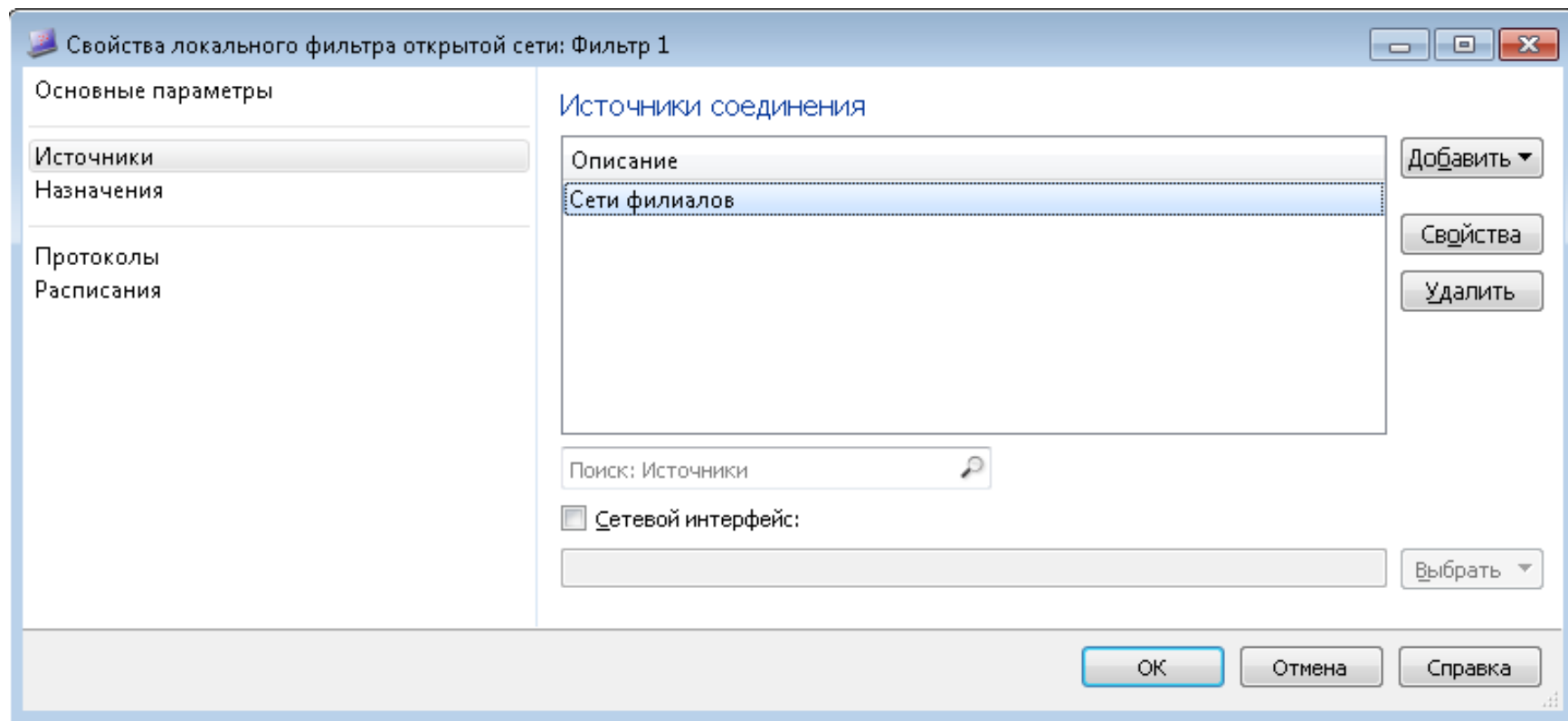
## Создание сетевого фильтра



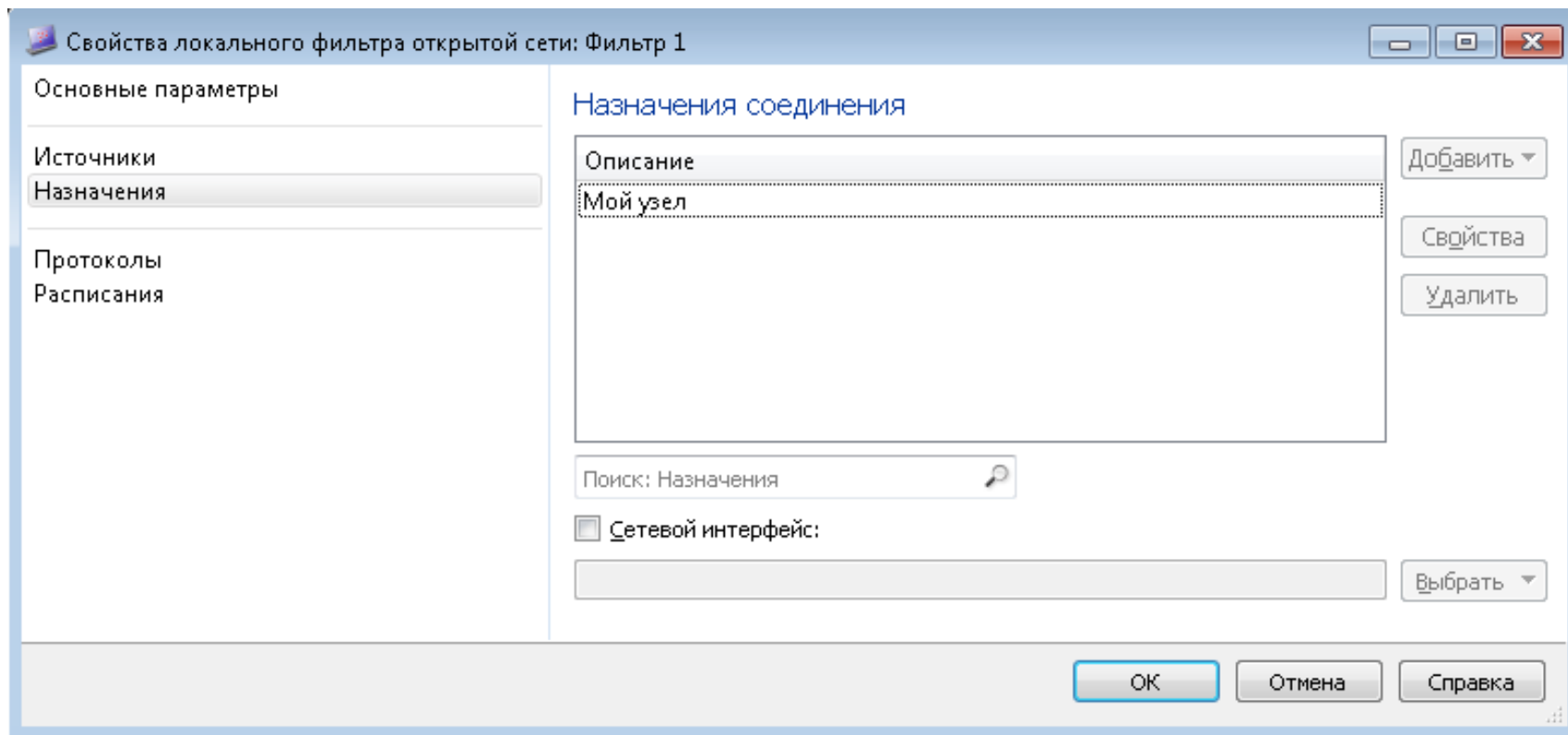
## Создание сетевого фильтра



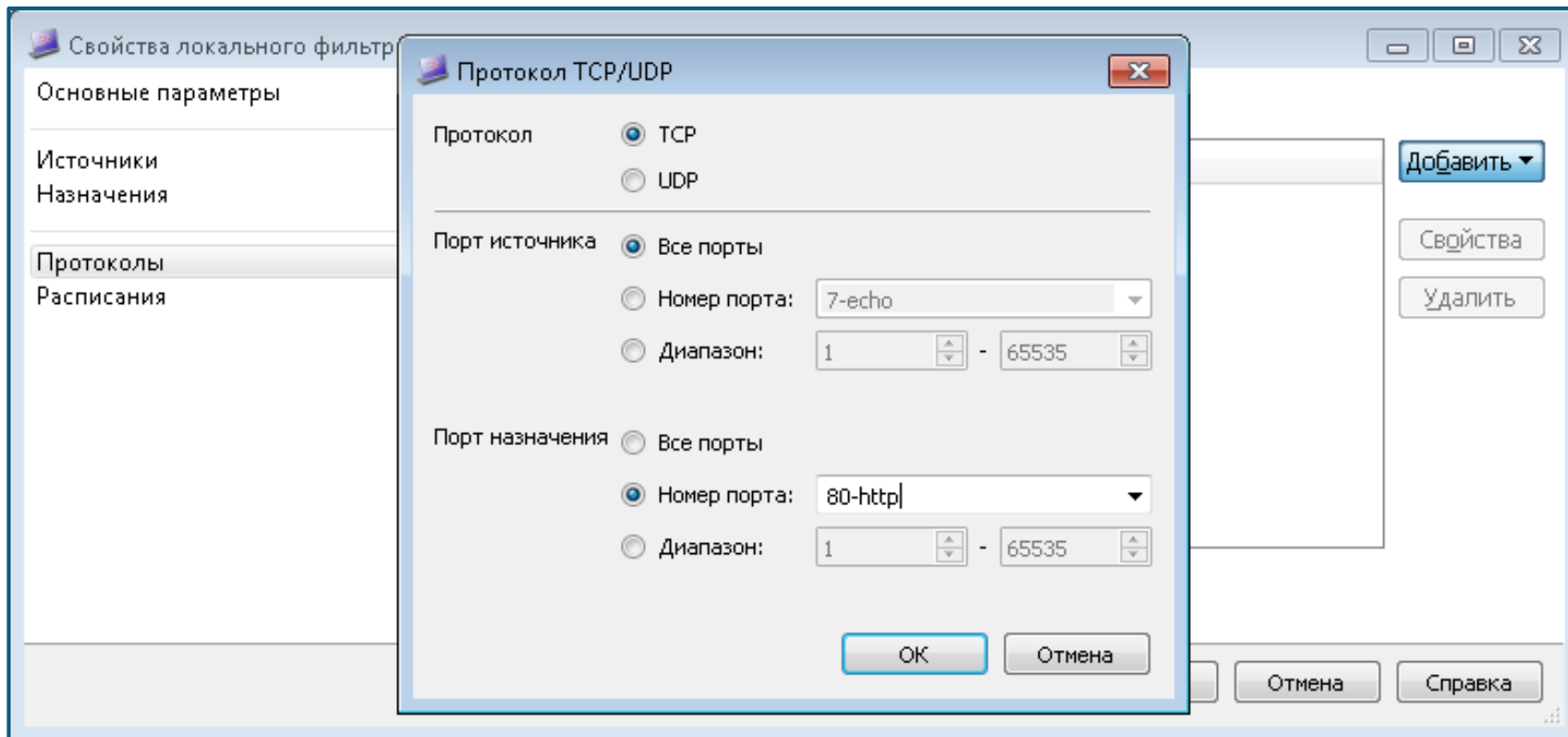
## Создание сетевого фильтра



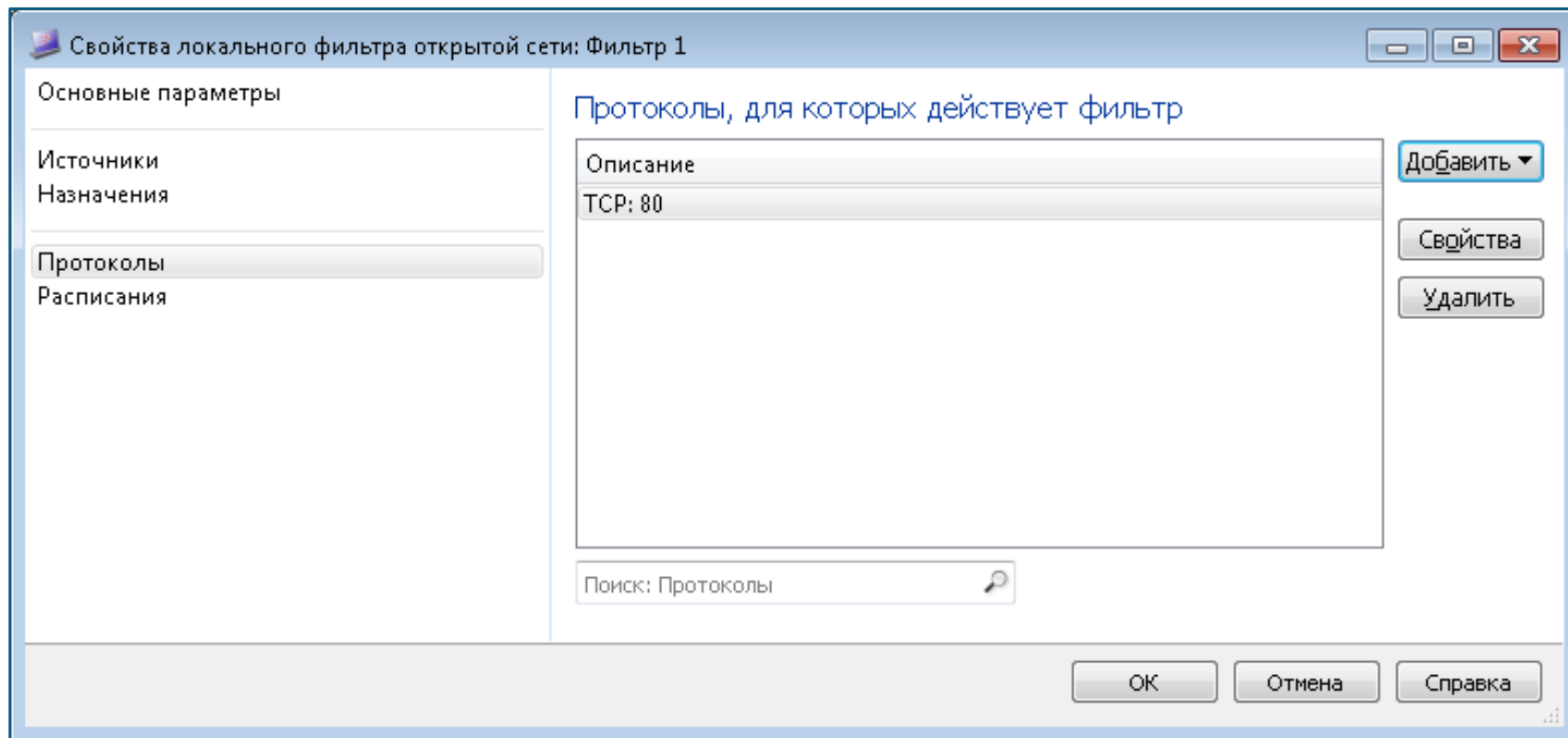
## Создание сетевого фильтра



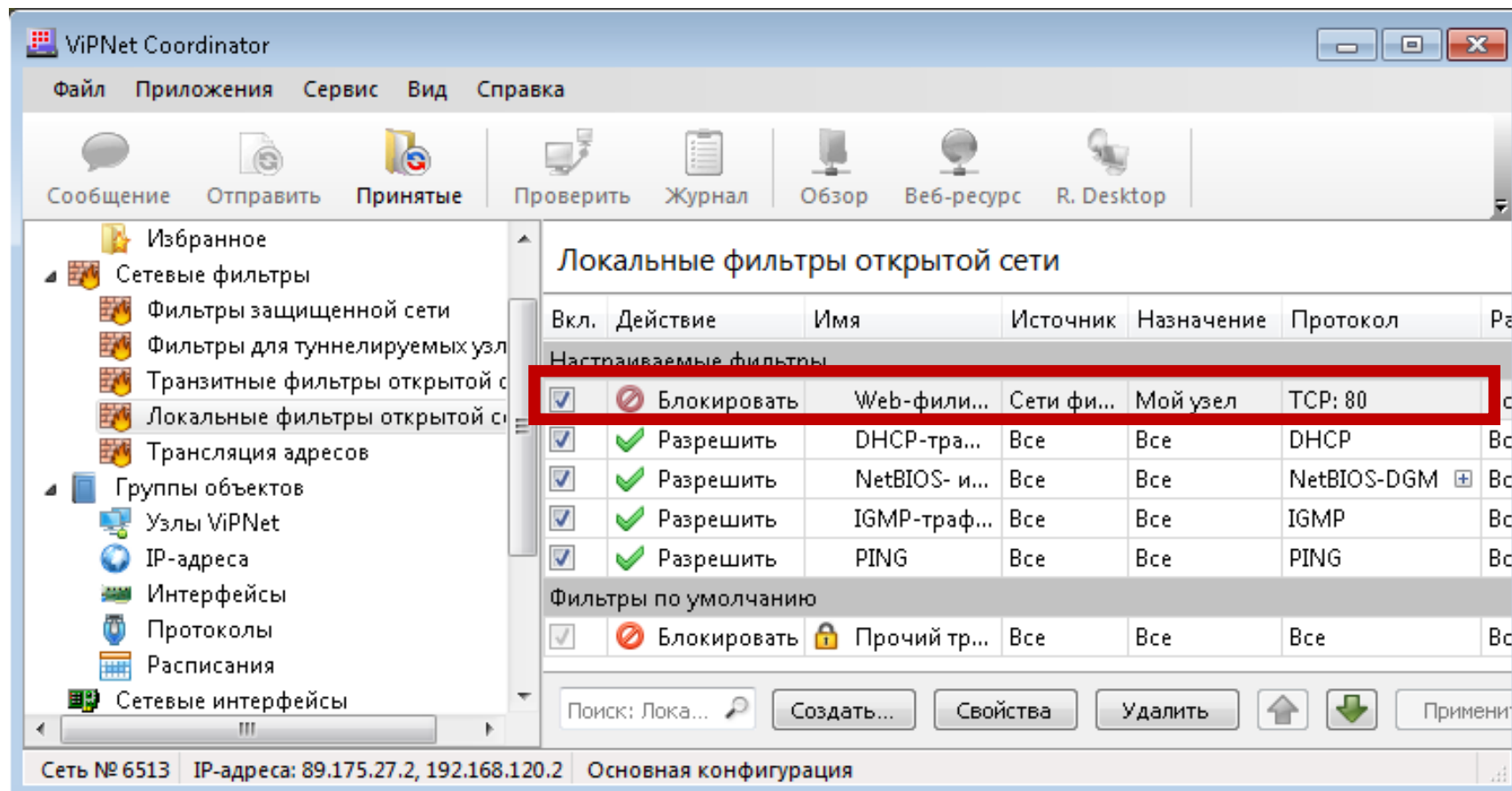
## Создание сетевого фильтра



## Создание сетевого фильтра



## Создание сетевого фильтра





## 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.

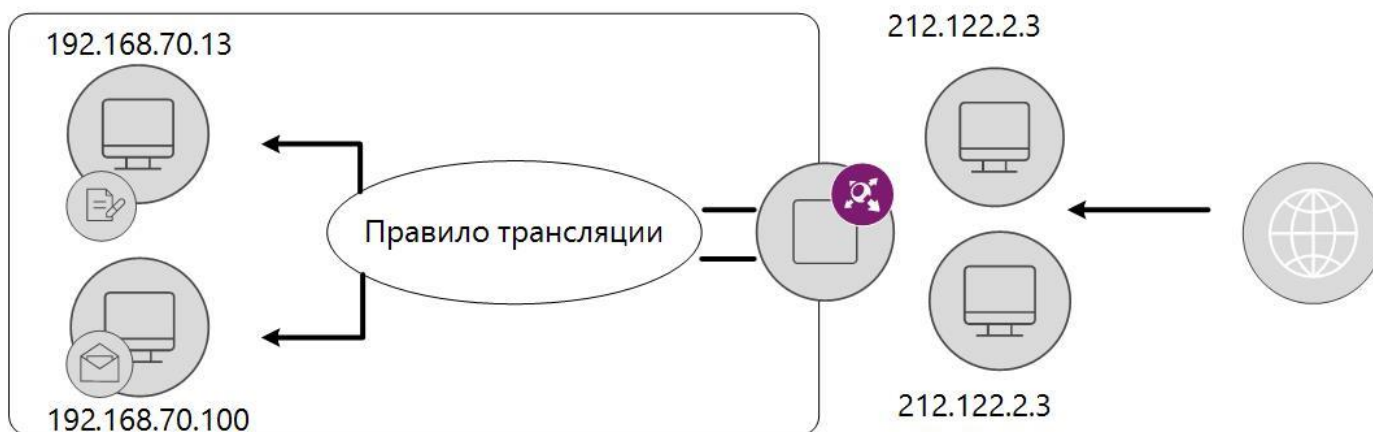
### Внимание!

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



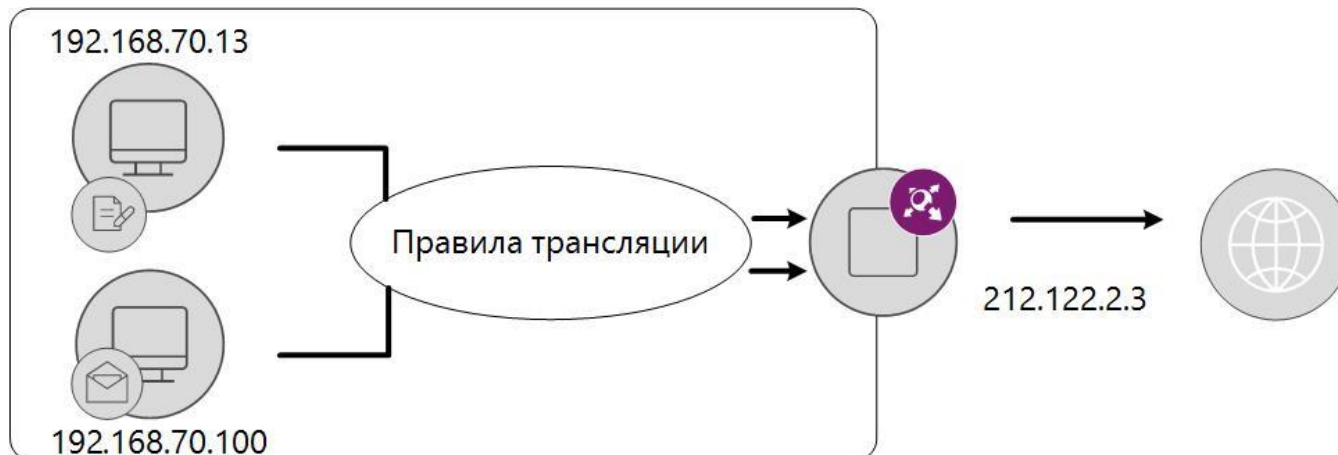
## Трансляция адреса узла назначения

- 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.

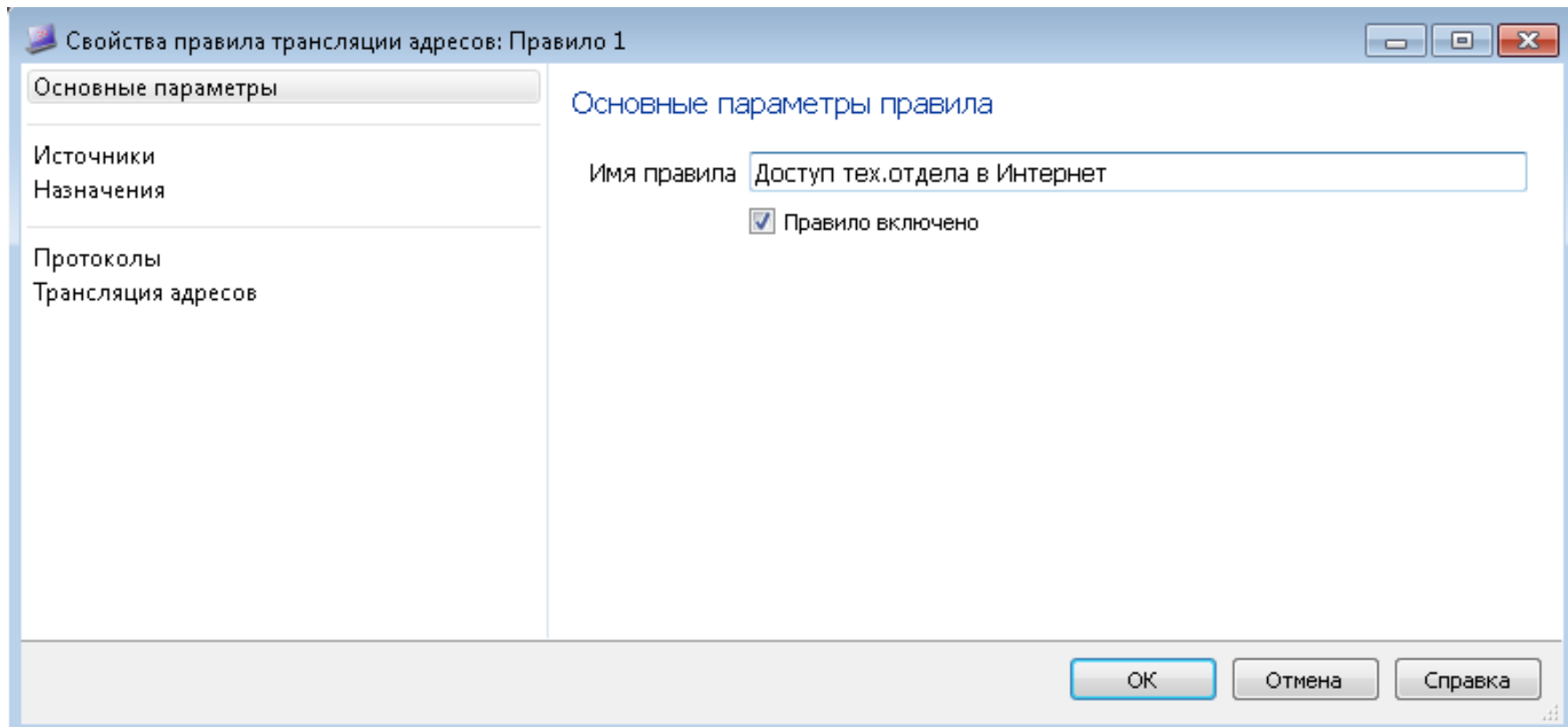


## Трансляция адреса источника

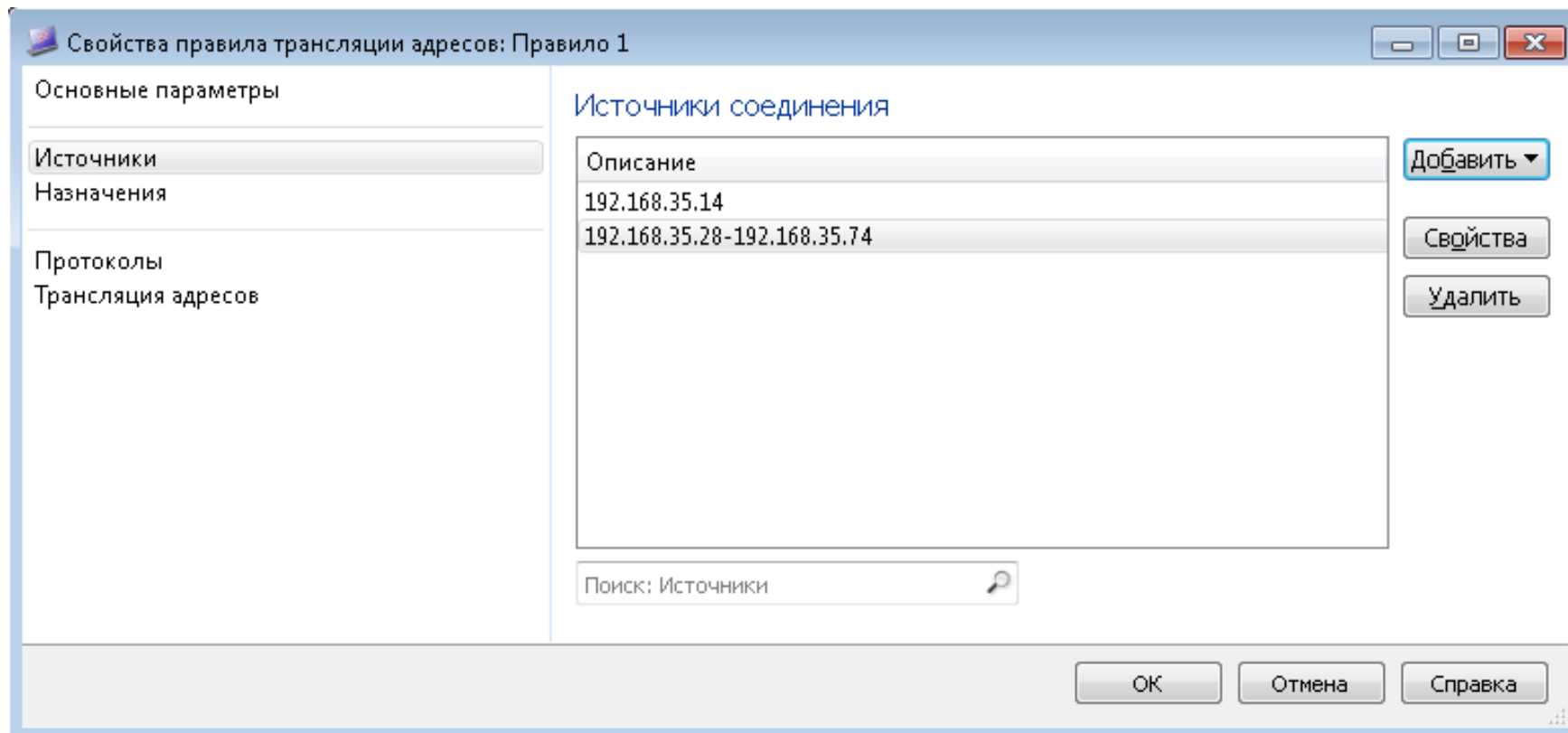
- Правило трансляции адреса источника ставит в соответствие нескольким частным IP-адресам локальных узлов публичный IP-адрес координатора.
- В заголовках IP-пакетов частные IP-адреса источника заменяются на публичный IP-адрес координатора. Узлы локальной сети могут устанавливать соединения с узлами в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



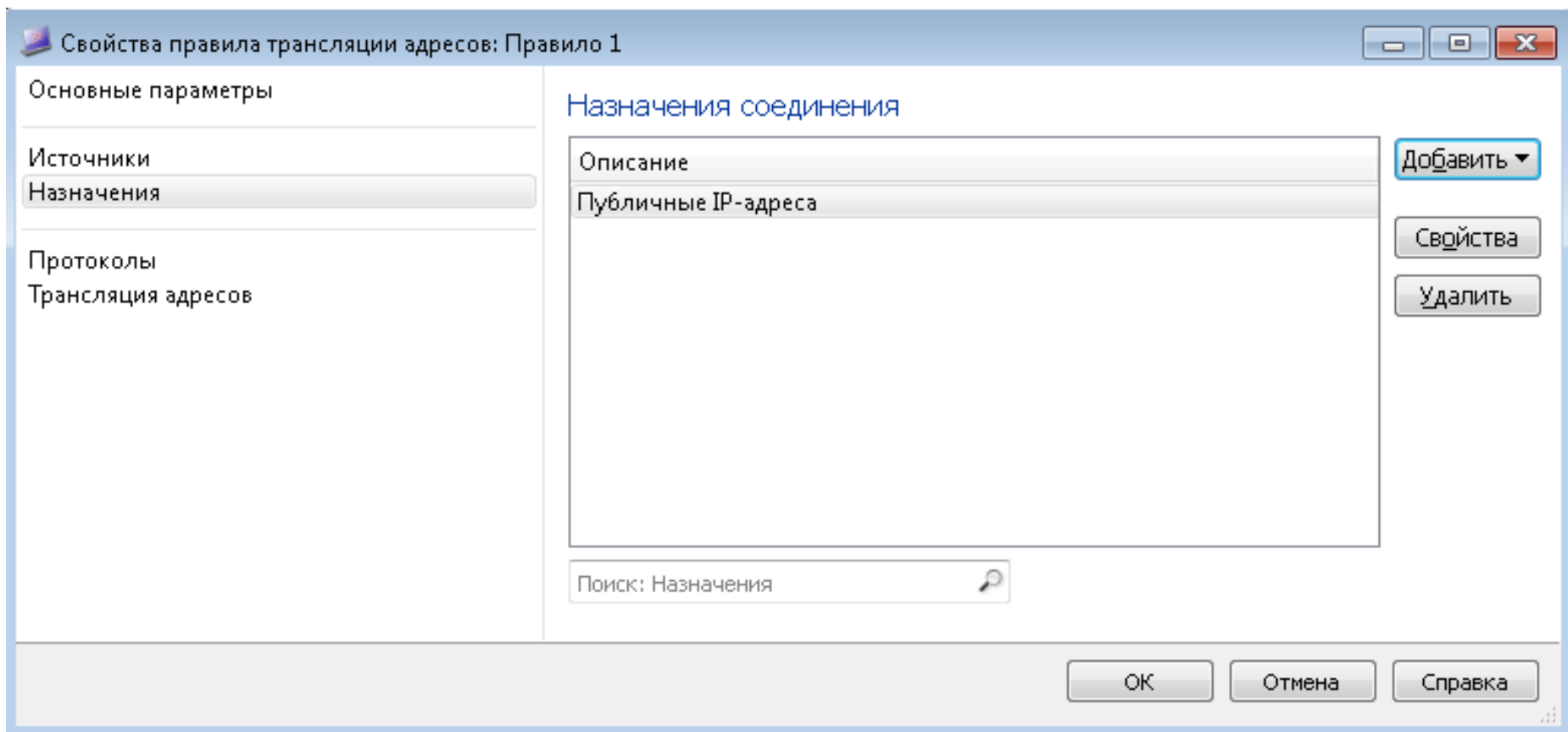
## Создание правила трансляции адресов



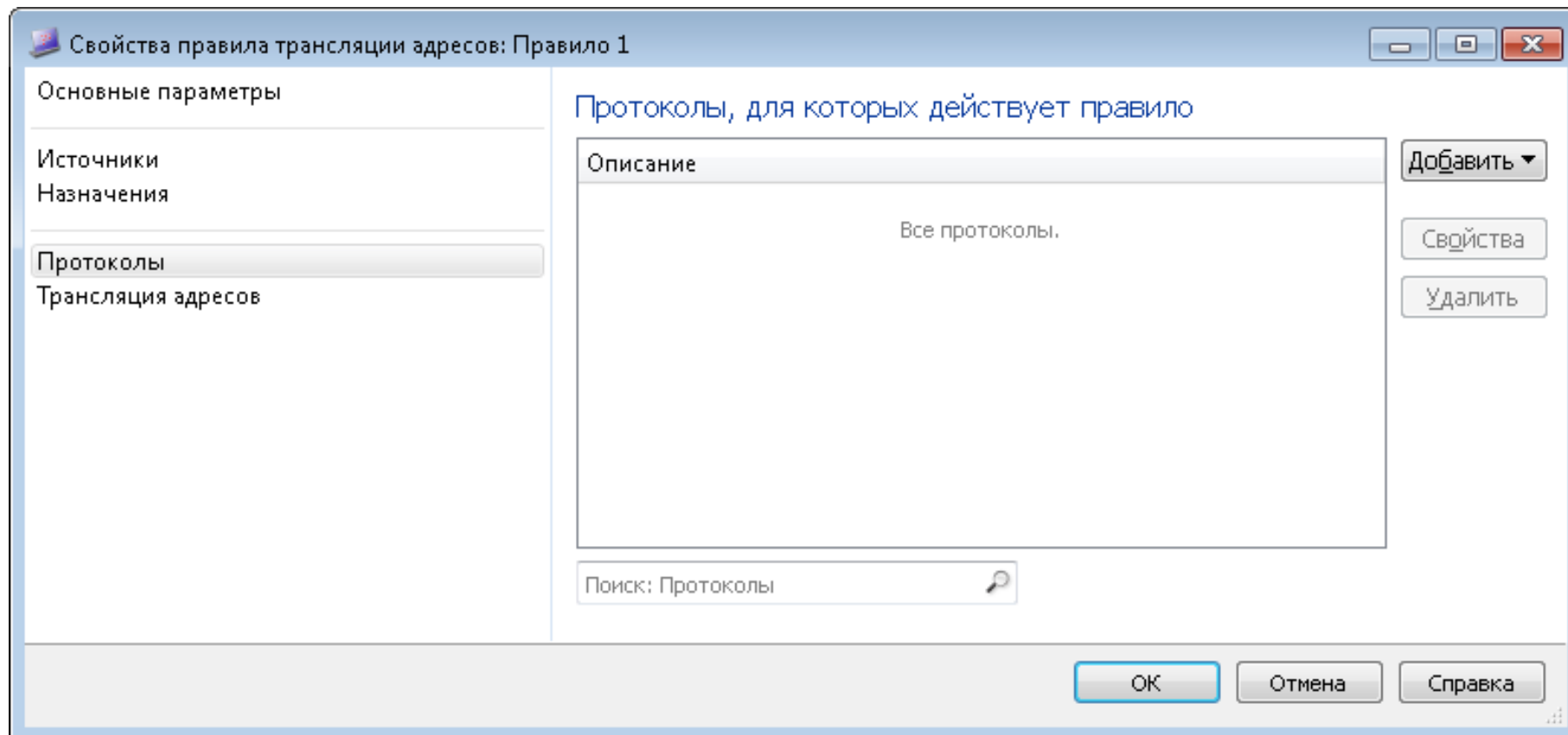
## Создание правила трансляции адресов



## Создание правила трансляции адресов



## Создание правила трансляции адресов



## Создание правила трансляции адресов

Свойства правила трансляции адресов: Правило 1

Основные параметры

Источники

Назначения

Протоколы

Трансляция адресов

### Настройка трансляции адресов

Трансляция источника

☒ Заменять адрес источника на:

☒ Адрес исходящего интерфейса (определяется автоматически)

☐ Другой адрес: . . .

Трансляция назначения

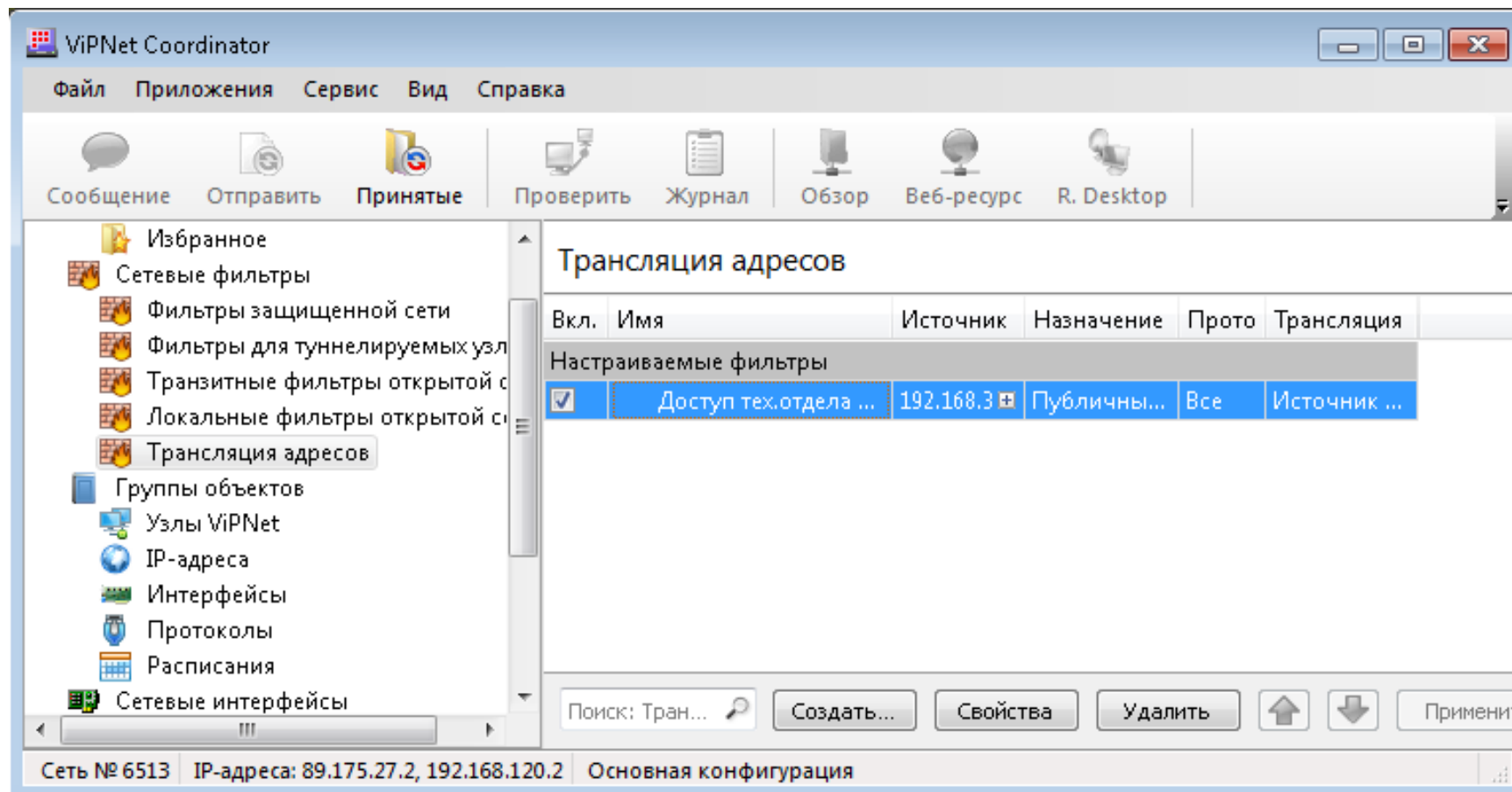
☐ Заменять адрес назначения на: . . .

☐ Заменять порт назначения на: 7-echo ▾

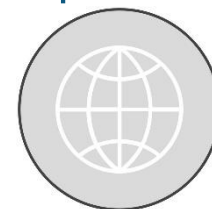
OK Отмена Справка



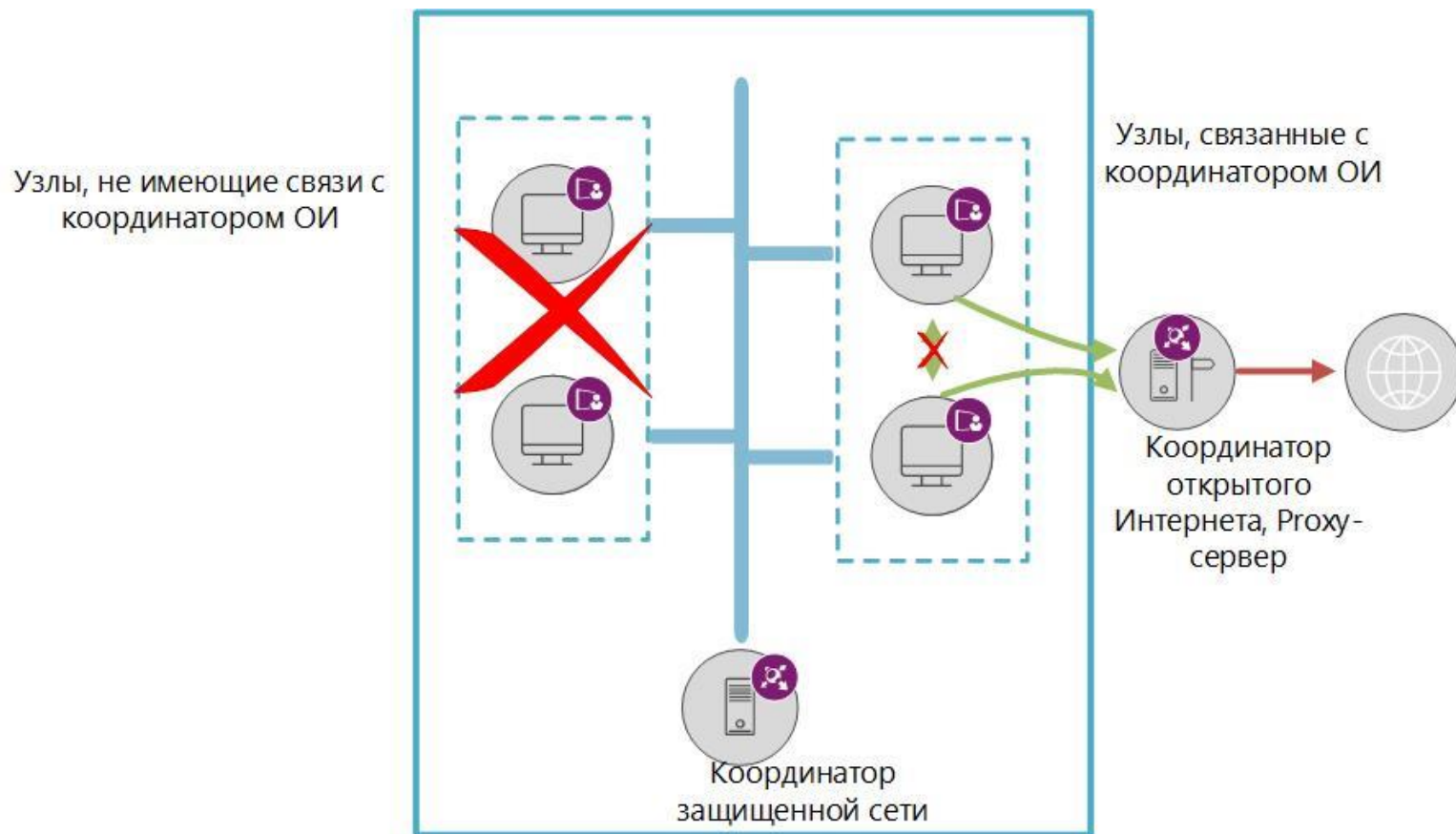
## Создание правила трансляции адресов



- 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.

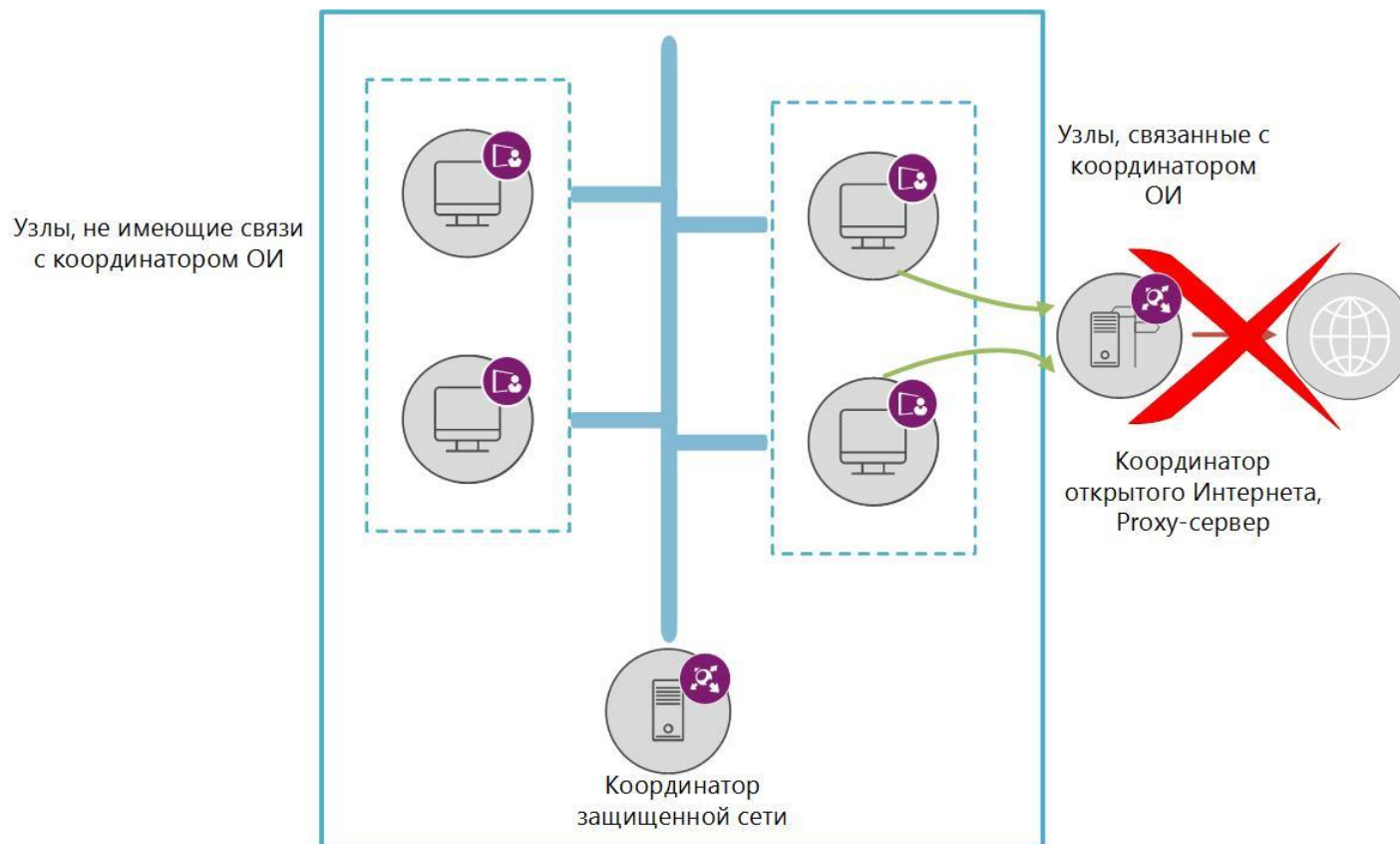


## Работа в конфигурации «Открытый Интернет»



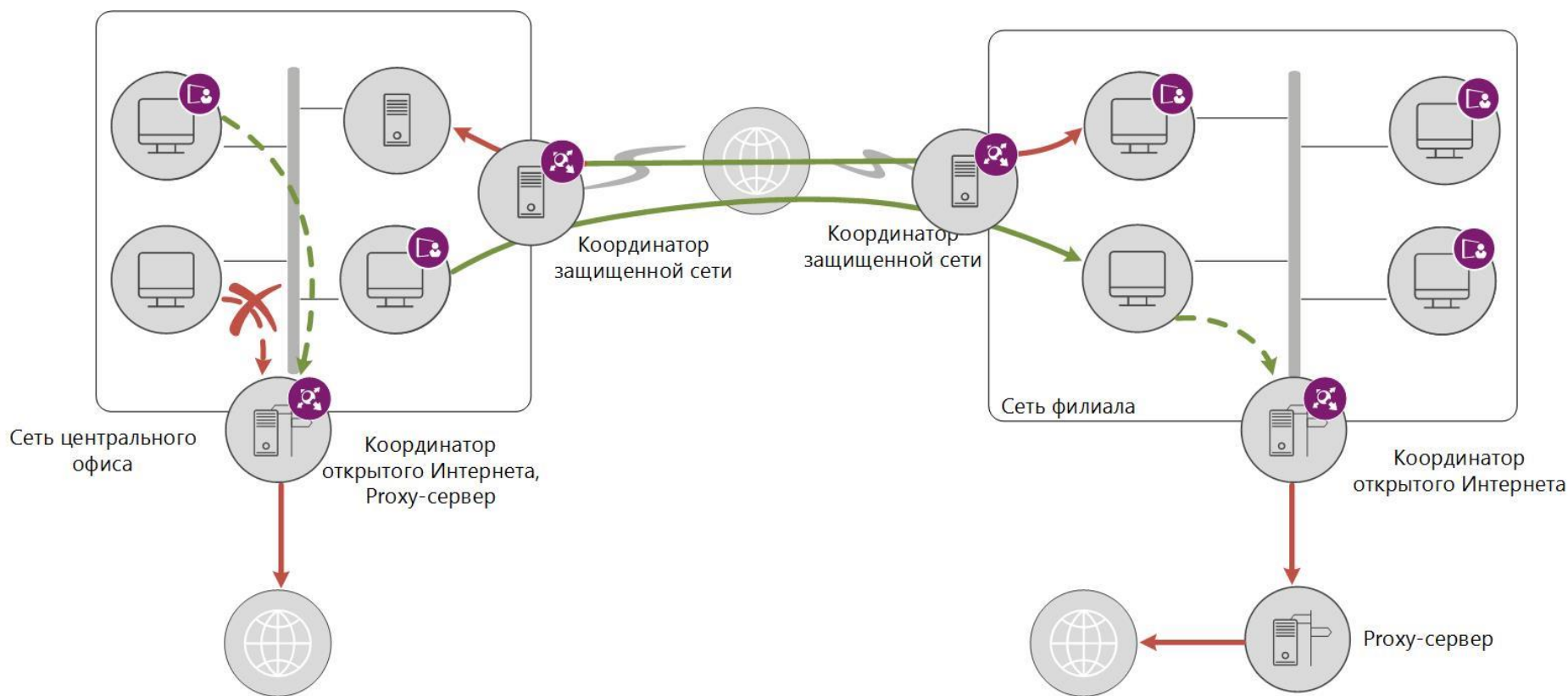
В конфигурации «Открытый Интернет» заблокированы соединения со всеми узлами (как защищенными так и открытыми), кроме координатора открытого Интернета.

## Работа в основной конфигурации



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

## 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 прокси-сервера. Выполнить на прокси-сервере необходимые настройки для доступа клиентов в Интернет.



Если прокси-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.

## Просмотр информации о ViPNet Coordinator

The screenshot shows the ViPNet Coordinator application window. The title bar reads "ViPNet Coordinator". The menu bar includes "Файл", "Приложения", "Сервис", "Вид", and "Справка". The toolbar contains icons for "Сообщение", "Отправить", "Принятые", "Проверить", "Журнал", "Обзор", "Веб-ресурс", and "R. Desktop".

The left sidebar displays a tree view of the application's structure:

- ViPNet Coordinator
  - Защищенная сеть
    - Избранное
    - Сетевые фильтры
      - Фильтры защищенной сети
      - Фильтры для туннелируемых узлов
      - Транзитные фильтры открытой сети
      - Локальные фильтры открытой сети
      - Трансляция адресов
    - Группы объектов
      - Узлы ViPNet
      - IP-адреса
      - Интерфейсы
      - Протоколы
      - Расписания
    - Сетевые интерфейсы
    - Статистика и журналы
      - Журнал IP-пакетов
      - Статистика
    - Конфигурации
      - Основная конфигурация

The main pane displays the "ViPNet Coordinator" configuration page. It shows the following information:

Сеть: **N 6513, Учебная сеть 6513**

Узел: **1971000A Координатор Центр офис**

Пользователь ViPNet: **Координатор Центр офис**

Сегодня: **15:52:54 18 июня 2020 г.**

Время запуска программы: **11:41:21 18 июня 2020 г.**

Ваш IP-адрес: **89.175.27.2, 192.168.120.2**

Общее число защищенных узлов, доступных Вам: **6**

Число узлов, в данный момент подключенных к сети: **3**

Число компьютеров, с которыми устанавливались защищенные соединения: **2**

Число компьютеров, с которыми устанавливались открытые соединения: **1**

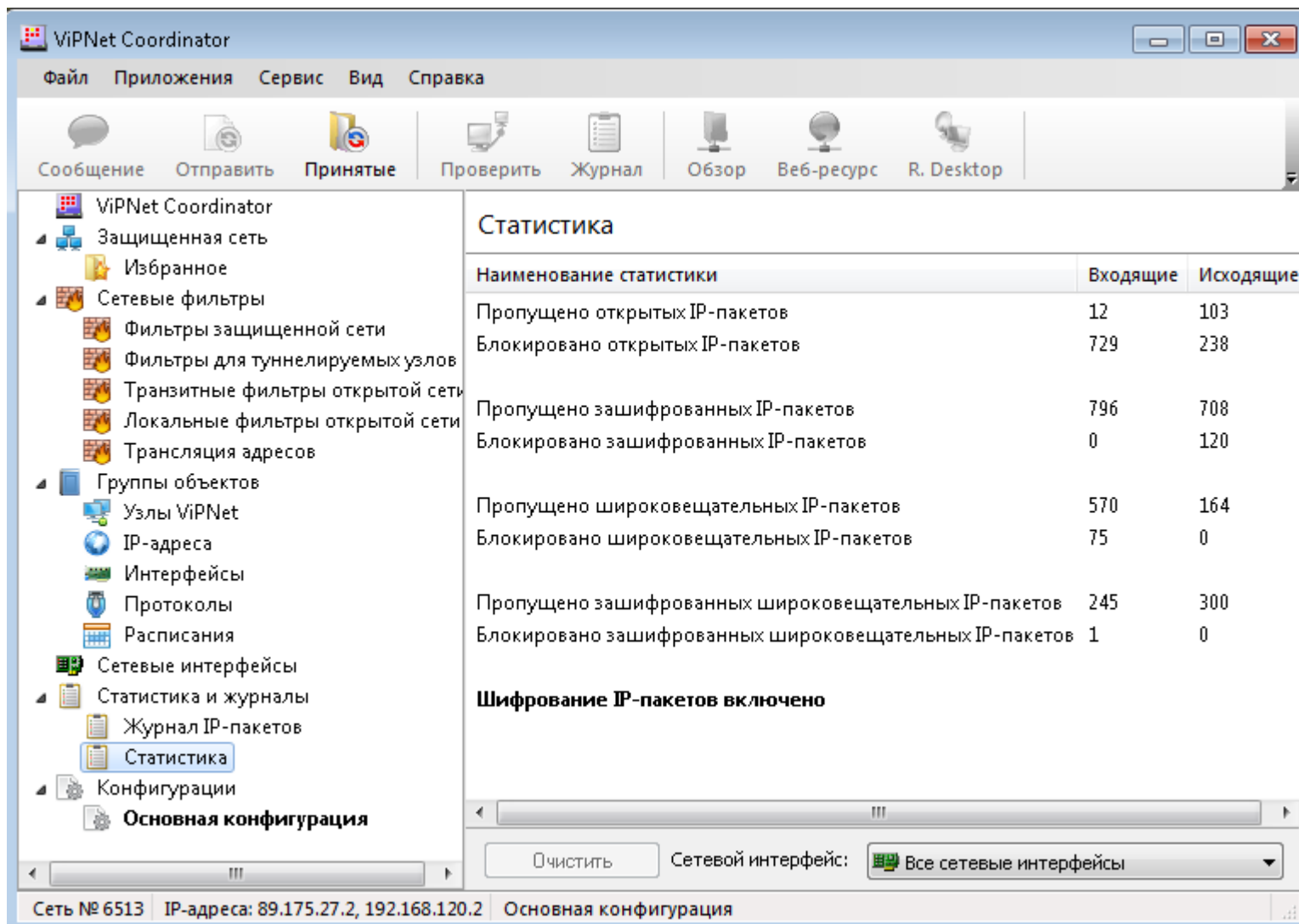
Число компьютеров, с которых блокировались попытки входящих соединений: **2**

Число компьютеров, на которые блокировались попытки исходящих соединений: **2**

The status bar at the bottom shows: "Сеть № 6513 IP-адреса: 89.175.27.2, 192.168.120.2 Основная конфигурация".



## Просмотр статистики IP-пакетов



The screenshot shows the ViPNet Coordinator application window. The left sidebar contains a tree view with the following items: ViPNet Coordinator, Защищенная сеть, Избранное, Сетевые фильтры (with sub-items: Фильтры защищенной сети, Фильтры для туннелируемых узлов, Транзитные фильтры открытой сети, Локальные фильтры открытой сети, Трансляция адресов), Группы объектов (with sub-items: Узлы ViPNet, IP-адреса, Интерфейсы, Протоколы, Расписания), Сетевые интерфейсы, Статистика и журналы (with sub-items: Журнал IP-пакетов, **Статистика**), and Конфигурации (with sub-item: Основная конфигурация). The main area is titled 'Статистика' and contains a table with the following data:

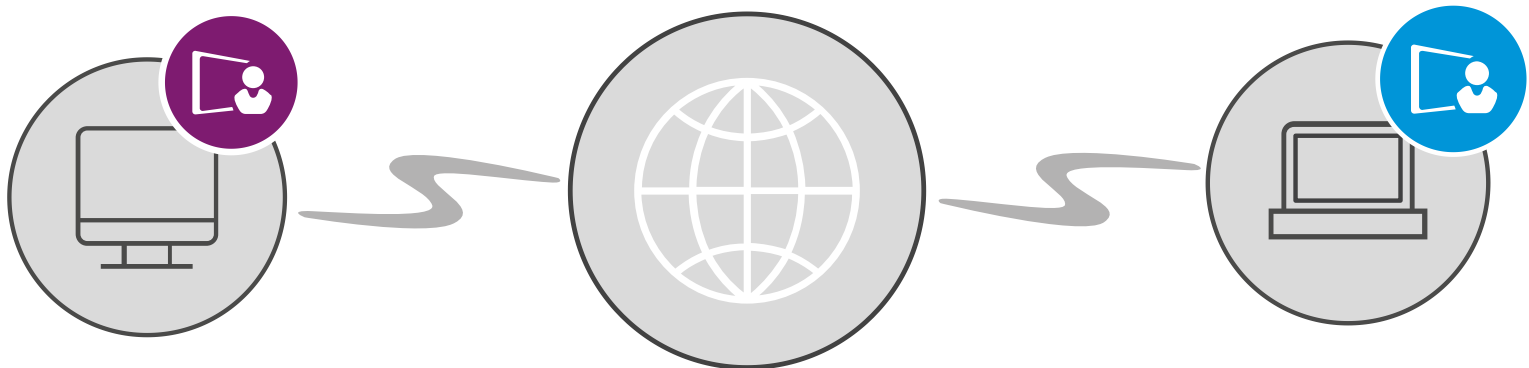
Наименование статистики	Входящие	Исходящие
Пропущено открытых IP-пакетов	12	103
Блокировано открытых IP-пакетов	729	238
Пропущено зашифрованных IP-пакетов	796	708
Блокировано зашифрованных IP-пакетов	0	120
Пропущено широковещательных IP-пакетов	570	164
Блокировано широковещательных IP-пакетов	75	0
Пропущено зашифрованных широковещательных IP-пакетов	245	300
Блокировано зашифрованных широковещательных IP-пакетов	1	0

Below the table, the text 'Шифрование IP-пакетов включено' is displayed. At the bottom of the window, there is a status bar showing 'Сеть № 6513', 'IP-адреса: 89.175.27.2, 192.168.120.2', and 'Основная конфигурация'. A toolbar at the bottom includes a 'Очистить' button and a dropdown menu for 'Сетевой интерфейс:' set to 'Все сетевые интерфейсы'.



## 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 источника и порт назначения;
  - код события;
  - ...



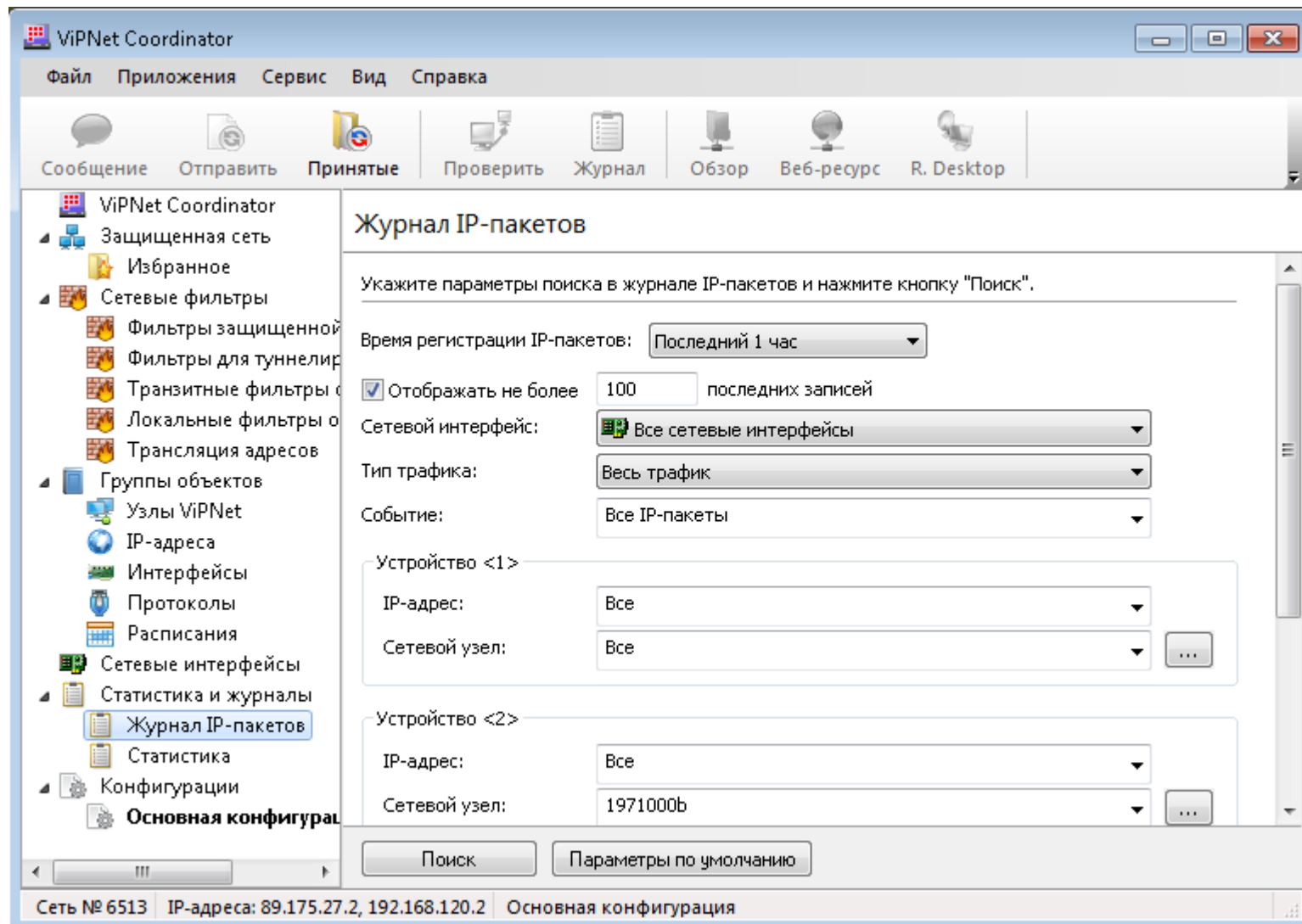
## События, отслеживаемые ViPNet

### 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

## Поиск в журнале IP-пакетов



## Поиск в журнале IP-пакетов

Время регистрации IP-пакетов: Последний 1 час

☒ Отображать не более 100 последних записей

Сетевой интерфейс: Все сетевые интерфейсы

Тип трафика: Весь трафик

Событие: Все IP-пакеты

## Устройство &lt;1&gt;

IP-адрес: Все

Сетевой узел: Координатор Филиал 1

## Устройство &lt;2&gt;

IP-адрес: Все

Сетевой узел: ViPNet Администратор

## Протокол

Протокол: TCP

Порт &lt;1&gt;: Все Порт &lt;2&gt;: Все

## Признаки IP-пакетов

Направление: Входящие Тип адреса: Одноадресный

Источник: Любое устройство Трансляция: Все

## Просмотр информации об IP-пакетах

1-Журнал регистрации IP-пакетов

Журнал Сервис Вид Справка

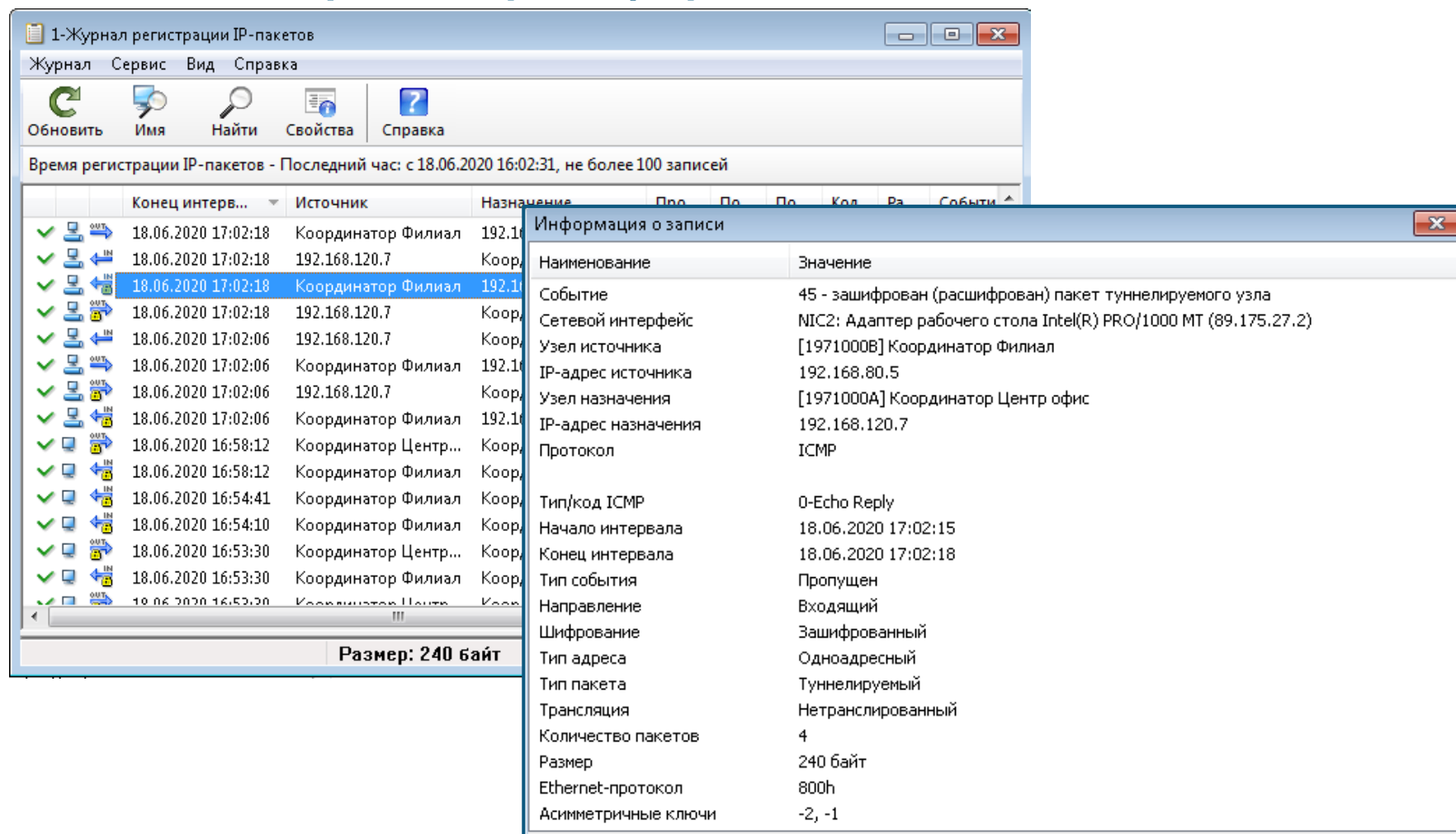
Обновить Имя Найти Свойства Справка

Время регистрации IP-пакетов - Последний час: с 18.06.2020 16:02:31, не более 100 записей

		Конец интерв...	Источник	Назначение	Про...	По...	По...	Кол...	Ра...	Событие
✓	OUT	18.06.2020 17:02:18	Координатор Филиал	192.168.120.7	ICMP	0-E...	4	468	63	63 - пакет пропущен фильтром для туннели...
✓	IN	18.06.2020 17:02:18	192.168.120.7	Координатор Фил...	ICMP	8-E...	4	240	63	63 - пакет пропущен фильтром для туннели...
✓	OUT	18.06.2020 17:02:18	Координатор Филиал	192.168.120.7	ICMP	0-E...	4	240	45	45 - зашифрован (расшифрован) пакет тунн...
✓	IN	18.06.2020 17:02:18	192.168.120.7	Координатор Фил...	ICMP	8-E...	4	240	45	45 - зашифрован (расшифрован) пакет тунн...
✓	OUT	18.06.2020 17:02:06	192.168.120.7	Координатор Фил...	ICMP	0-E...	4	240	63	63 - пакет пропущен фильтром для туннели...
✓	IN	18.06.2020 17:02:06	Координатор Филиал	192.168.120.7	ICMP	8-E...	4	468	63	63 - пакет пропущен фильтром для туннели...
✓	OUT	18.06.2020 17:02:06	192.168.120.7	Координатор Фил...	ICMP	0-E...	4	240	45	45 - зашифрован (расшифрован) пакет тунн...
✓	IN	18.06.2020 17:02:06	Координатор Филиал	192.168.120.7	ICMP	8-E...	4	240	45	45 - зашифрован (расшифрован) пакет тунн...
✓	OUT	18.06.2020 16:58:12	Координатор Центр...	Координатор Фил...	ICMP	8-E...	8	480	40	40 - пропущен зашифрованный IP-пакет
✓	IN	18.06.2020 16:58:12	Координатор Филиал	Координатор Цент...	ICMP	0-E...	8	480	40	40 - пропущен зашифрованный IP-пакет
✓	OUT	18.06.2020 16:54:41	Координатор Филиал	Координатор Цент...	ICMP	8-E...	4	240	40	40 - пропущен зашифрованный IP-пакет
✓	IN	18.06.2020 16:54:10	Координатор Филиал	Координатор Цент...	ICMP	8-E...	4	240	40	40 - пропущен зашифрованный IP-пакет
✓	OUT	18.06.2020 16:53:30	Координатор Центр...	Координатор Фил...	UDP	2046	2046	21	2553	40 - пропущен зашифрованный IP-пакет
✓	IN	18.06.2020 16:53:30	Координатор Филиал	Координатор Цент...	UDP	2046	2046	11	1270	40 - пропущен зашифрованный IP-пакет
✓	OUT	18.06.2020 16:53:30	Координатор Центр...	Координатор Фил...	UDP	2046	2046	5	500	40 - пропущен зашифрованный IP-пакет
✓	IN	18.06.2020 16:52:41	Координатор Филиал	Координатор Цент...	TCP	492...	5000	8	578	40 - пропущен зашифрованный IP-пакет
✓	OUT	18.06.2020 16:52:41	Координатор Центр...	Координатор Фил...	TCP	5000	492...	7	413	40 - пропущен зашифрованный IP-пакет
✓	IN	18.06.2020 16:52:11	Координатор Центр...	Координатор Фил...	TCP	5000		1	52	40 - пропущен зашифрованный IP-пакет
✓	OUT	18.06.2020 16:52:11	Координатор Филиал	Координатор Цент...	TCP		5000	2	92	40 - пропущен зашифрованный IP-пакет
✓	IN	18.06.2020 16:50:58	Координатор Филиал	Координатор Цент...	TCP	5000	492...	9	639	40 - пропущен зашифрованный IP-пакет
✓	OUT	18.06.2020 16:50:58	Координатор Центр...	Координатор Фил...	TCP	492...	5000	10	1968	40 - пропущен зашифрованный IP-пакет
✓	IN	18.06.2020 16:50:28	Координатор Центр...	Координатор Фил...	TCP		5000	4	1564	40 - пропущен зашифрованный IP-пакет
✓	OUT	18.06.2020 16:50:28	Координатор Филиал	Координатор Цент...	TCP	5000		4	200	40 - пропущен зашифрованный IP-пакет
✗	IN	18.06.2020 16:42:46	192.168.120.5	192.168.80.3	ICMP	8-E...	4	240	22	22 - незашифрованный IP-пакет от сетевого...

Размер: 240 байт      Запись: 4      Всего: 24

## Просмотр информации об IP-пакетах



1-Журнал регистрации IP-пакетов

Журнал Сервис Вид Справка

Обновить Имя Найти Свойства Справка

Время регистрации IP-пакетов - Последний час: с 18.06.2020 16:02:31, не более 100 записей

	Конец интерв...	Источник	Назначение	Про	По	По	Код	Па	Событи
✓	18.06.2020 17:02:18	Координатор Филиал	192.168.120.7	OUT	IN				
✓	18.06.2020 17:02:18	192.168.120.7	Коор...	IN	OUT				
✓	18.06.2020 17:02:18	Координатор Филиал	192.168.120.7	OUT	IN				
✓	18.06.2020 17:02:18	192.168.120.7	Коор...	IN	OUT				
✓	18.06.2020 17:02:06	192.168.120.7	Коор...	IN	OUT				
✓	18.06.2020 17:02:06	Координатор Филиал	192.168.120.7	OUT	IN				
✓	18.06.2020 17:02:06	192.168.120.7	Коор...	IN	OUT				
✓	18.06.2020 17:02:06	Координатор Филиал	192.168.120.7	OUT	IN				
✓	18.06.2020 17:02:06	Координатор Филиал	192.168.120.7	OUT	IN				
✓	18.06.2020 16:58:12	Координатор Центр...	Коор...	IN	OUT				
✓	18.06.2020 16:58:12	Координатор Филиал	Коор...	IN	OUT				
✓	18.06.2020 16:54:41	Координатор Филиал	Коор...	IN	OUT				
✓	18.06.2020 16:54:10	Координатор Филиал	Коор...	IN	OUT				
✓	18.06.2020 16:53:30	Координатор Центр...	Коор...	IN	OUT				
✓	18.06.2020 16:53:30	Координатор Филиал	Коор...	IN	OUT				
✓	18.06.2020 16:53:30	Координатор Центр...	Коор...	IN	OUT				

Размер: 240 байт

Информация о записи

Наименование	Значение
Событие	45 - зашифрован (расшифрован) пакет туннелируемого узла
Сетевой интерфейс	NIC2: Адаптер рабочего стола Intel(R) PRO/1000 MT (89.175.27.2)
Узел источника	[1971000B] Координатор Филиал
IP-адрес источника	192.168.80.5
Узел назначения	[1971000A] Координатор Центр офис
IP-адрес назначения	192.168.120.7
Протокол	ICMP
Тип/код ICMP	0-Echo Reply
Начало интервала	18.06.2020 17:02:15
Конец интервала	18.06.2020 17:02:18
Тип события	Пропущен
Направление	Входящий
Шифрование	Зашифрованный
Тип адреса	Одноадресный
Тип пакета	Туннелируемый
Трансляция	Нетранслированный
Количество пакетов	4
Размер	240 байт
Ethernet-протокол	800h
Асимметричные ключи	-2, -1

## Просмотр информации об IP-пакетах в веб-браузере

1-Журнал регистрации IP-пакетов

Журнал Сервис Вид Справка

Обновить Имя Най

Информация о записи

Наименование Значение

Событие 45 - зашифрован (расшифрован) пакет туннелируемого узла

Время регистрации IP-пакета

Конец интервала

✓	OUT	18.06.2020 17:00	Сетевой интерфейс
✓	IN	18.06.2020 17:00	Узел источника
✓	IN	18.06.2020 17:00	IP-адрес источника
✓	IN	18.06.2020 17:00	Узел назначения
✓	IN	18.06.2020 17:00	IP-адрес назначения
✓	IN	18.06.2020 17:00	Протокол
✓	OUT	18.06.2020 17:00	Тип/код ICMP
✓	OUT	18.06.2020 17:00	Начало интервала
✓	OUT	18.06.2020 17:00	Конец интервала
✓	OUT	18.06.2020 16:59	Тип события
✓	OUT	18.06.2020 16:59	Направление
✓	OUT	18.06.2020 16:59	Шифрование
✓	OUT	18.06.2020 16:59	Тип адреса
✓	OUT	18.06.2020 16:59	Тип пакета
✓	OUT	18.06.2020 16:59	Трансляция
✓	OUT	18.06.2020 16:59	Количество пакетов
✓	OUT	18.06.2020 16:59	Размер
✓	OUT	18.06.2020 16:59	Ethernet-протокол
✓	OUT	18.06.2020 16:59	Асимметричные ключи

45 - зашифрован (расшифрован) пакет туннелируемого узла

C:\Program Files (x86)\InfoTeCS\VIPNet Coordinator\%tmpdir%\htmB770 Координатор Центр офис 1971 - Windows Internet Expl...

C:\Program Files (x86)\InfoTeCS\VIPNet Coordinator\%tmpdir%\

Избранное Рекомендуемые узлы Коллекция веб-фрагм...

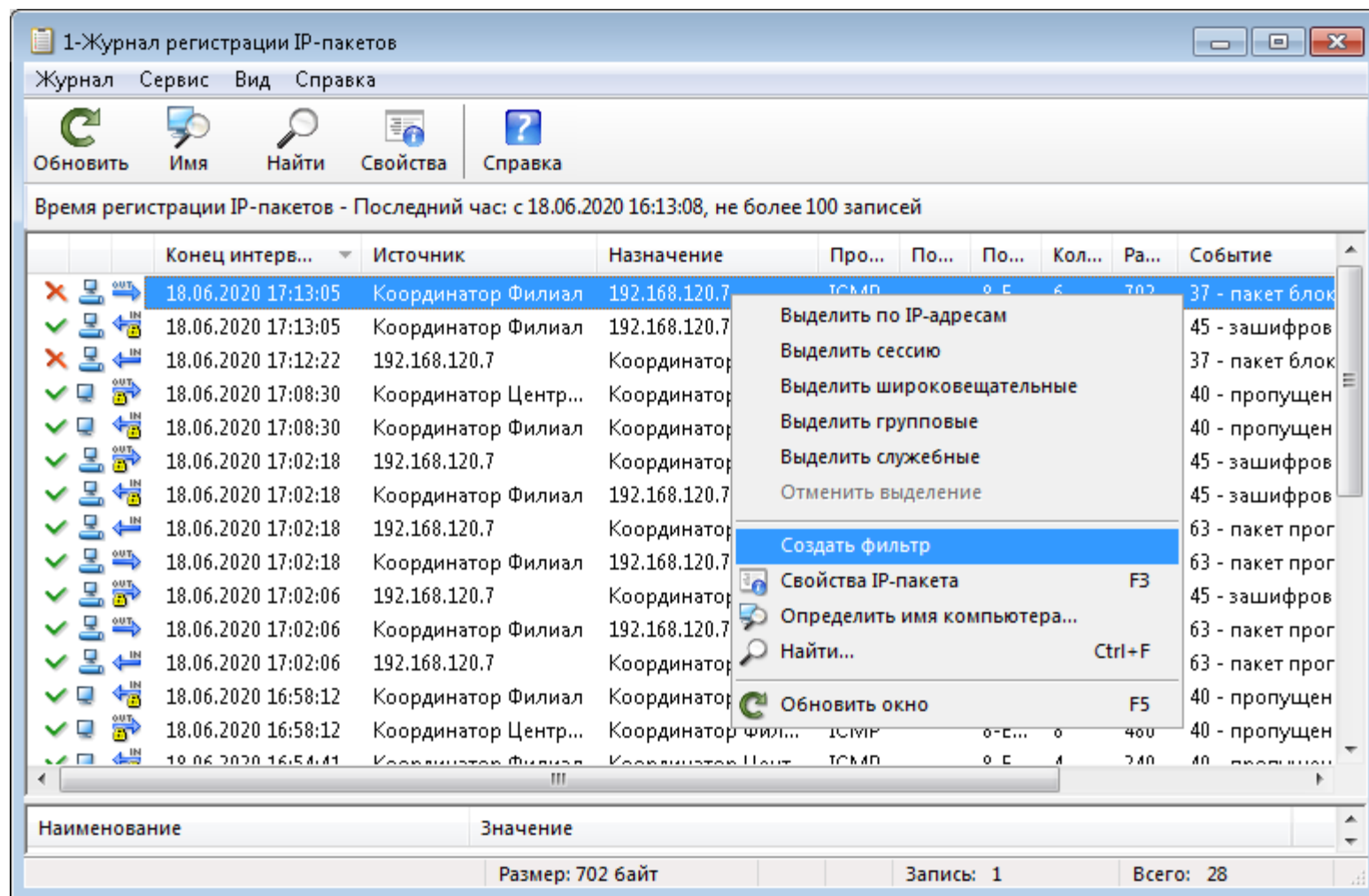
C:\Program Files (x86)\InfoTeCS\VIPNet Coordin...

Пропущен	Туннелируемый	Исходящий Зашифрованный	Одноадресный	Нетранслированный	18.06.2020 17:02:03	18.06.2020 17:02:06	NIC2: рабоч Intel(R) PRO/1 (89.17
Пропущен	Туннелируемый	Входящий Зашифрованный	Одноадресный	Нетранслированный	18.06.2020 17:02:03	18.06.2020 17:02:06	NIC2: рабоч Intel(R) PRO/1 (89.17
Пропущен	Локальный	Исходящий Зашифрованный	Одноадресный	Нетранслированный	18.06.2020 16:57:25	18.06.2020 16:58:12	NIC2: рабоч Intel(R) PRO/1 (89.17
Пропущен	Локальный	Входящий Зашифрованный	Одноадресный	Нетранслированный	18.06.2020 16:57:25	18.06.2020 16:58:12	NIC2: рабоч Intel(R) PRO/1 (89.17

Готово

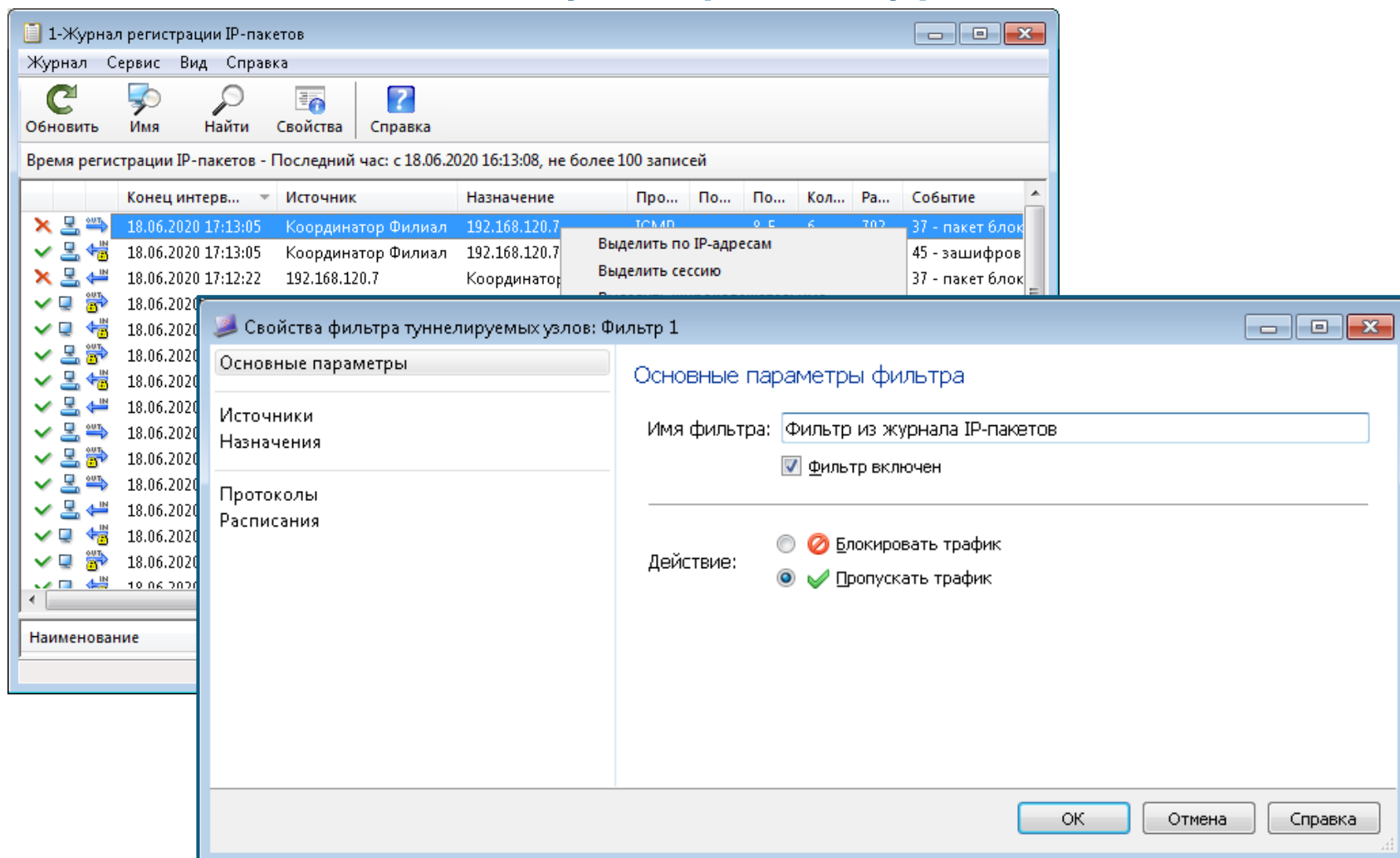
Компьютер | Защищенный режим: выкл.

## Создание сетевого фильтра из журнала IP-пакетов

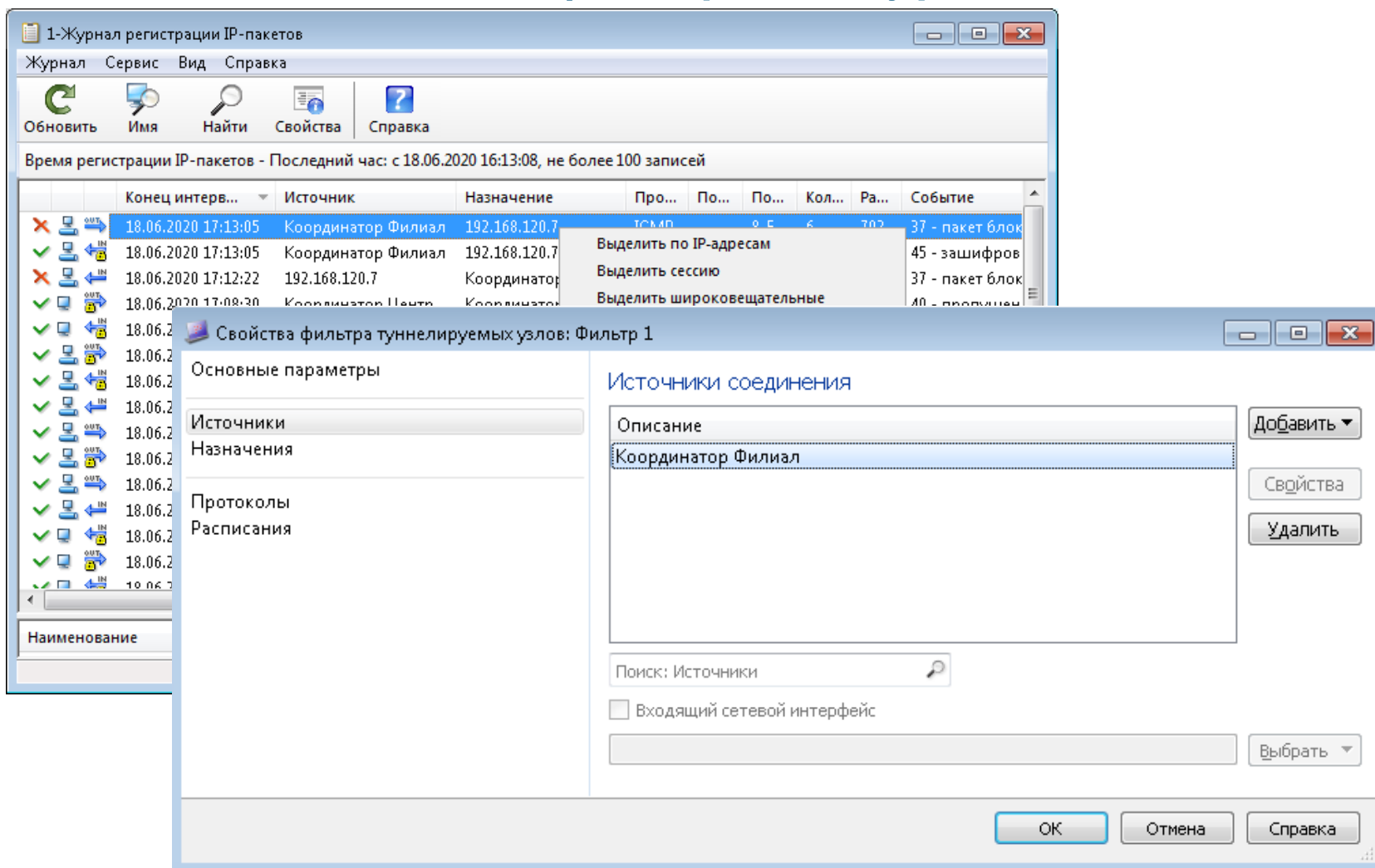




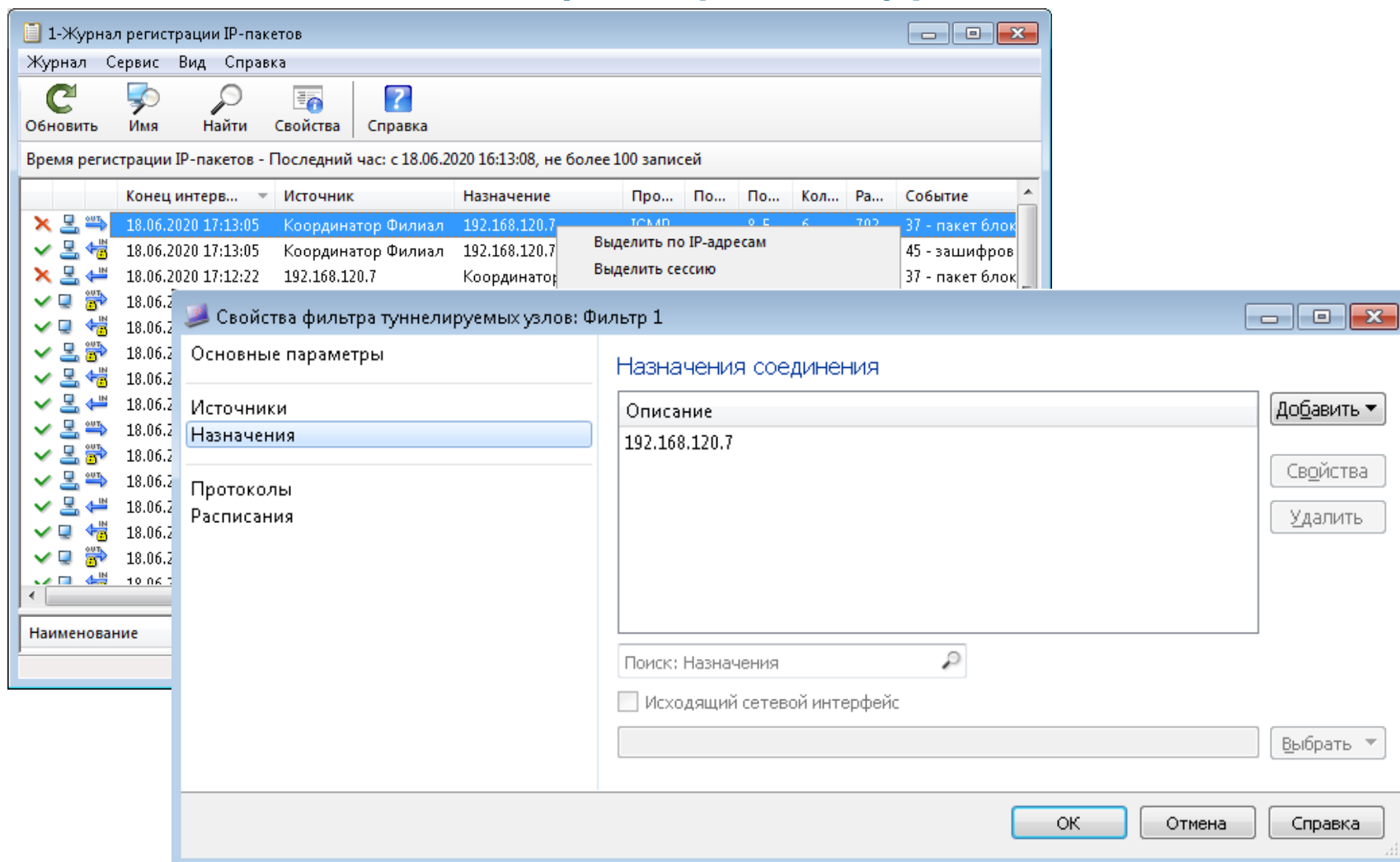
## Создание сетевого фильтра из журнала IP-пакетов



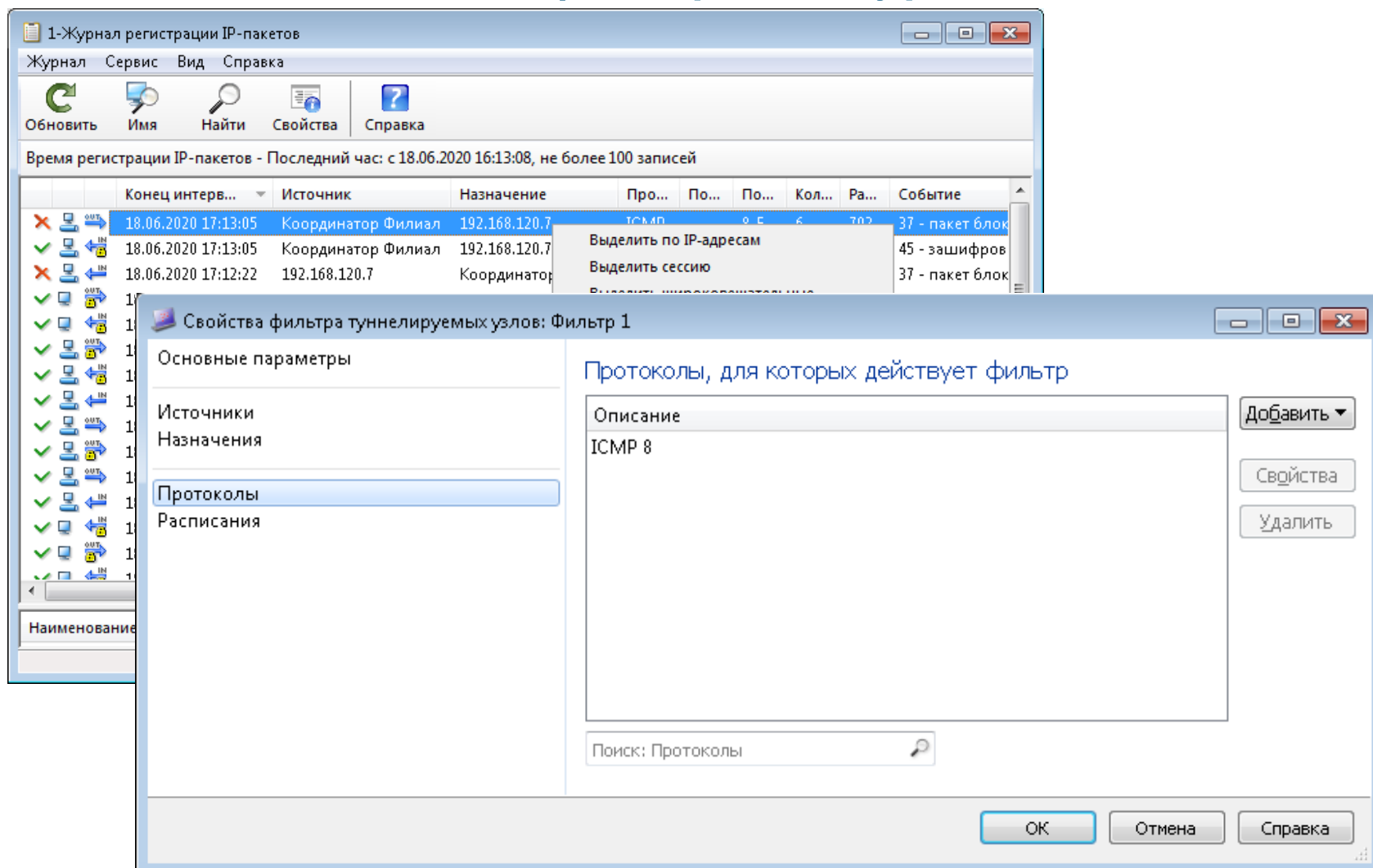
## Создание сетевого фильтра из журнала IP-пакетов



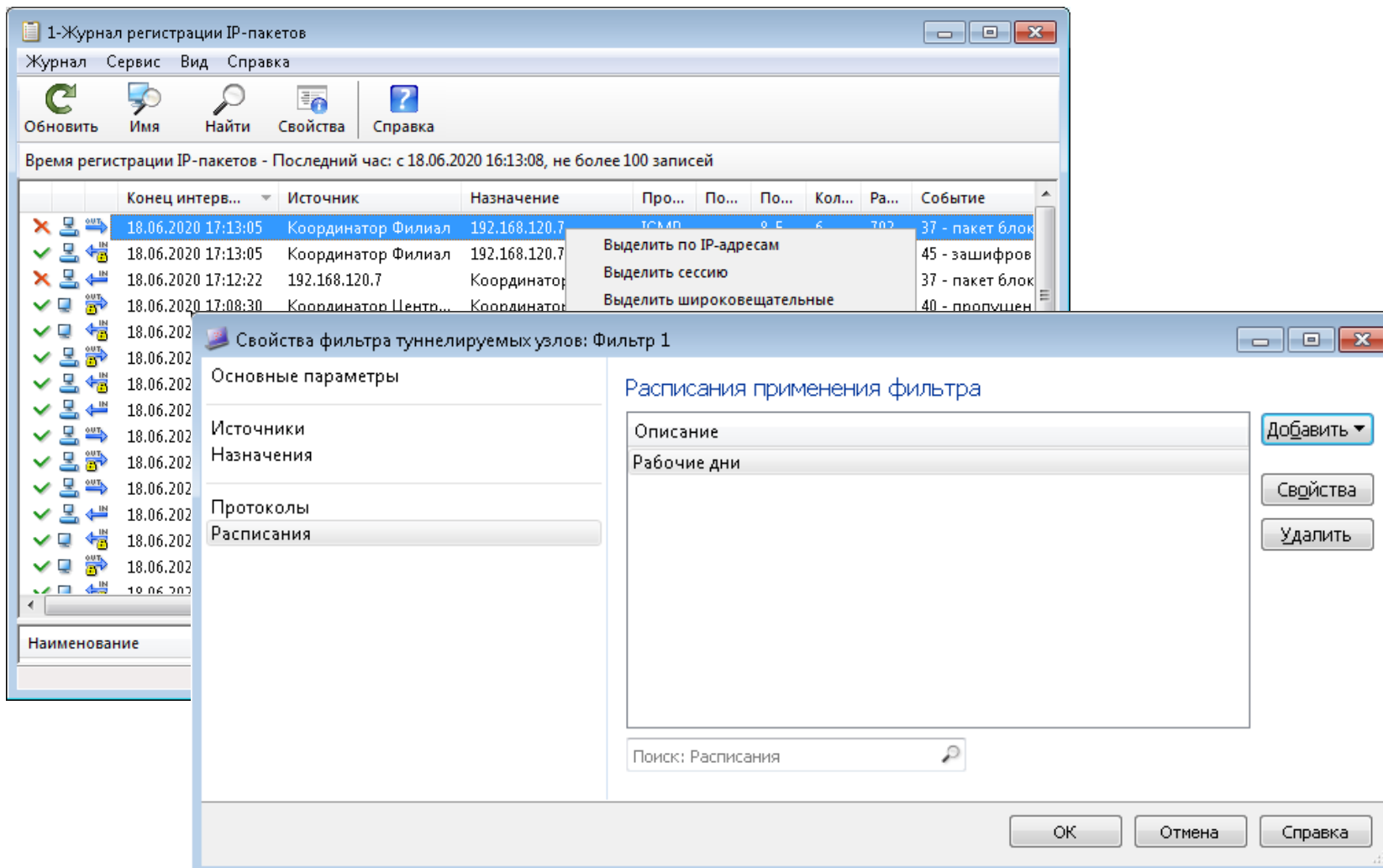
## Создание сетевого фильтра из журнала IP-пакетов



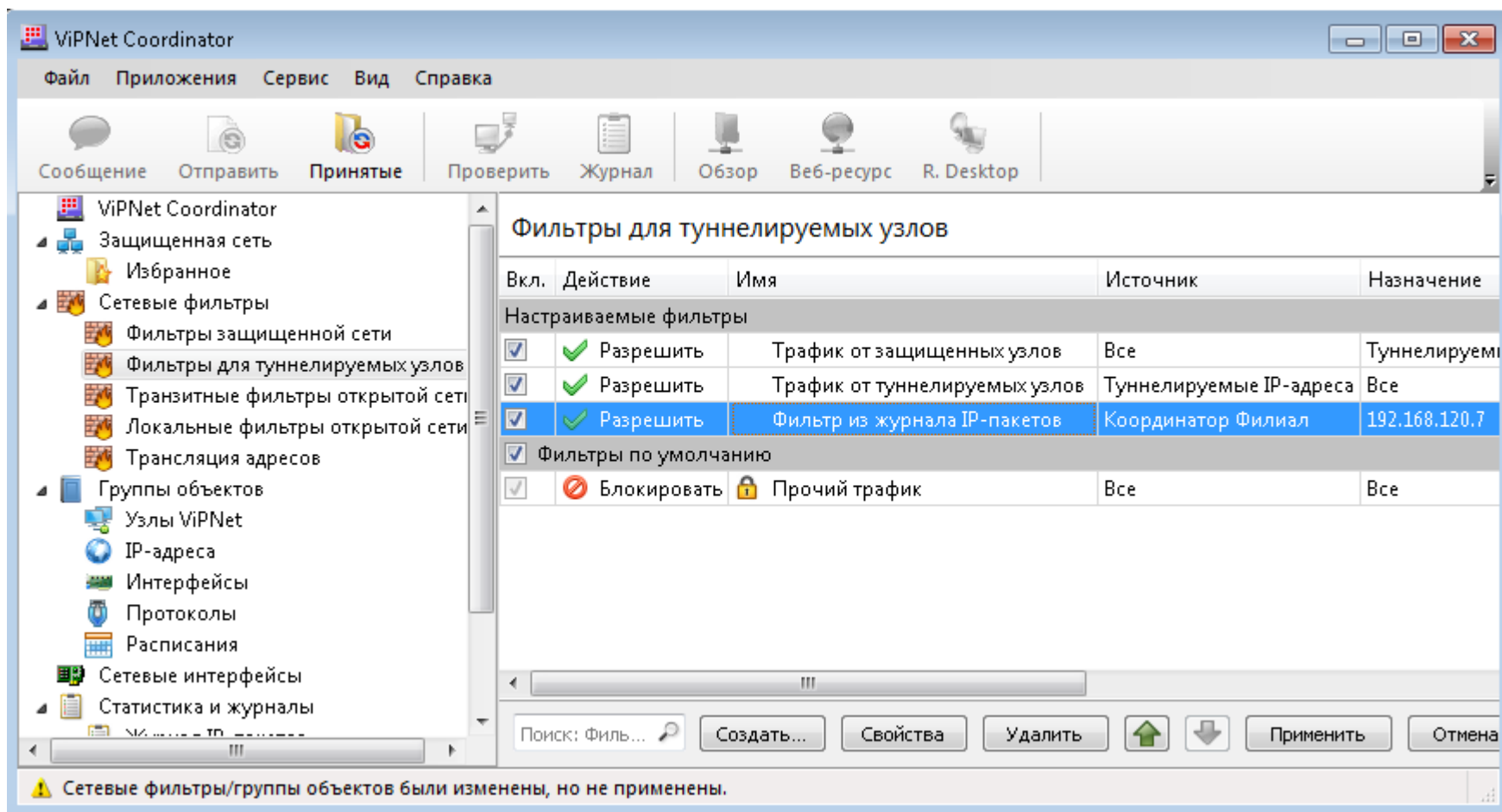
## Создание сетевого фильтра из журнала IP-пакетов



## Создание сетевого фильтра из журнала IP-пакетов



## Создание сетевого фильтра из журнала IP-пакетов

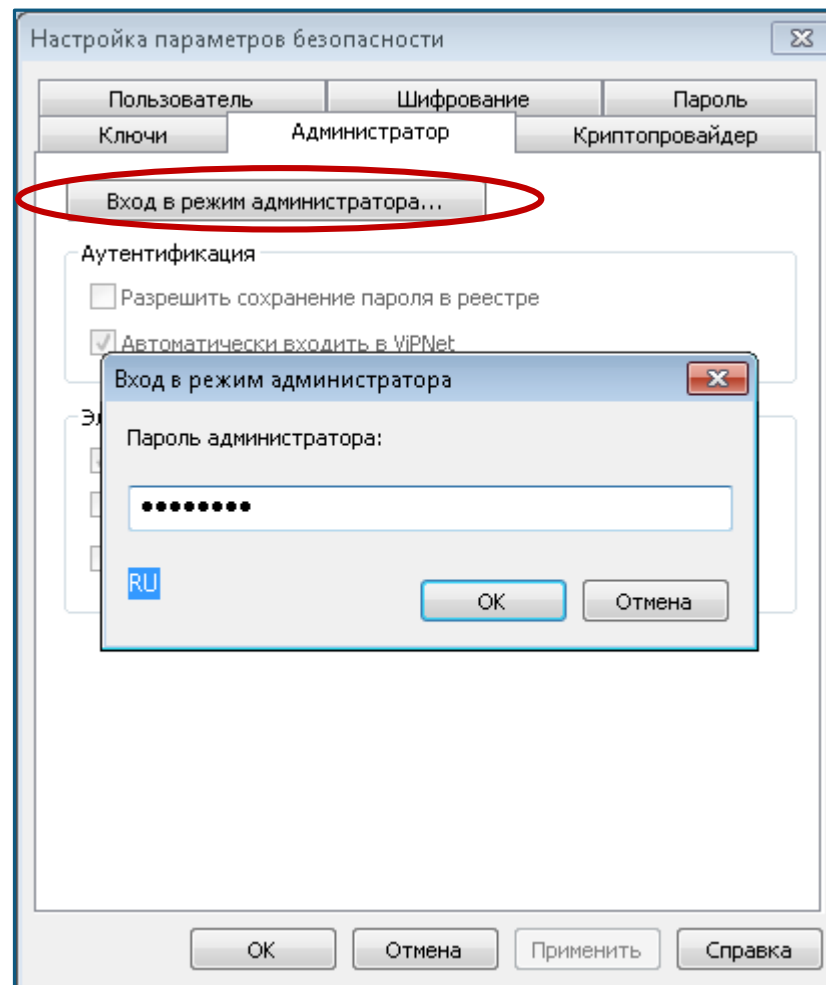
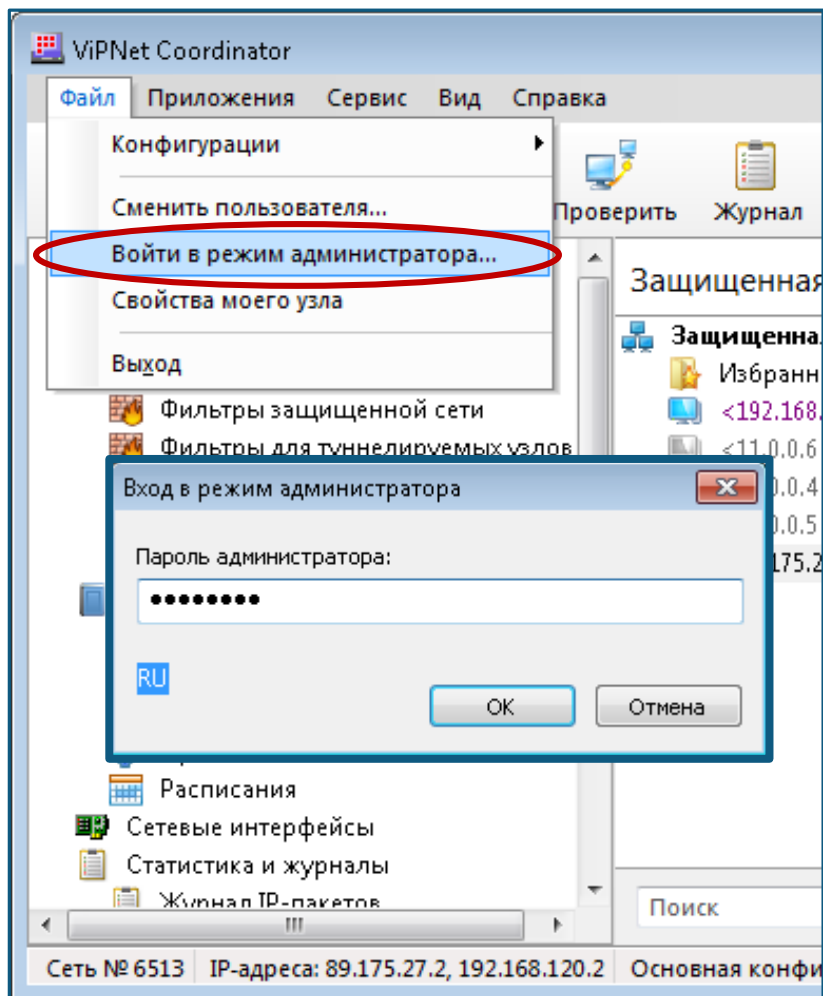


## Администратор сетевого узла

- 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

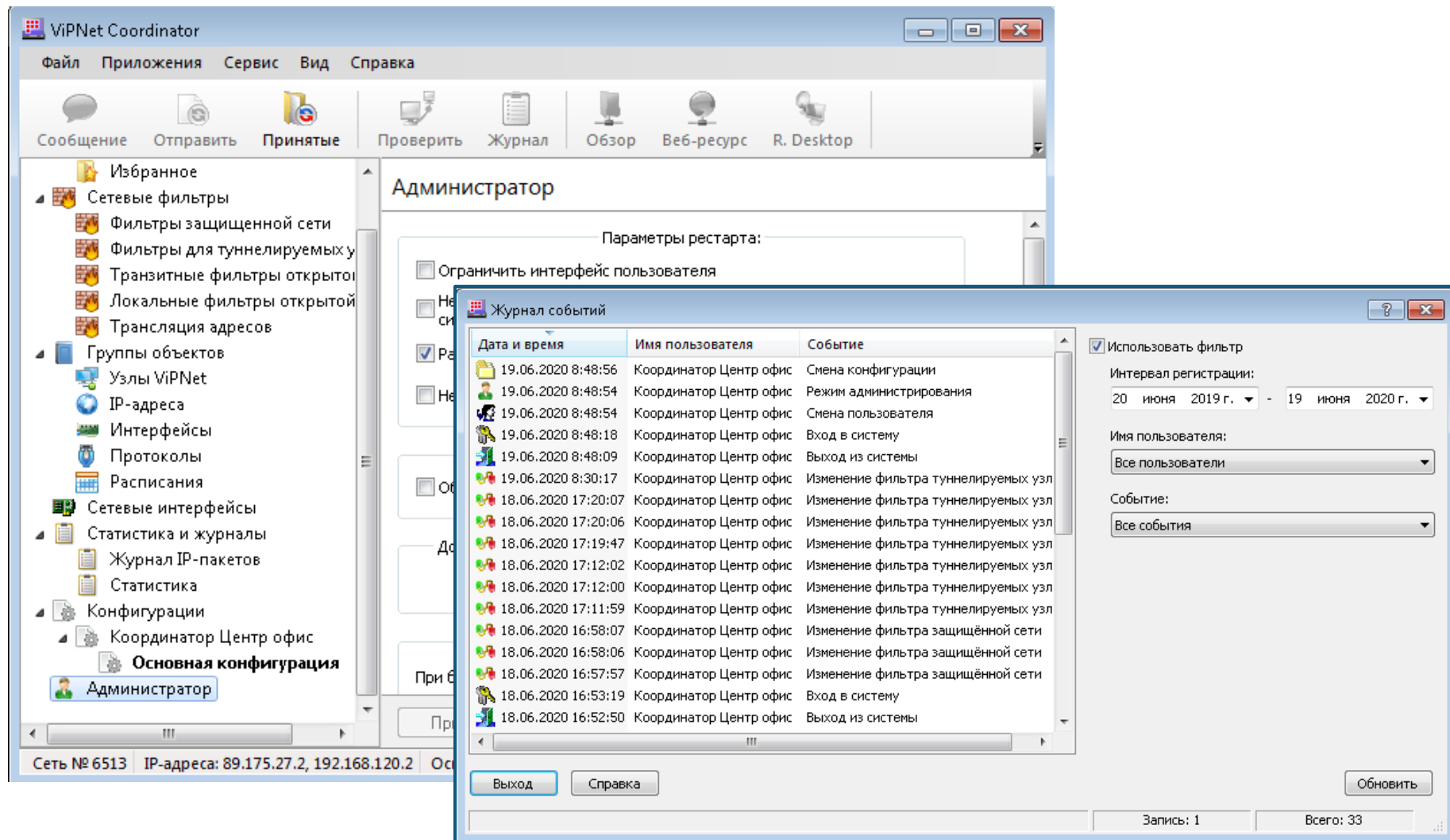


## Вход в режим администратор сетевого узла





## Просмотр журнала событий



The screenshot displays the VIPNet Coordinator application interface. The main window shows a tree view of network settings, including 'Сетевые фильтры' (Network filters), 'Группы объектов' (Object groups), 'Сетевые интерфейсы' (Network interfaces), 'Статистика и журналы' (Statistics and logs), and 'Конфигурации' (Configurations). The 'Администратор' (Administrator) configuration is selected.

The 'Журнал событий' (Event Log) window is open, showing a list of events. The table below represents the data shown in the event log:

Дата и время	Имя пользователя	Событие
19.06.2020 8:48:56	Координатор Центр офис	Смена конфигурации
19.06.2020 8:48:54	Координатор Центр офис	Режим администрирования
19.06.2020 8:48:54	Координатор Центр офис	Смена пользователя
19.06.2020 8:48:18	Координатор Центр офис	Вход в систему
19.06.2020 8:48:09	Координатор Центр офис	Выход из системы
19.06.2020 8:30:17	Координатор Центр офис	Изменение фильтра туннелируемых узл
18.06.2020 17:20:07	Координатор Центр офис	Изменение фильтра туннелируемых узл
18.06.2020 17:20:06	Координатор Центр офис	Изменение фильтра туннелируемых узл
18.06.2020 17:19:47	Координатор Центр офис	Изменение фильтра туннелируемых узл
18.06.2020 17:12:02	Координатор Центр офис	Изменение фильтра туннелируемых узл
18.06.2020 17:12:00	Координатор Центр офис	Изменение фильтра туннелируемых узл
18.06.2020 17:11:59	Координатор Центр офис	Изменение фильтра туннелируемых узл
18.06.2020 16:58:07	Координатор Центр офис	Изменение фильтра защищённой сети
18.06.2020 16:58:06	Координатор Центр офис	Изменение фильтра защищённой сети
18.06.2020 16:57:57	Координатор Центр офис	Изменение фильтра защищённой сети
18.06.2020 16:53:19	Координатор Центр офис	Вход в систему
18.06.2020 16:52:50	Координатор Центр офис	Выход из системы

The event log window also includes a filter section with the following settings:

- ☒ Использовать фильтр
- Интервал регистрации: 20 июня 2019 г. - 19 июня 2020 г.
- Имя пользователя: Все пользователи
- Событие: Все события

Buttons at the bottom of the event log window include 'Выход' (Exit), 'Справка' (Help), and 'Обновить' (Refresh). The status bar shows 'Запись: 1' (Record: 1) and 'Всего: 33' (Total: 33).

## Дополнительные настройки программы ViPNet Монитор

### Параметры рестарта:

- ☐ Ограничить интерфейс пользователя
- ☐ Не активизировать защиту IP-трафика при загрузке операционной системы
- ☒ Разрешить запуск монитора в удалённой сессии
- ☐ Не запускать монитор после входа в операционную систему

### Параметры ввода пароля:

- ☐ Обязательный ввод пароля при входе в операционную систему

### Допустимая разница между временами отправки и приема пакета:

120 (минуты)

### Блокировать компьютер:

- При бездействии пользователя в течение 15 (минут)
- ☒ При отключении устройства аутентификации

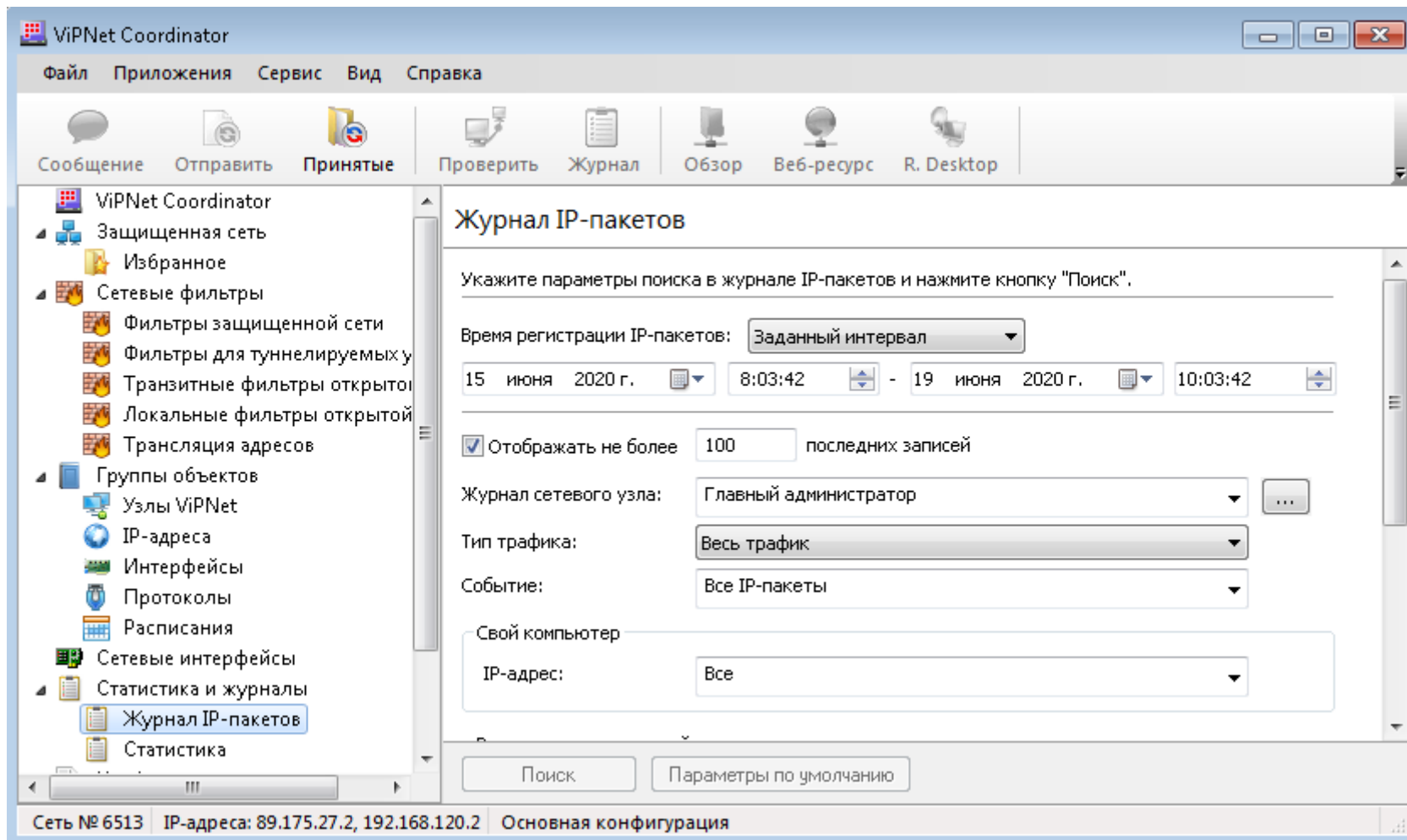
### Политики безопасности

- ☒ Применять политики безопасности

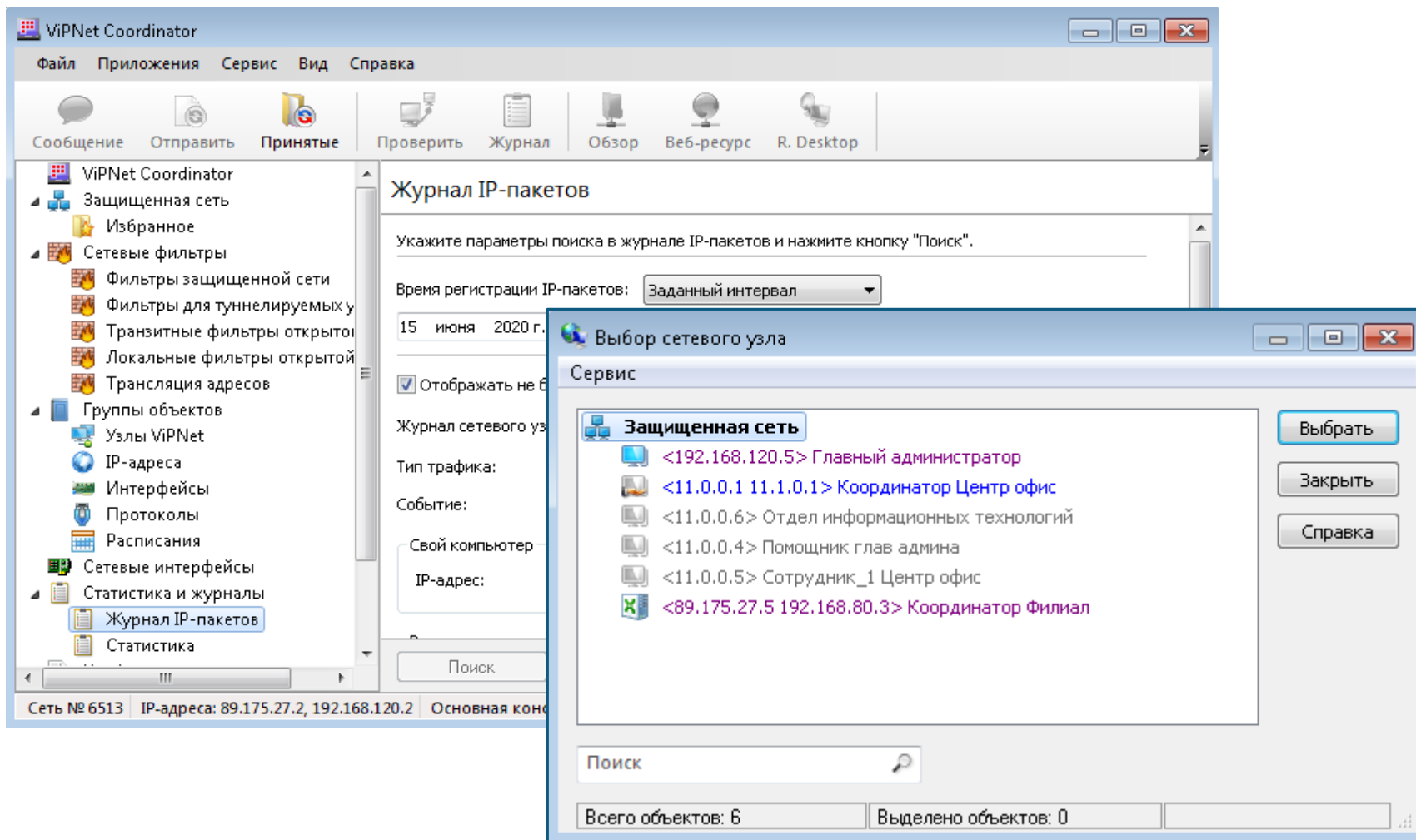
### Журнал событий Windows

- ☐ Дублировать записи о заблокированных IP-пакетах
- ☐ Дублировать записи об авторизованном изменении правил фильтрации
- ☐ Дублировать записи о несанкционированном изменении правил фильтрации

## Просмотр журнала IP-пакетов другого сетевого узла



## Просмотр журнала IP-пакетов другого сетевого узла



## Просмотр журнала IP-пакетов другого сетевого узла

The screenshot displays the ViPNet Coordinator application window. The left sidebar shows a tree view of the network configuration, with 'Журнал IP-пакетов' (IP Packet Log) selected under 'Статистика и журналы' (Statistics and Logs). The main window shows the '3-Журнал регистрации IP-пакетов (Координатор Филиал)' (3-IP Packet Registration Log (Coordinator Branch)) window. This window displays a table of IP packet registration data for the last 24 hours, showing 100 records.

Журнал регистрации IP-пакетов (Координатор Филиал)

Журнал Сервис Вид Справка

Обновить Имя Найти Свойства Справка

Время регистрации IP-пакетов - Последние 24 часа: с 18.06.2020 9:15:34, не более 100 записей

	Конец ...	Источник	Назначение	Про...	По...	По...	Кол...	Разм...	Событие
✓	19.06.2020...	Координатор Це...	Координатор Фи...	TCP	494...	2047	4	416	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Фи...	Координатор Це...	TCP	2047	494...	5	817	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Фи...	Координатор Це...	TCP	2047	494...	5	1668	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Це...	Координатор Фи...	TCP	494...	2047	5	268	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Це...	Координатор Фи...	TCP		2047	28	1216	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Фи...	Координатор Це...	TCP	2047		24	9616	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Фи...	Координатор Це...	UDP	2046	2046	14	2199	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Фи...	Координатор Це...	TCP	2047	494...	4	592	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Це...	Координатор Фи...	TCP	494...	2047	4	237	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Це...	Координатор Фи...	TCP	493...	2047	4	237	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Фи...	Координатор Це...	TCP	2047	493...	4	592	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Фи...	Координатор Це...	TCP	2047	493...	4	592	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Це...	Координатор Фи...	TCP	493...	2047	4	237	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Це...	Координатор Фи...	UDP	2046	2046	14	1907	40 - пропущен зашифрованный IP-п
✓	19.06.2020...	Координатор Це...	Координатор Фи...	TCP	5000	402	7	412	40 - пропущен зашифрованный IP-п

Размер: 0 байт      Запись: 0      Всего: 100

# Транспортный модуль ViPNet MFTP

## Транспортный модуль ViPNet MFTP :

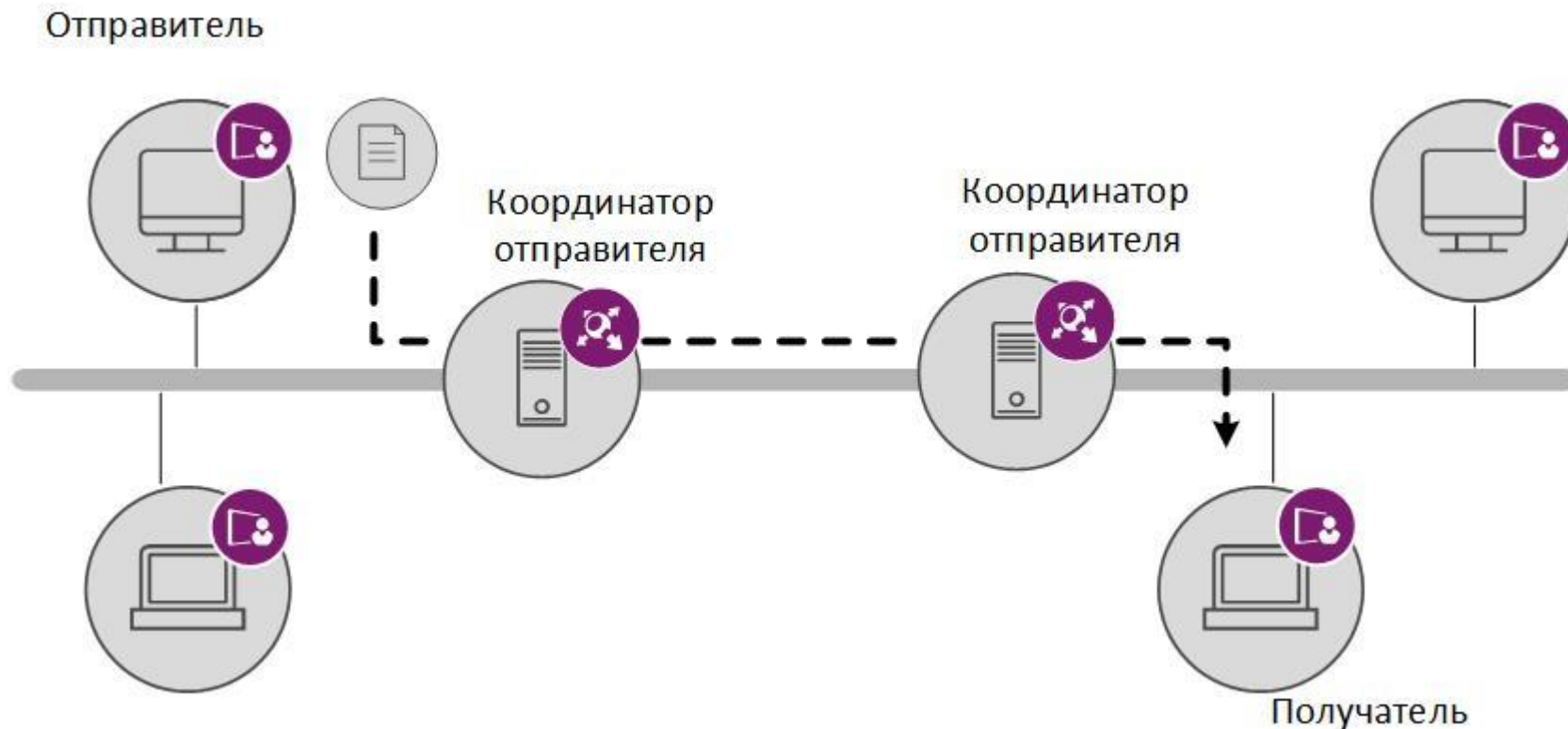
- Обеспечивает надежную и безопасную передачу транспортных конвертов между узлами сети ViPNet.
- Запускается вместе с ПО ViPNet, в состав которого входит.
- Устанавливается только в комплекте с другим ПО ViPNet.

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





## Принцип работы транспортного модуля





## Режимы работы транспортного модуля

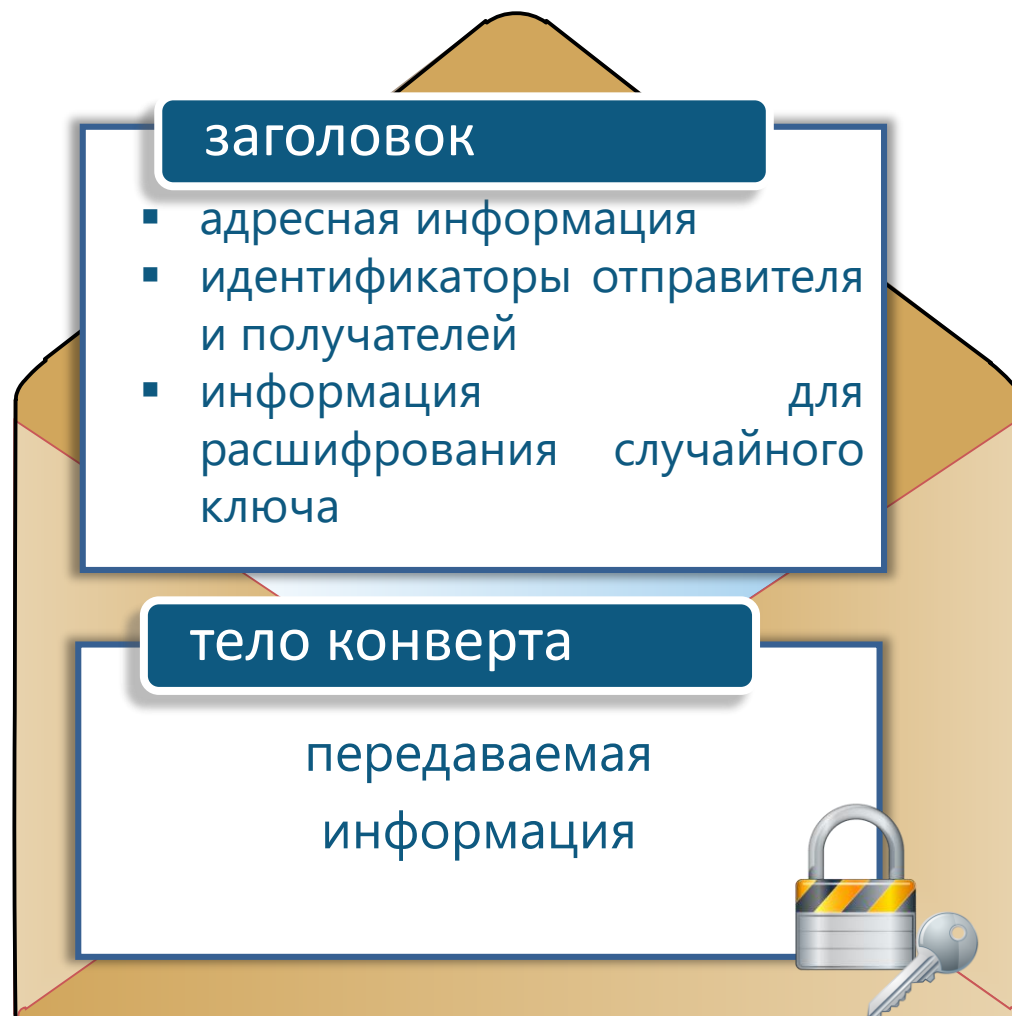
### серверный режим работы

- **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 клиентами, 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

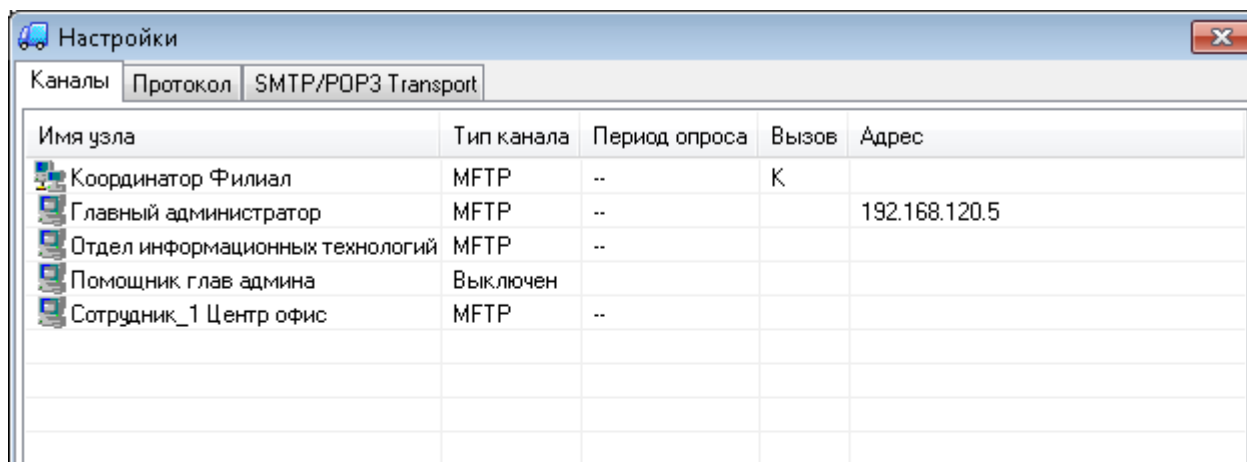
### транспортная квитанция

- файл, оповещающий отправителя о невозможности доставки конверта

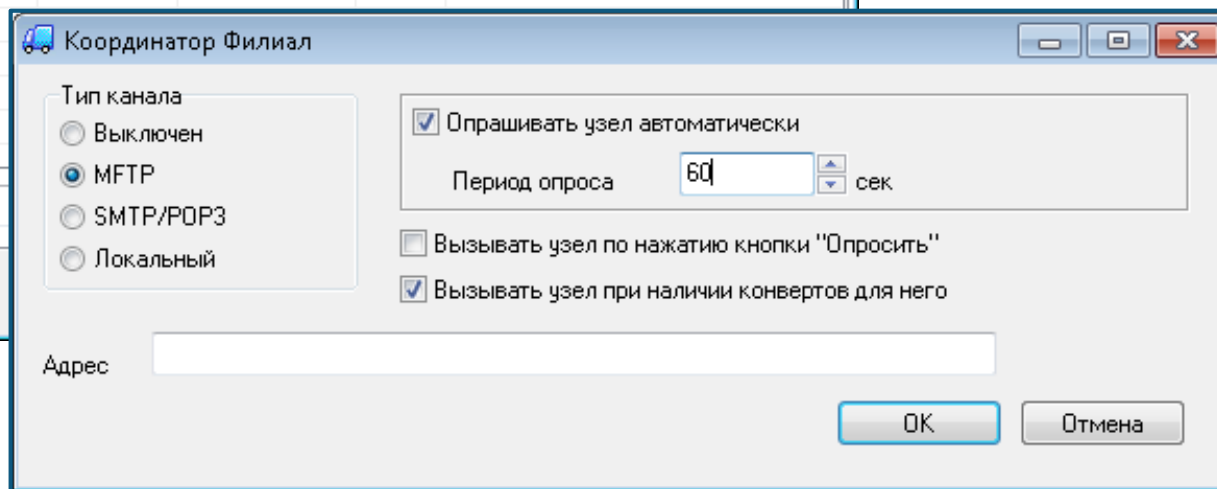
### служебный конверт

- 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 каналов передачи конвертов

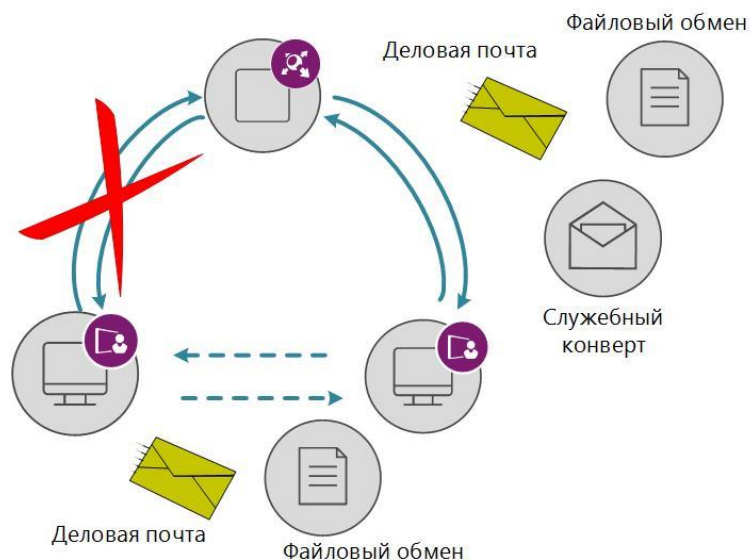


- Выключен
- MFTP
- SMTP/POP3
- Локальный



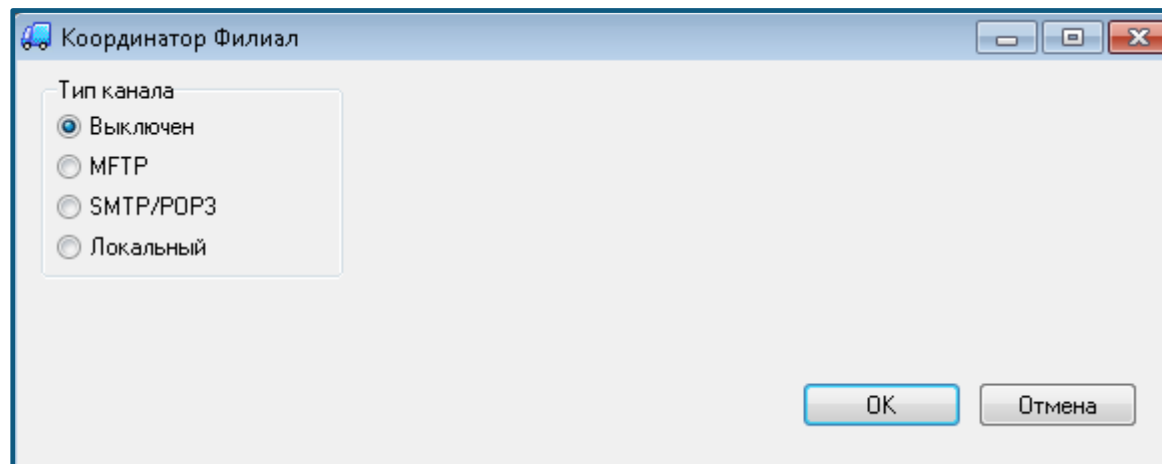
**тип канала «Выключен»**

- 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



## 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



## 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



## 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

Координатор Филиал

Тип канала

- ☐ Выключен
- ☒ MFTP
- ☐ SMTP/POP3
- ☐ Локальный

☒ Опрашивать узел автоматически

Период опроса 60 сек

☒ Вызывать узел по нажатию кнопки "Опросить"

☒ Вызывать узел при наличии конвертов для него

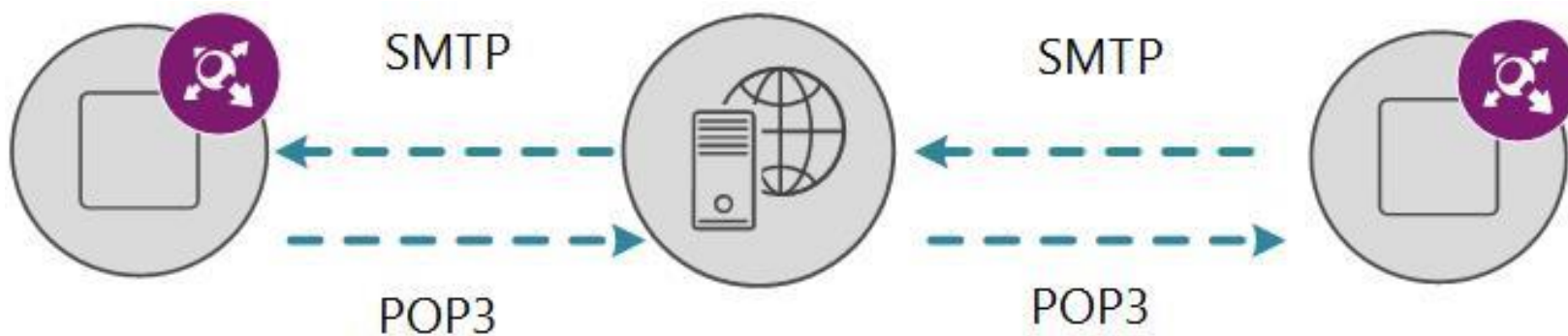
Адрес 89.175.27.3

OK Отмена



## 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



## 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

Настройки

Каналы | Протокол | SMTP/POP3 Transport

Сервер исходящих сообщений (SMTP)

Адрес сервера: mail

Порт: 25

Адрес электронной почты: petrov@office.ru

☒ Сервер использует авторизацию Настройка ...

☒ Разбивать письма на фрагменты размера: 30 МБ

Сервер входящих сообщений (POP3)

Адрес сервера: pop3

Порт: 110

Период опроса: 1 мин.

Учётная запись: ivanov@company.ru

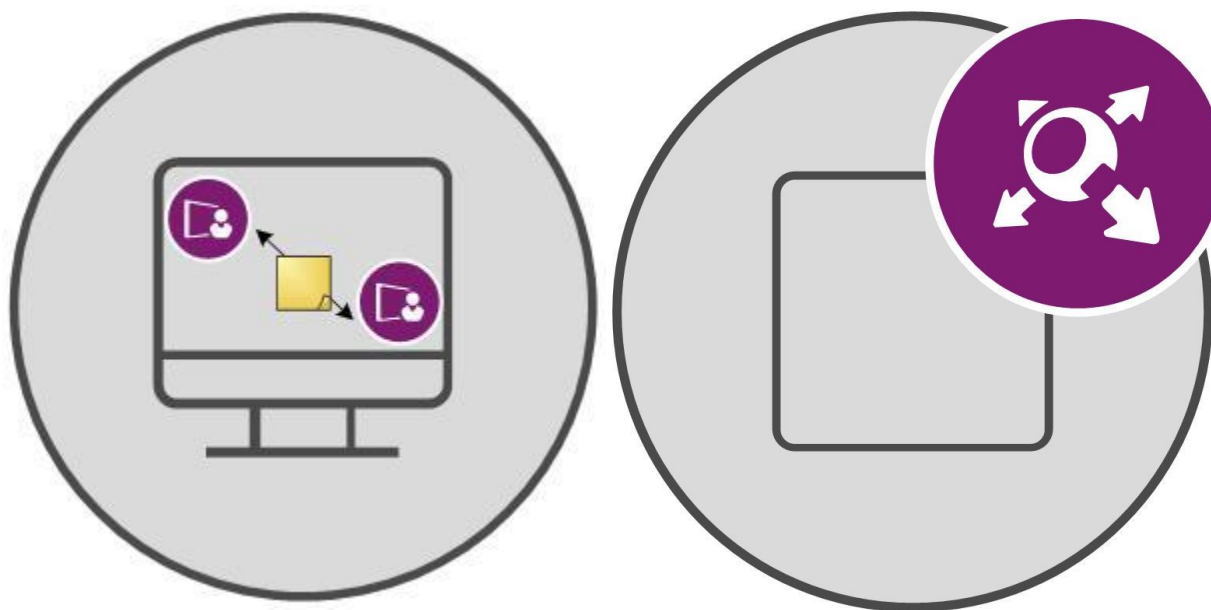
Пароль: .....

☒ Запомнить пароль

OK Отмена

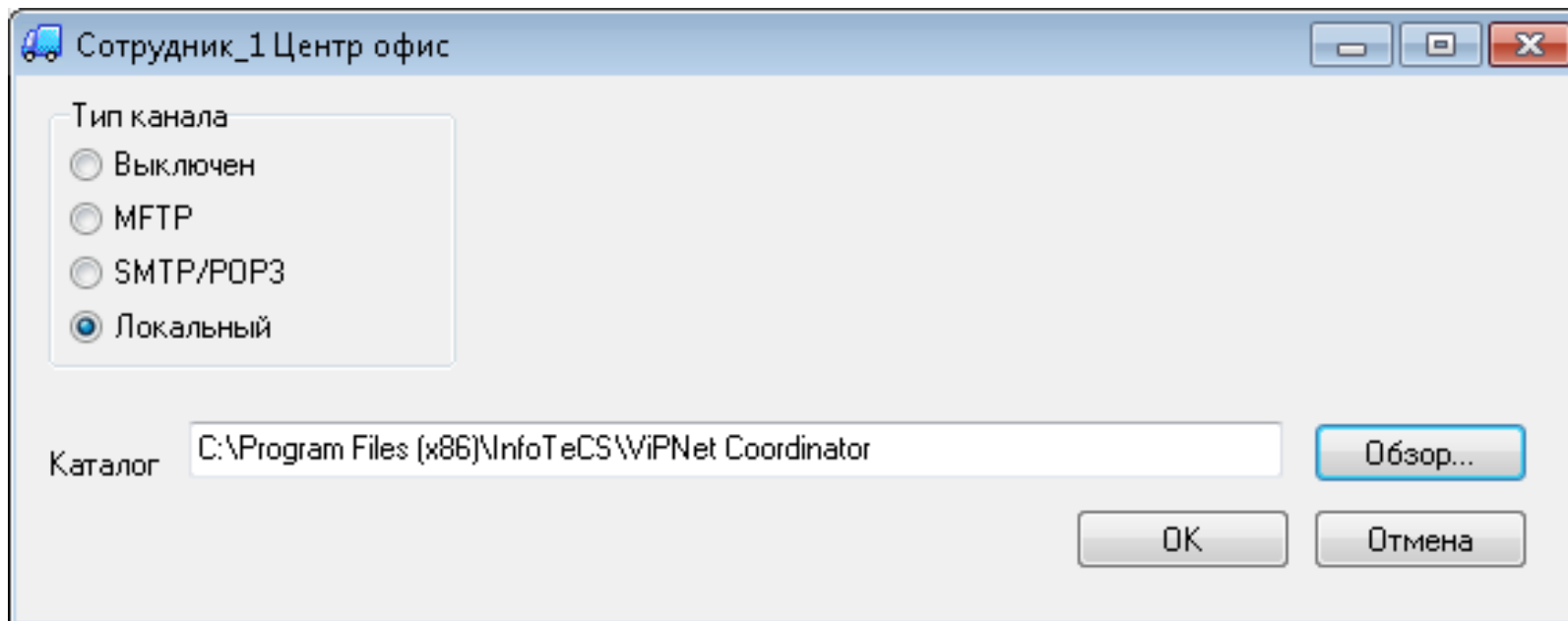
## тип канала «Локальный»

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

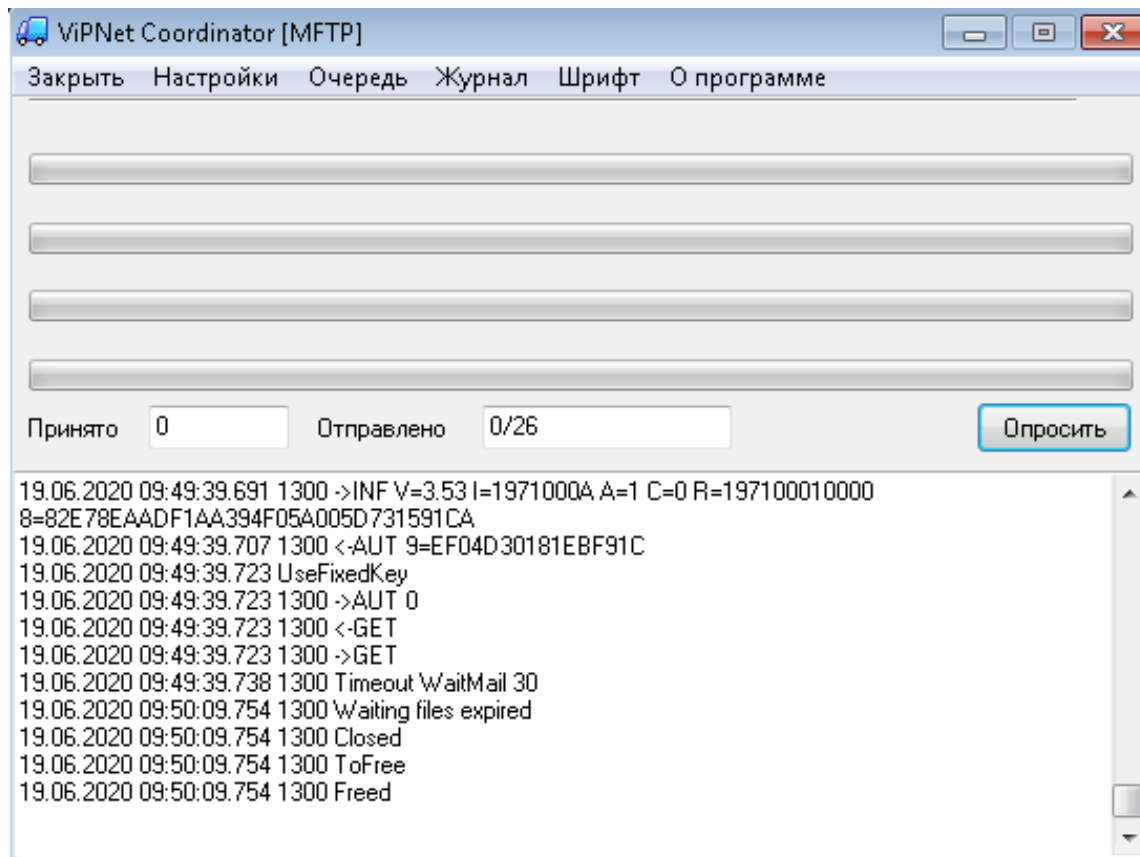


## тип канала «Локальный»

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



## Работа с очередью и журналом конвертов



## Работа с очередью и журналом конвертов

ViPNet Coordinator [MFTP]

Заккрыть Настройки Очередь Журнал Шрифт О программе

Принято 0

19.06.2020 09:49:39.691  
8=82E78EADF1AA394F  
19.06.2020 09:49:39.707  
19.06.2020 09:49:39.723  
19.06.2020 09:49:39.723  
19.06.2020 09:49:39.723  
19.06.2020 09:49:39.738  
19.06.2020 09:50:09.754  
19.06.2020 09:50:09.754  
19.06.2020 09:50:09.754  
19.06.2020 09:50:09.754

Имя конверта \*

Описание конверта \*

Отправитель

Получатель

Найти конверты

☐ в интервале дат

от ☒ 19.06.20

по ☒ 19.06.20

☒ за последние 10

OK

Журнал конвертов

Имя конверта	Отправитель	Получатель	Дата/Время	Событие	Длина	Оп...	Задача	КБ/сек
~!L&5%FZ.FU#	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Отправлен	778590		Файловый обм...	12557
~!L&5%FZ.FU#	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Принят	778590		Файловый обм...	12358
~95RQA9.19P	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Отправлен	880149		Файловый обм...	11283
~95RQA9.19P	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Принят	880149		Файловый обм...	13970
~S59U_DG.21J	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Отправлен	755		Файловый обм...	47
~S59U_DG.21J	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Принят	755		Файловый обм...	
M@TXAE%3.C...	Главный адм...	Координатор Фил...	19.06.2020 09:1...	Отправлен	2343		Управление	
m@txae%3.ctl	Главный адм...	Координатор Фил...	19.06.2020 09:1...	Принят	2343		Управление	146
MJ300AZI.CTL	Главный адм...	Координатор Фил...	18.06.2020 16:5...	Отправлен	2792		Управление	
mj300azi.ctl	Главный адм...	Координатор Фил...	18.06.2020 16:5...	Принят	2792		Управление	
M\$1}A6QI.CTL	Главный адм...	Координатор Фил...	18.06.2020 13:0...	Отправлен	2802		Управление	
m\$1}a6qi.ctl	Главный адм...	Координатор Фил...	18.06.2020 13:0...	Принят	2802		Управление	
M79IU6BH.CTL	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	3317		Управление	
M}SK#271.CTL	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	2777		Управление	
M1QU67H.CTL	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	2740		Управление	
MX@TU@{K.C...	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	2740		Управление	
M\$55U&5K.CTL	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	2736		Управление	
M9@TU@{K.C...	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	2285		Управление	
MNK5U&9K.CTL	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	2285		Управление	
MNUQU6CH.C...	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	1729		Управление	
MT7RA&W}.CTL	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	1444		Управление	96

Найдено записей: 30

## Работа с очередью и журналом конвертов

ViPNet Coordinator [MFTP]

Заккрыть Настройки Очередь Журнал Шрифт О программе

Принято 0

19.06.2020 09:49:39.691  
8=82E78EADF1AA394F  
19.06.2020 09:49:39.707  
19.06.2020 09:49:39.723  
19.06.2020 09:49:39.723  
19.06.2020 09:49:39.723  
19.06.2020 09:49:39.723  
19.06.2020 09:49:39.738  
19.06.2020 09:50:09.754  
19.06.2020 09:50:09.754  
19.06.2020 09:50:09.754  
19.06.2020 09:50:09.754

Имя конверта \*

Описание конверта \*

Отправитель

Получатель

Найти конверты

☐ в интервале дат

от ☒ 19.06.20

по ☒ 19.06.20

☒ за последние 10

OK

Поиск конвертов в журнале

Журнал конвертов

Имя конверта	Отправитель	Получатель	Дата/Время	Событие	Длина	Оп...	Задача	КБ/сек
~!L&5%FZ.FU#	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Отправлен	778590		Файловый обм...	12557
~!L&5%FZ.FU#	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Принят	778590		Файловый обм...	12358
~95RQA9.19P	Главный адм...	Координатор Фил...	19.06.2020 10:0...	Отправлен	880149		Файловый обм...	11283
~95RQA9.19P	Главный адм...						Файловый обм...	13970
~S59U_DG.21J	Главный адм...						Файловый обм...	47
~S59U_DG.21J	Главный адм...						Файловый обм...	
M@TXAE%3.C...	Главный адм...						Управление	
m@txae%3.ctl	Главный адм...						Управление	146
MJ30QA.ZI.CTL	Главный адм...						Управление	
mj30Qazi.ctl	Главный адм...						Управление	
M\$1}A6QI.CTL	Главный адм...						Управление	
m\$1}a6qi.ctl	Главный адм...						Управление	
M79IU68H.CTL	Главный адм...						Управление	
M}SK#271.CTL	Главный адм...						Управление	
M1QU67H.CTL	Главный адм...						Управление	
MX@TU@{K.C...	Главный адм...						Управление	
M\$S5U&5K.CTL	Главный адм...						Управление	
M9@TU@{K...	Главный адм...						Управление	
MNK5U&9K.CTL	Главный адм...						Управление	
MNUQU6CH.C...	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	1729		Управление	
MT7RA@W}.CTL	Главный адм...	Координатор Фил...	18.06.2020 12:4...	Отправлен	1444		Управление	96

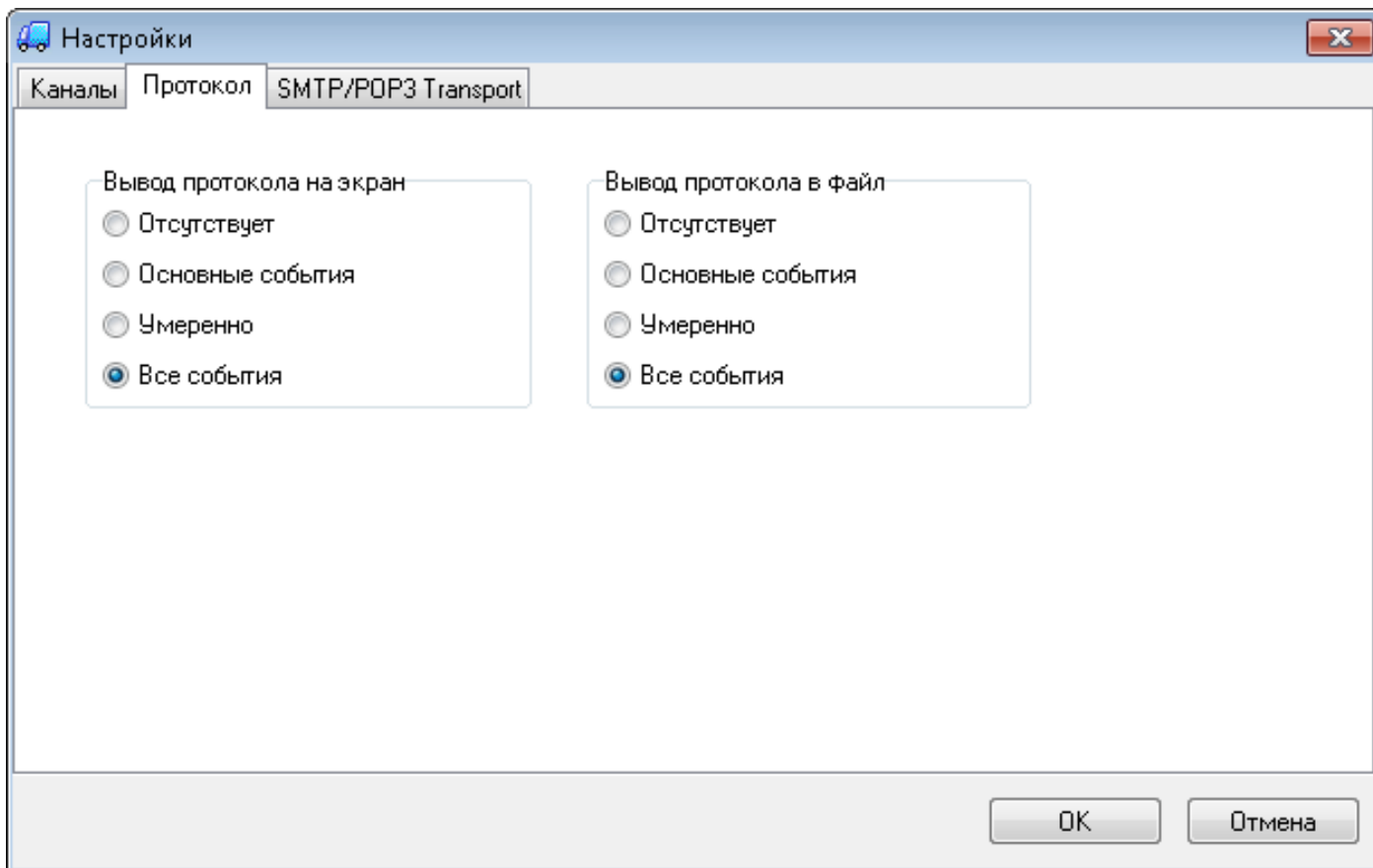
Найдено записей: 30

Информация

Имя конверта=m@txae%3.ctl  
Отправитель=Главный администратор  
Получатель=Координатор Филиал  
Дата/Время=19.06.2020 09:11:51.589  
Событие=Принят  
Длина=2343  
Описание=  
Задача=Управление

OK

## Настройка отображения журнала событий





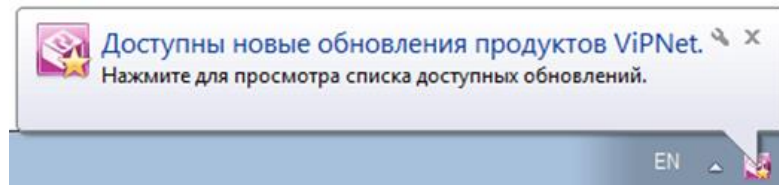
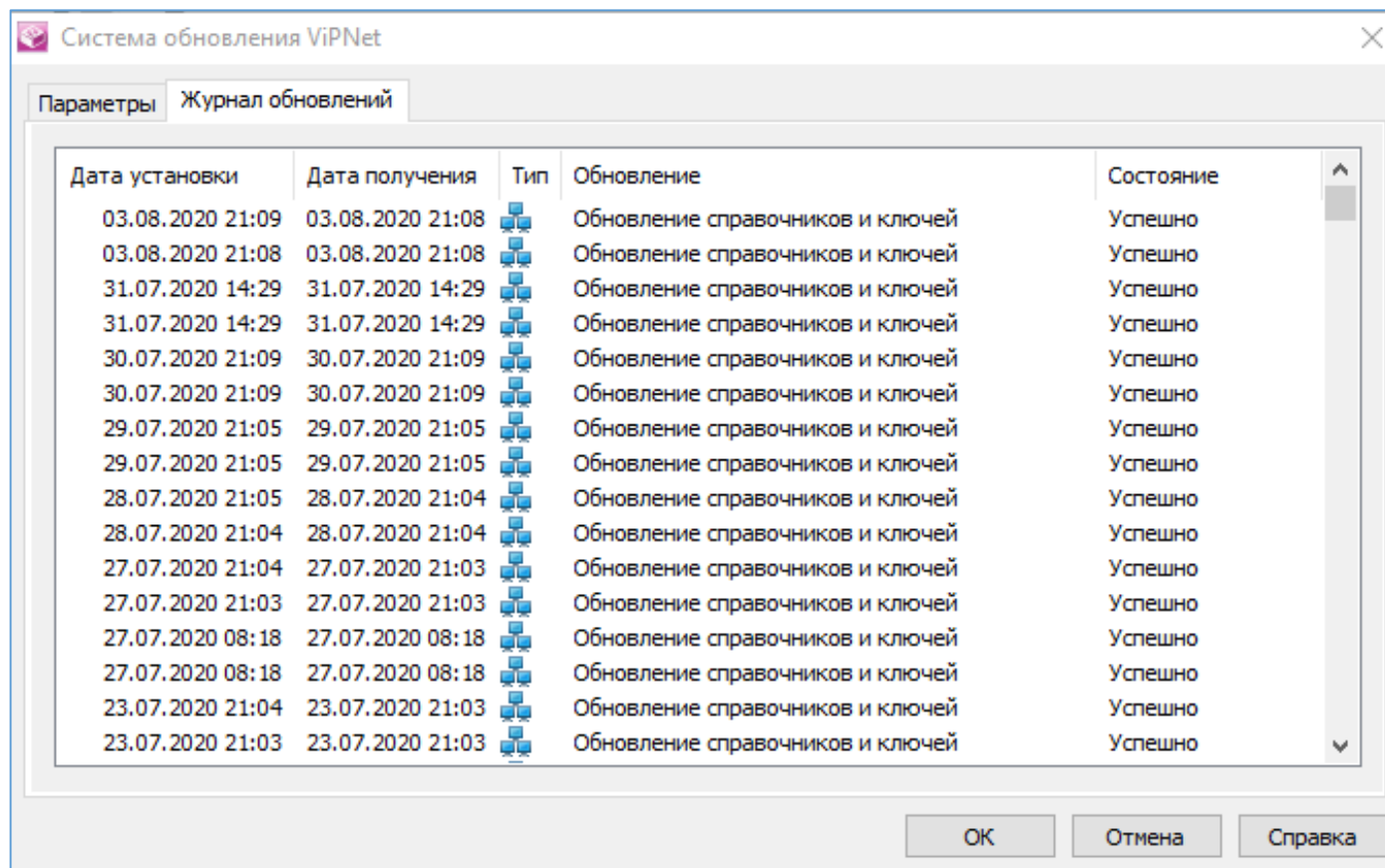
# Система обновлений ViPNet

## Система обновления ViPNet :

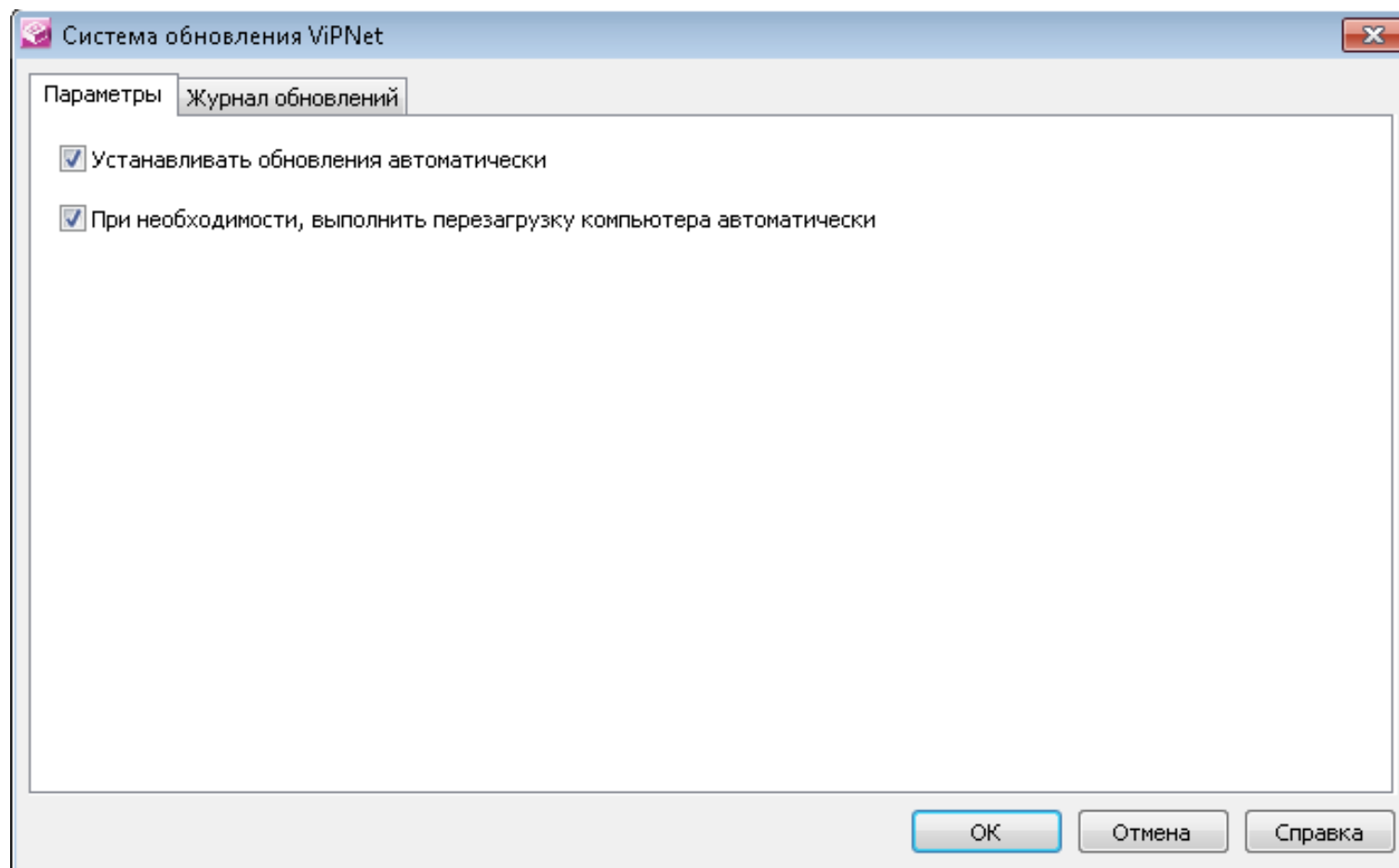
- **отвечает за получение и установку обновлений следующих типов:**
  - обновления ПО ViPNet Coordinator, полученные из программы ViPNet Administrator
  - обновления справочников и ключей, полученные из программы ViPNet Administrator
  - обновления политик безопасности, полученные из программы ViPNet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



## Настройка системы обновлений



## Настройка системы обновлений



# ViPNet StateWatcher

## ViPNet StateWatcher:

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



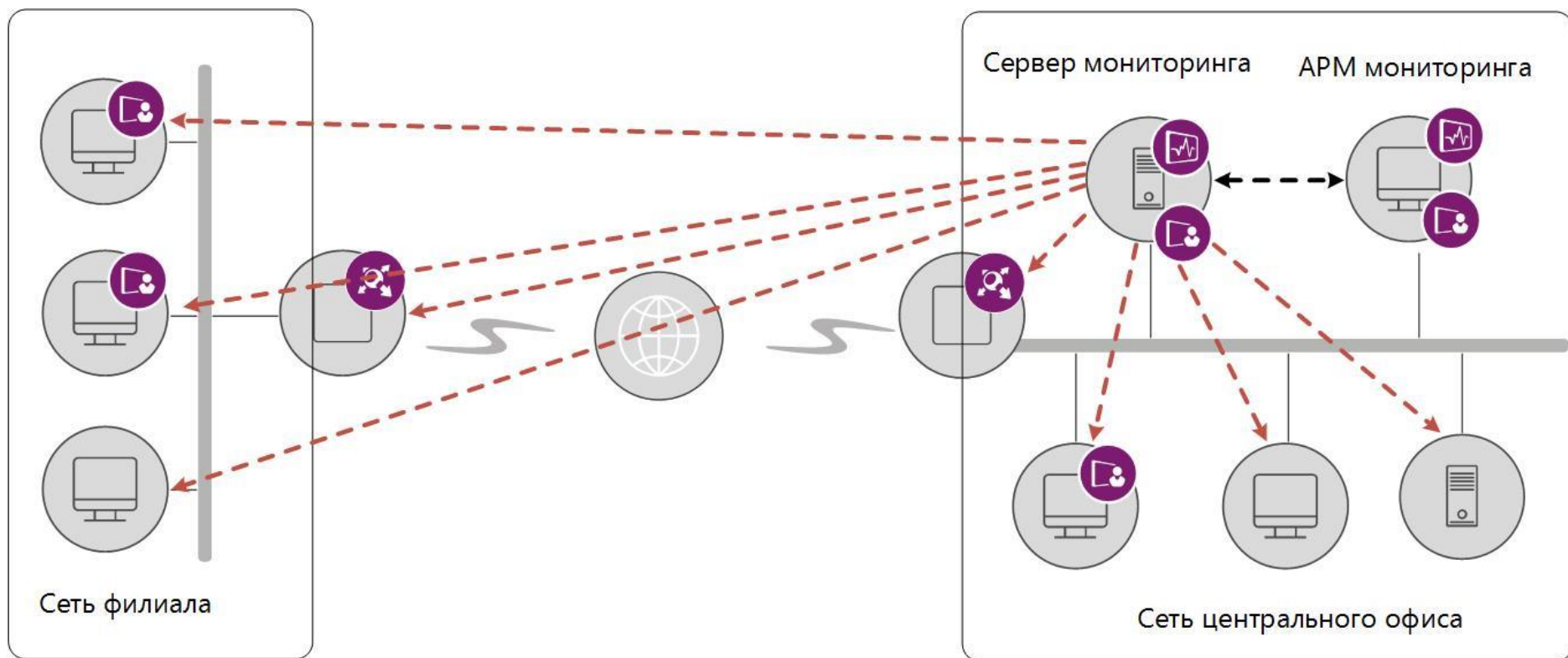
## Функции ViPNet StateWatcher

- 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.





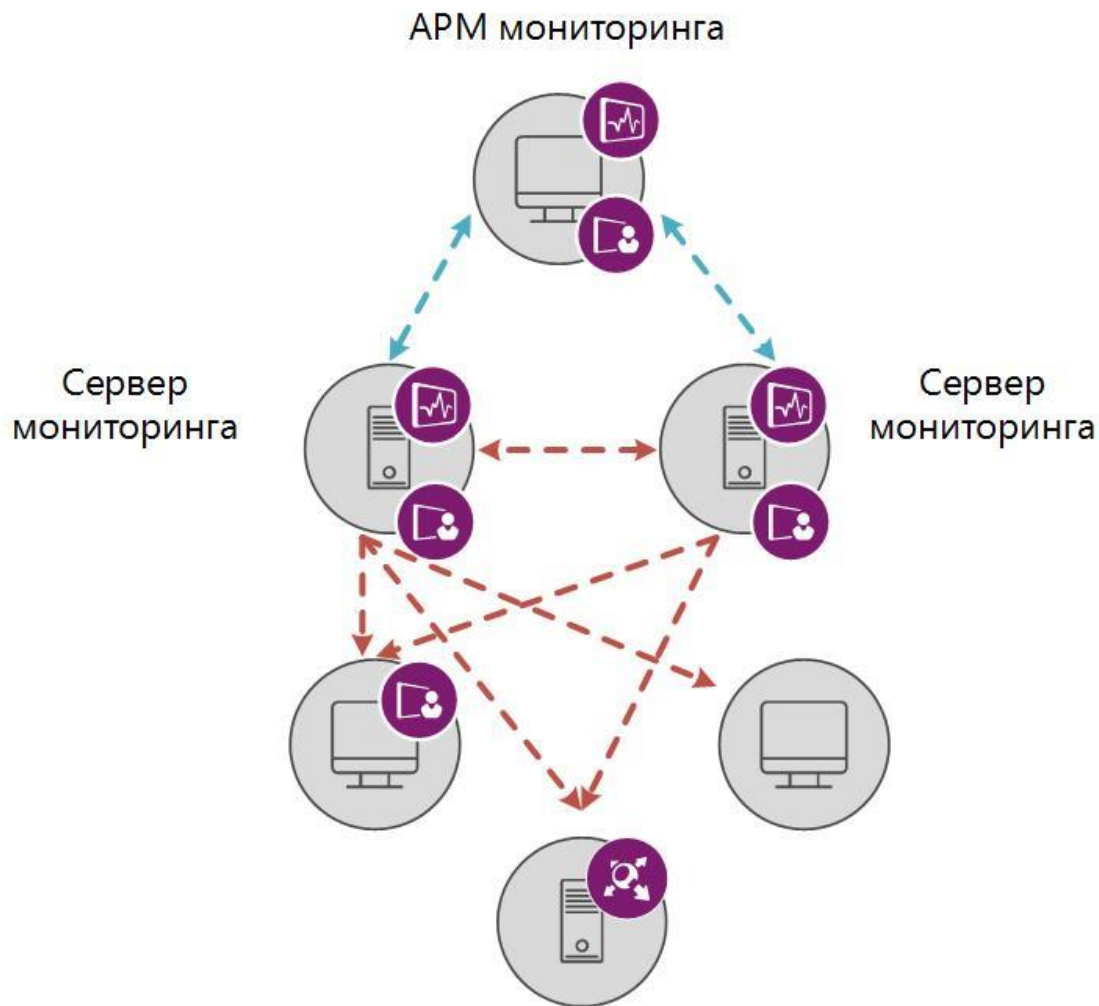
## Архитектура ViPNet StateWatcher



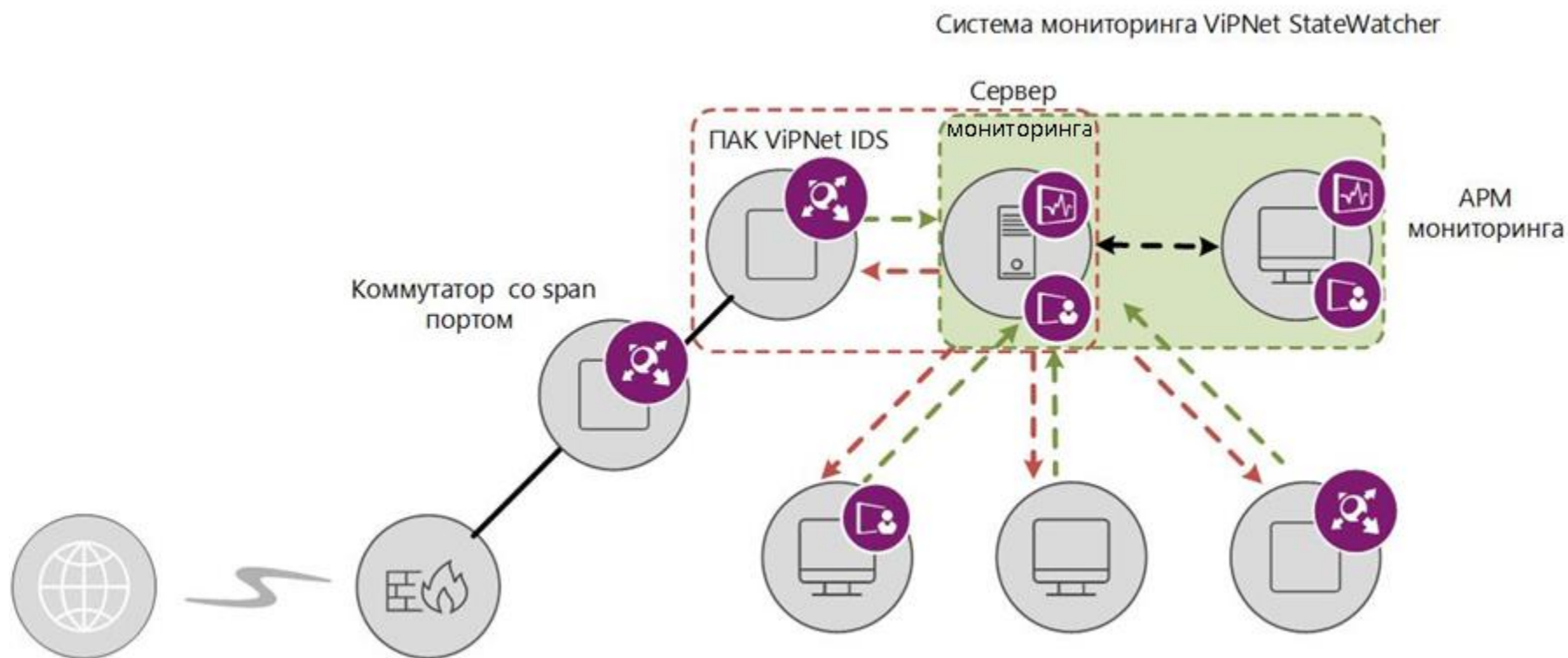


## Архитектура ViPNet StateWatcher

- *организация перекрестного мониторинга*



## Взаимодействие с ViPNet IDS



# Программно-аппаратные комплексы ViPNet

## 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 KB.
- 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** - промышленные шлюзы безопасности с поддержкой промышленных протоколов, обеспечивающие защиту каналов связи и сетевое экранирование
- 5. И др.





**ViPNet Coordinator HW-VA**



**ViPNet Coordinator HW100**



**ViPNet Coordinator HW1000**



**ViPNet Coordinator HW2000**



**ViPNet Coordinator HW5000**



**ViPNet Coordinator HW-VPNМ**

- 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.





- 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



- 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



- Семейство шлюзов безопасности в составе продуктовой линейки ViPNet Network Security с повышенным уровнем безопасности класса KB.
- 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.

- 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 пользователей к предоставляемым организацией ресурсам и сервисам.



Сертификат соответствия ФСБ России

Сертификат соответствия ФСБ России

- 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 узлам, защиты соединений между корпоративной сетью и удаленными узлами, защиты от атак.



- Сетевой шлюз безопасности в промышленном 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 промышленной сети, промышленной 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 промышленной сети в Интернет.*
- ✓ *Защищенный удаленный доступ в промышленную 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*



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.

# Спасибо за внимание!

## Вопросы?

НОЧУ ДПО ЦПК «Учебный центр «ИнфоТеКС»  
[education@infotecs.ru](mailto:education@infotecs.ru)

ОАО «ИнфоТеКС», Москва  
(495) 737-61-92  
[www.infotecs.ru](http://www.infotecs.ru)