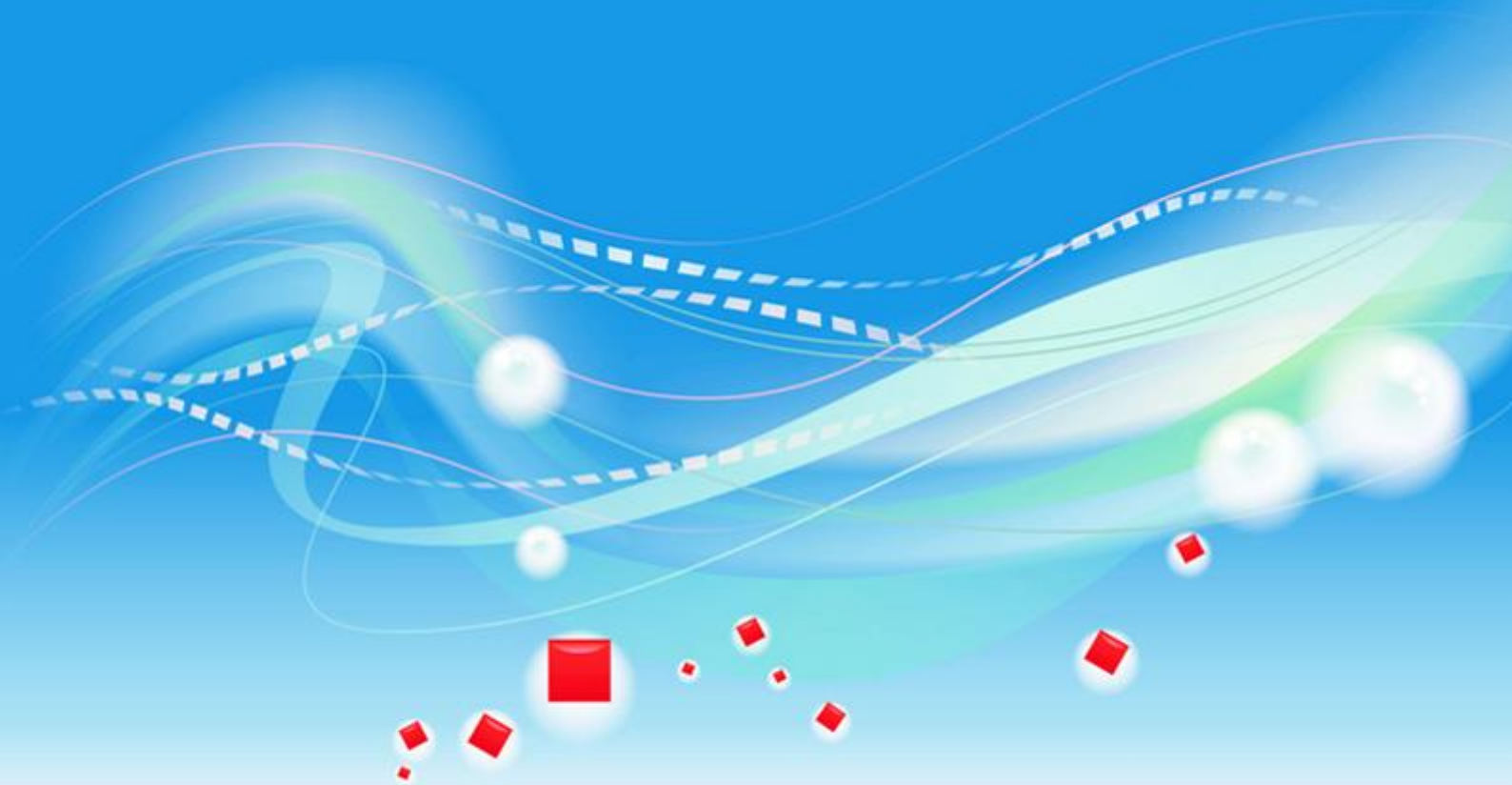


ViPNet Coordinator Монитор 4.2

Руководство администратора

ViPNet Virtual Private Network

infotecs

ФРКЕ.00110-03 32 01

ОАО «ИнфоТеКС»

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

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

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

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В документе содержится подробное описание основного компонента программы ViPNet Coordinator — ViPNet Монитор, его функций и назначения. Также документ содержит информацию, необходимую для настройки и использования ПО ViPNet Coordinator.

Примечание. В данном документе возможности программы ViPNet Монитор описаны с точки зрения пользователя, полномочия которого не ограничены. Если для вас недоступны какие-либо функции или настройки программы, обратитесь к администратору вашей сети ViPNet.

Прежде чем приступить к изучению этого руководства, рекомендуется ознакомиться с документом по развертыванию сети ViPNet, в котором приведена общая концепция построения сети ViPNet, описано назначение всех возможных видов узлов сети, даны рекомендации и краткий пошаговый сценарий по развертыванию сети ViPNet.

Для кого предназначен документ

Данное руководство предназначено для системных администраторов, отвечающих за установку, настройку и эксплуатацию ПО ViPNet Coordinator.

Предполагается, что администратор обладает знаниями и опытом в области сетевых технологий, достаточными для развертывания локальной сети, умеет устанавливать и настраивать серверные операционные системы, а также производить настройку межсетевых экранов.

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.

Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

О программе

Назначение ПО ViPNet Coordinator

Программное обеспечение ViPNet Coordinator входит в состав пакетов ViPNet CUSTOM и ViPNet VPN. ПО ViPNet Coordinator устанавливается на компьютеры, которые играют роль серверов в защищенной сети ViPNet (см. «Функции координатора в защищенной сети ViPNet» на стр. 32). Функциональность ViPNet Coordinator складывается из возможностей его отдельных модулей.

Состав ПО ViPNet Coordinator

ViPNet Coordinator состоит из следующих компонентов:

- ViPNet-драйвер (низкоуровневый драйвер сетевой защиты).
- Транспортный модуль ViPNet MFTP.
- Программа ViPNet Монитор — является графическим интерфейсом для управления ViPNet-драйвером, обеспечивает ведение журнала событий в системе, а также набор коммуникационных и других функций.
- Программа ViPNet Контроль приложений (при наличии лицензии).
- Криптопровайдер ViPNet CSP.

Примечание. В состав ViPNet Coordinator не включается программа ViPNet Деловая почта.

ViPNet-драйвер

ViPNet-драйвер (см. «Принцип работы ViPNet-драйвера» на стр. 29) — это низкоуровневый драйвер сетевой защиты, осуществляющий шифрование и фильтрацию IP-трафика. ViPNet-драйвер взаимодействует непосредственно с драйверами сетевых интерфейсов компьютера (реальных или их эмулируемых), что обеспечивает независимость программы от операционной системы и ее недокументированных возможностей. ViPNet-драйвер перехватывает и контролирует весь входящий и исходящий IP-трафик компьютера.

Одна из важнейших функций драйвера — эффективный контроль IP-трафика во время загрузки операционной системы. В ОС Windows для инициализации загрузки компьютера используется только одна служба. Инициализация ViPNet-драйвера и ключей шифрования ViPNet выполняется перед входом пользователя в Windows, то есть до инициализации остальных служб и драйверов операционной системы.

В результате ViPNet-драйвер первым получает контроль над стеком протоколов TCP/IP. К моменту инициализации драйверов сетевых интерфейсов ViPNet-драйвер подготовлен к шифрованию и фильтрации трафика, тем самым обеспечивается защищенное соединение с контроллером домена, контроль сетевой активности запущенных на компьютере приложений и блокирование нежелательных пакетов извне. В момент загрузки операционной системы ПО ViPNet проверяет собственные контрольные суммы, гарантирующие целостность программного обеспечения, наборов ключей и списка приложений, которым разрешена сетевая активность.

ViPNet Монитор

Основной функцией программы ViPNet Монитор является настройка различных параметров ViPNet-драйвера (см. «Принцип работы ViPNet-драйвера» на стр. 29) и запись событий, возникающих в процессе обработки трафика драйвером, в журнал регистрации IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 274). Если выгрузить программу ViPNet Монитор из памяти компьютера, ViPNet-драйвер продолжит работу и будет обеспечивать безопасность компьютера, но в журнале регистрации IP-пакетов может отсутствовать информация о трафике, обработанном драйвером при закрытой программе ViPNet Монитор (ViPNet-драйвер может хранить в памяти не более 10000 записей журнала).

На компьютере программа ViPNet Монитор:

- Позволяет настраивать параметры встроенного сетевого экрана (см. «Интегрированный сетевой экран» на стр. 155).
- Позволяет управлять параметрами обработки прикладных протоколов (см. «Обработка прикладных протоколов» на стр. 198).
- Предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена и так далее (см. «Встроенные средства коммуникации» на стр. 251).

ViPNet MFTP

Транспортный модуль ViPNet MFTP реализует в координаторе функцию сервера-маршрутизатора почтовых конвертов, а также обеспечивает обмен управляющей, адресной и ключевой информацией с программой ViPNet Центр управления сетью или

ViPNet Network Manager. Подробнее о программе см. документ «ViPNet MFTP. Руководство администратора».

ViPNet Контроль приложений

Программа «Контроль приложений» является необязательным модулем программного обеспечения ViPNet Coordinator. Чтобы иметь возможность контролировать сетевую активность приложений на каждом компьютере, необходима специальная лицензионная запись в регистрационном файле на ПО ViPNet.

Программа «Контроль приложений» позволяет:

- Получать информацию обо всех приложениях, которые запрашивали доступ в сеть.
- Ограничивать (разрешить или запретить) доступ приложений к сети.
- Просматривать журнал событий по сетевой активности приложений.

Подробнее о программе см. документ «ViPNet Контроль приложений. Руководство пользователя».

ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций через интерфейс Microsoft CryptoAPI 2.0. Она позволяет использовать криптографические функции, реализованные в соответствии с российскими стандартами, в различных приложениях, например Microsoft Office.

С помощью криптопровайдера ViPNet CSP вы можете выполнять следующие операции:

- Формирование и проверка электронной подписи.
- Шифрование данных, в том числе сообщений электронной почты.
- Аутентификация и защита соединений по протоколу TLS/SSL.

Подробнее об использовании криптопровайдера ViPNet CSP см. документ «ViPNet CSP. Руководство пользователя».

Что нового в версии 4.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.2 по сравнению с версией 4.1. Более подробная информация приведена в документе «Новые возможности ViPNet Client и ViPNet Coordinator версии 4.x. Приложение к документации ViPNet».

- **Возможность настройки TCP-туннеля**

  В программном обеспечении ViPNet Coordinator версии 4.x можно настроить TCP-туннель, через который будут осуществляться соединения клиентов, находящихся во внешних сетях, с другими узлами сети ViPNet, в том случае, если при подключении клиентов к внешним сетям провайдером услуг блокируется UDP-протокол.

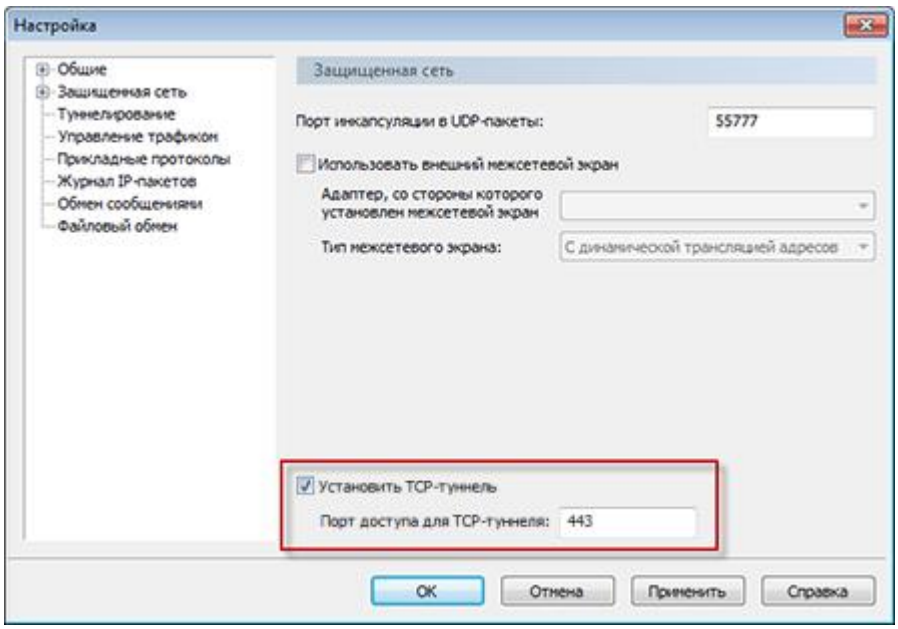


Рисунок 1: Возможность настройки TCP-туннеля в ViPNet Coordinator

Информация о настройке TCP-туннеля с номером порта для передачи TCP-пакетов рассылается на все клиенты, для которых координатор является координатором соединений. В дальнейшем, если удаленный клиент не сможет связаться с другими узлами сети ViPNet по протоколу UDP, он автоматически начнет устанавливать с ними соединение через TCP-туннель, настроенный на его координаторе соединений. На координаторе полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.

Стоит учесть, что TCP-туннель можно настроить только на координаторе, который не установлен за межсетевой экран или установлен за межсетевой экран со статической трансляцией адресов.

- **Изменения в мастере обновления сертификата**

  В мастере обновления сертификата была удалена настройка способа передачи запроса в связи с тем, что способ передачи запроса через файл стал невостребованным. В программе ViPNet Удостоверяющий и ключевой центр (УКЦ) версии 4.x обработка файлов с расширением `*.sok`, полученных напрямую от пользователя, невозможна. Теперь созданные запросы на обновление сертификатов могут быть переданы в УКЦ только через транспортный модуль ViPNet MFTP.

  Кроме этого, в мастере была исключена возможность выбора режима ожидания сертификата из УКЦ в реальном времени и параметра ввода сертификата в действие сразу после получения. Использование указанных настроек в некоторых случаях приводило к сбою процесса ввода в действие полученного из УКЦ сертификата. Теперь возможность сбоя при вводе в действие полученного сертификата исключена. Он автоматически вводится в действие при получении, если в окне настроек параметров безопасности на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по инициативе пользователя**.

- **Система обновления ViPNet**

  В версии 4.2, если настроена автоматическая установка обновлений, то все операции система обновления ViPNet производит в «тихом» режиме без выдачи сообщений на экран. Если настроена установка обновлений вручную, то при поступлении файлов обновления в области уведомлений отображается соответствующая информация.

  В предыдущих версиях значок системы обновлений в области уведомлений присутствовал всегда. В текущей версии значок присутствует только тогда, когда требуется выполнить дополнительные действия, например, перезагрузить компьютер после установки обновления или принять обновления, если настроена установка обновлений вручную. Также в текущей версии окно системы обновления ViPNet можно открыть из меню **Пуск**.

- **Изменения в совместном использовании программ ViPNet Coordinator и ViPNet SafeDisk-V**

  Для повышения уровня защиты конфиденциальной информации изменены условия запуска программы ViPNet SafeDisk-V, интегрированной с ViPNet Coordinator. Теперь, если в программе ViPNet Монитор отключена защита IP-трафика, программа ViPNet SafeDisk-V не запускается, а при запущенной программе ViPNet SafeDisk-V нельзя отключить защиту IP-трафика.

- **Новые возможности при обмене защищенными сообщениями**

В программе обмена защищенными сообщениями версии 4.2 появились дополнительные возможности. Теперь вы можете:

- осуществлять поиск слов в сообщениях открытых сеансов;
- осуществлять переход к предыдущему или к следующему просмотренному сеансу;
- узнать дату и время последнего обмена сообщениями с участником сеанса;
- отправлять файлы во время сеанса обмена сообщениями.

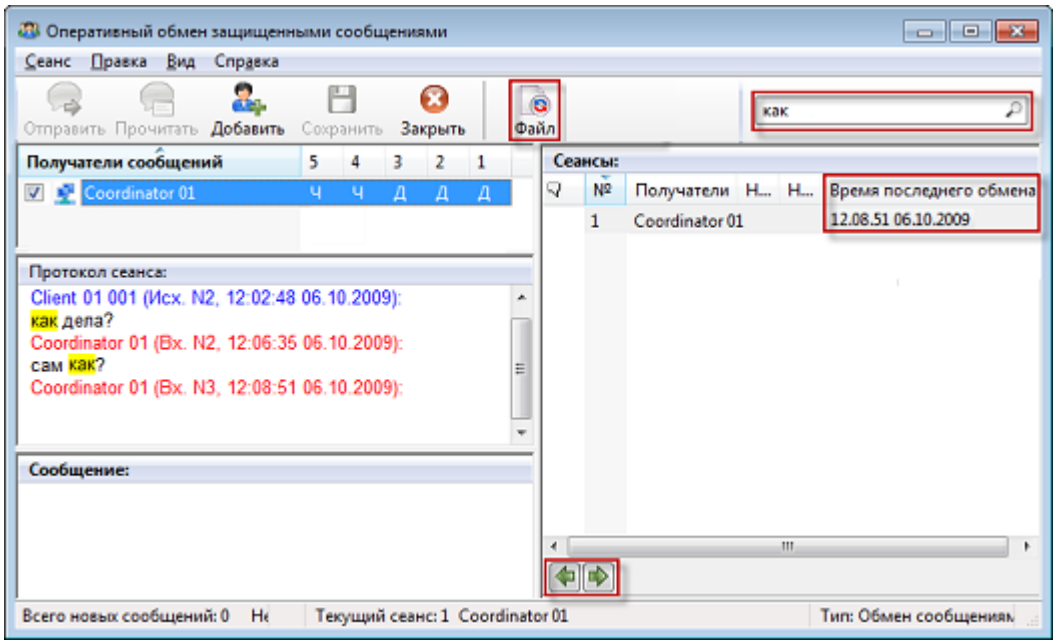


Рисунок 2: Новые возможности при обмене защищенными сообщениями

Кроме этого, теперь вы можете закрыть программу без завершения сеансов обмена сообщениями.

- **Оповещение об изменении групп объектов, сетевых фильтров или правил трансляции**

  В новой версии при добавлении или изменении групп объектов, сетевых фильтров или правил трансляции в строке состояния главного окна программы появляется сообщение о том, что соответствующие объекты были изменены, но изменения не применены. Сообщение в строке состояния будет отображаться до тех пор, пока не будет нажата кнопка **Применить** и в течение 30 секунд не будет подтверждено сохранение изменений.

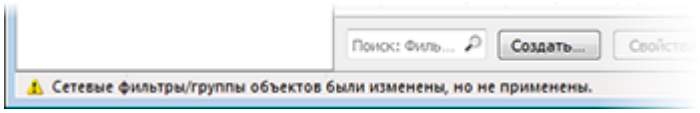


Рисунок 3: Оповещение об изменении групп объектов и сетевых фильтров

Системные требования

Требования к компьютеру для установки программы ViPNet Coordinator:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти зависит от числа клиентов, зарегистрированных на координаторе:

Число клиентов	ОЗУ
до 1000 шт.	не менее 1 Гбайт
до 5000 шт.	не менее 2 Гбайт

- Свободное место на жестком диске — не менее 1 Гбайт.
- Сетевой интерфейс или модем. Количество сетевых интерфейсов зависит от требований к функциональности координатора.
- Операционная система — Microsoft Windows XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Server 2012 (64-разрядная).

  Для операционной системы должен быть установлен самый последний пакет обновлений.
- При использовании более ранних версий Windows, чем Windows 8, на компьютере должен быть установлен накопительный пакет обновления часовых поясов KB2570791.
- При использовании Internet Explorer — версия 6.0 или выше.

Примечание. Для обеспечения работоспособности ViPNet Coordinator на компьютере не должны быть установлены другие сетевые экраны (также называемые брандмауэрами) и программные NAT-устройства.

Комплект поставки

Комплект поставки ViPNet Coordinator включает:

- Установочный файл программы.
- При поставке в составе программного комплекса ViPNet CUSTOM включена документация в формате PDF, в том числе:
  - «ViPNet Coordinator Монитор. Руководство администратора».
  - «ViPNet Coordinator. Быстрый старт».
  - «ViPNet MFTP. Руководство администратора».
  - «ViPNet Контроль приложений. Руководство пользователя».
  - «ViPNet CSP. Руководство пользователя».
  - «Развертывание сети ViPNet CUSTOM 4.x. Руководство администратора».
  - «Классификация полномочий. Приложение к документации ViPNet CUSTOM».
  - «Новые возможности ViPNet Client и ViPNet Coordinator версии 4.x. Приложение к документации ViPNet».
  - «Основные термины и определения. Приложение к документации ViPNet CUSTOM».

Обратная связь

Дополнительная информация

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

- Веб-портал документации ViPNet http://docs.infotecs.ru.
- Описание комплекса ViPNet CUSTOM http://www.infotecs.ru/products/line/custom.php.
- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/vpn/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами ОАО «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки: hotline@infotecs.ru.
- Форма запроса в службу технической поддержки http://www.infotecs.ru/support/request/.
- Форум ОАО «ИнфоТеКС» http://www.infotecs.ru/forum.
- 8 (495) 737-6196 — «горячая линия» службы технической поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

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

1

Общие сведения

Защищенная сеть ViPNet

Программные комплексы ViPNet CUSTOM и ViPNet VPN являются универсальными инструментами для развертывания виртуальных защищенных сетей (VPN) любых конфигураций, обеспечивающих прозрачное взаимодействие компьютеров, включенных в сеть ViPNet, независимо от способа и места подключения к сети.

Полная безопасность работы обеспечивается при установке соответствующих программных средств на каждый компьютер корпоративной сети. После этого информация, которой обмениваются участники сети, становится недоступной для других пользователей, не участвующих в обмене. Данные, хранящиеся на компьютерах ViPNet-сети, надежно защищены от несанкционированного доступа как с компьютеров корпоративной сети, так и с компьютеров, не входящих в сеть ViPNet.

Виртуальная сеть ViPNet строится путем установки на компьютеры (сетевые узлы) ПО ViPNet Client (рабочие места пользователей — клиенты) и ПО ViPNet Coordinator (серверы защищенной сети — координаторы). ViPNet Client обеспечивает сетевую защиту и включение в VPN отдельных компьютеров. Компьютер с ПО ViPNet Coordinator обычно устанавливается на границах локальных сетей и их сегментов и обеспечивает:

- включение в корпоративную сеть открытых и защищенных компьютеров, находящихся в этих локальных сетях, независимо от способа подключения и типа IP-адреса компьютера;
- разделение сетей;
- оповещение клиентских компьютеров о состоянии других сетевых узлов, связанных с ним.

Административные функции в сети ViPNet CUSTOM выполняет ПО ViPNet Administrator, состоящее из двух модулей: Центр управления сетью и Ключевой и удостоверяющий центр. Аналогичные функции в сети ViPNet VPN выполняет программа ViPNet Network Manager.

Подробнее о сети ViPNet CUSTOM см. документ «Развертывание сети ViPNet. Руководство администратора». Информация о комплексе ViPNet VPN содержится в документе «ViPNet VPN. Руководство пользователя».

Принцип работы ViPNet-драйвера

Ядром программного обеспечения ViPNet является ViPNet-драйвер, основной функцией которого является фильтрация, шифрование и расшифрование входящих и исходящих IP-пакетов.

Каждый исходящий пакет обрабатывается ViPNet-драйвером одним из следующих способов:

- шифруется и отправляется;
- отправляется в исходном виде (без шифрования);
- блокируется (в соответствии с установленными сетевыми фильтрами).

Каждый входящий пакет обрабатывается следующим образом:

- пропускается (если он не зашифрован и это разрешено сетевыми фильтрами для нешифрованного трафика);
- расшифровывается (если пакет был зашифрован);
- блокируется (в соответствии с установленными сетевыми фильтрами).

ViPNet-драйвер работает между канальным уровнем и сетевым уровнем модели OSI, что позволяет осуществлять обработку IP-пакетов до того, как они будут обработаны стеком протоколов TCP/IP и переданы на прикладной уровень. Таким образом, ViPNet-драйвер защищает IP-трафик всех приложений, не нарушая привычный порядок работы пользователей.

Рисунок 4: ViPNet-драйвер в модели OSI

Благодаря такому подходу внедрение технологии ViPNet не требует изменения сложившихся бизнес-процессов, а затраты на развертывание сети ViPNet невелики.

Примечание. На приведенной схеме модели OSI допущены следующие упрощения:

- Транспортный и сеансовый уровни объединены в транспортный уровень.
- Прикладной уровень и уровень представления объединены в прикладной уровень.

Следующая схема иллюстрирует работу ViPNet-драйвера при обработке запроса на просмотр веб-страницы. Страница размещена на IIS-сервере, который работает на компьютере Б.

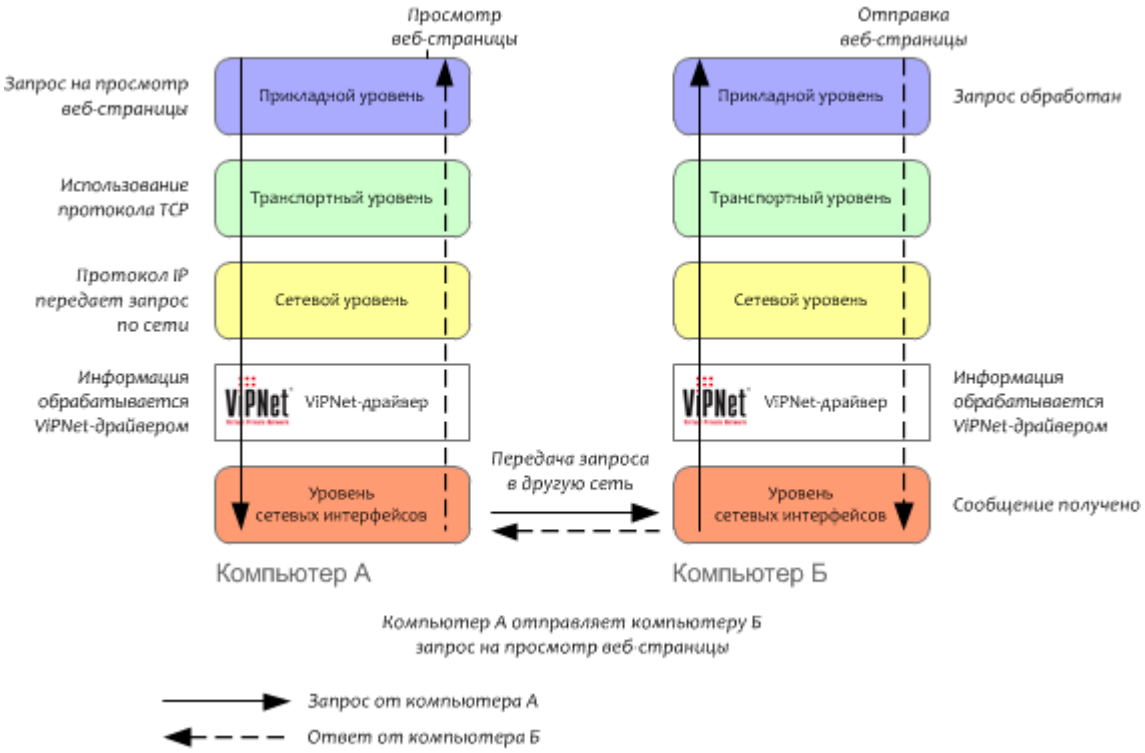


Рисунок 5: Схема работы сети TCP/IP, защищенной ПО ViPNet

Компьютер А отправляет на компьютер Б запрос по протоколу HTTP. Запрос передается на нижние уровни стека TCP/IP, при этом на каждом уровне к нему добавляется служебная информация. Когда запрос достигает ViPNet-драйвера, он зашифровывает запрос и добавляет к нему собственную информацию. ViPNet-драйвер, работающий на компьютере В, принимает запрос и удаляет из него служебную информацию ViPNet. Затем ViPNet-драйвер расшифровывает запрос и передает по стеку TCP/IP на прикладной уровень для обработки.

Функции координатора в защищенной сети ViPNet

В защищенной сети ViPNet координатор выступает в роли VPN-сервера. Как правило, узел с программным обеспечением ViPNet Coordinator выполняет в сети одну или несколько функций в зависимости от задач, решаемых в рамках корпоративной сети, ее структуры, нагрузки на координатор и других факторов.

Координатор выполняет в защищенной сети ViPNet следующие функции:

- Сервер IP-адресов (на стр. 33). Функция, которая позволяет обеспечить взаимодействие защищенных узлов ViPNet (см. «Защищенный узел» на стр. 484). Сервер IP-адресов сообщает сетевым узлам информацию об адресах и параметрах доступа других узлов.

- Маршрутизатор VPN-пакетов (на стр. 34). Функция, которая позволяет обеспечить маршрутизацию транзитного защищенного IP-трафика, проходящего через координатор на другие защищенные узлы. В случае фильтрации и трансляции трафика сторонними устройствами координатор может выступать в роли координатора соединений.

- VPN-шлюз (на стр. 35). Функция, которая позволяет создавать защищенные каналы (туннели) для организации защищенных соединений с открытыми узлами (см. «Открытый узел» на стр. 487).

- Сервер-маршрутизатор (на стр. 37). Функция, которая обеспечивает доставку на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью или ViPNet Network Manager, а также обмен прикладными транспортными конвертами между узлами (см. «Транспортный конверт» на стр. 492).

- Межсетевой экран (на стр. 38). Функция, которая позволяет обеспечить фильтрацию открытого трафика. Одновременно координатор может выполнять функции трансляции адресов для проходящего через него открытого трафика.

- Сервер открытого Интернета (на стр. 39). Функция, которая позволяет обеспечить раздельный доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet, если этого требует политика безопасности организации.

- TCP-туннель (на стр. 40). Функция, которая позволяет обеспечить получение IP-пакетов по протоколу TCP и их дальнейшую передачу по протоколу UDP.

Чтобы на сетевой узел можно было установить программное обеспечение ViPNet Coordinator, в программе ViPNet Центр управления сетью этот узел следует зарегистрировать в качестве координатора и добавить на него роль «VPN-сервер».

Сервер IP-адресов

При подключении любого клиента с программой ViPNet Client (см. «Клиент (ViPNet-клиент)» на стр. 485) к сети или изменении его параметров подключения эти параметры сообщаются координатору, который играет роль сервера IP-адресов для данного клиента. В свою очередь, сервер IP-адресов отправляет на клиент информацию о параметрах подключения и о состоянии всех узлов, с которыми у данного клиента имеется связь.

Таким образом, роль сервера IP-адресов заключается:

- в сборе сведений о сетевых узлах;
- в информировании о параметрах доступа и состоянии тех узлов сети, с которыми у данного клиента имеется связь.

Рисунок 6: Роль сервера IP-адресов в сети ViPNet

Список всех узлов, с которыми у клиента имеется связь, а также параметры доступа к ним отображаются в окне программы ViPNet Монитор в разделе **Защищенная сеть.**

Чтобы подтвердить свое присутствие в сети, клиент через заданный промежуток времени (по умолчанию — 5 минут) отправляет на сервер сообщение о своей активности. Если такое сообщение не поступило, координатор переводит клиент в статус «Недоступен».

Аналогичным образом происходит обмен информацией о параметрах доступа между координаторами. Периодически (по умолчанию каждые 15 минут) координатор отсылает на другие связанные с ним координаторы подтверждение о своей активности. Кроме того,

координаторы обеспечивают рассылку информации об узлах, для которых они выполняют функцию сервера IP-адресов.

Сервер IP-адресов работает по следующей логике:

- При появлении новой информации о своем клиенте (то есть о клиенте, который использует данный координатор в качестве сервера IP-адресов) координатор рассылает ее на другие свои клиенты и связанные координаторы.
- При появлении новой информации о клиентах других координаторов рассылает эту информацию на свои клиенты, которые связаны с клиентами другого координатора.
- При отсутствии информации от своего клиента по истечении периода опроса координатор считает этот клиент недоступным и рассылает информацию об этом.
- В случае взаимодействия координатора с другой сетью ViPNet на шлюзовой координатор другой сети высылается информация о состоянии всех узлов своей сети, связанных с узлами другой сети ViPNet. При получении такой информации из другой сети ViPNet координатор рассылает эту информации на все координаторы своей сети, а также на свои клиенты, связанные с узлами другой сети.

По умолчанию для клиента роль сервера IP-адресов выполняет его сервер-маршрутизатор (координатор, на котором клиент зарегистрирован в программе ViPNet Центр управления сетью или ViPNet Network Manager). В отличие от сервера-маршрутизатора, сервер IP-адресов можно сменить, выбрав любой другой координатор, с которым у данного клиента есть связь.

Маршрутизатор VPN-пакетов

Координатор осуществляет маршрутизацию транзитного защищенного трафика, который проходит через координатор на другие защищенные сетевые узлы. Маршрутизация осуществляется как внутри одной сети ViPNet, так и при взаимодействии с другими сетями ViPNet.

Рисунок 7: Функция маршрутизации защищенного трафика в сети ViPNet

Маршрутизация защищенного трафика осуществляется на основании идентификаторов защищенных узлов, содержащихся в открытой части IP-пакетов, которая защищена от подделки, и на основании защищенного протокола динамической маршрутизации трафика. Одновременно с этим для защищенного трафика выполняется трансляция адресов (NAT) (см. «Трансляция сетевых адресов (NAT)» на стр. 492). Все транзитные защищенные пакеты, поступающие на координатор, отправляются на другие узлы от имени IP-адреса координатора. Трансляция адресов для защищенного трафика выполняется автоматически в соответствии с параметрами, которые не могут быть изменены.

Если на границе сети ViPNet установлено какое-либо стороннее устройство осуществляющее фильтрацию и трансляцию передаваемого трафика, то в этом случае координатор может выступать в роли координатора соединений. С помощью координатора соединений клиенты устанавливают соединения друг с другом в том случае, если напрямую установить соединение они не могут. Для каждого клиента может быть назначен свой координатор соединений. По умолчанию координатором соединений для клиента выбран сервер IP-адресов (на стр. 33).

Рисунок 8: Организация соединений между сетевыми узлами ViPNet

VPN-шлюз

VPN-шлюз позволяет включить открытые узлы в защищенную сеть ViPNet без установки на данные узлы ПО ViPNet, а также защитить соединения с участием открытых узлов при передаче данных через Интернет или другие публичные сети. Для решения этих задач используется технология туннелирования (см. «Защита трафика открытых узлов (туннелирование)» на стр. 217).

Туннелирование заключается в шифровании трафика открытых узлов координатором, который играет роль VPN-шлюза. С помощью технологии туннелирования можно

организовать защищенное соединение между открытым узлом и защищенным узлом ViPNet или между двумя открытыми узлами, которые туннелируются разными координаторами.

Туннелирование позволяет организовать защиту трафика узлов, на которых не может быть установлено программное обеспечение ViPNet Client или ViPNet Coordinator (например, различных серверов, компьютеров Apple, сетевых принтеров, сетевых хранилищ данных и так далее).

Защита трафика открытого узла при туннелировании осуществляется следующим образом:

- Открытые IP-пакеты от туннелируемого узла поступают на координатор.
- На координаторе IP-пакеты обрабатываются сетевыми фильтрами, зашифровываются и передаются на защищенный узел, для которого эти пакеты предназначены, либо на другой координатор.
- Если на координатор поступают зашифрованные IP-пакеты, предназначенные для туннелируемого узла, эти IP-пакеты обрабатываются сетевыми фильтрами, расшифровываются и передаются на узел назначения в открытом виде.

Рисунок 9: Использование туннелирования в сети ViPNet

Чтобы координатор мог выполнять функцию туннелирования, администратор сети ViPNet в программе ViPNet Центр управления сетью или ViPNet Network Manager задает максимальное разрешенное число одновременных туннельных соединений на данном координаторе. Также в программе ViPNet Центр управления сетью или ViPNet Network Manager либо на самом координаторе задаются IP-адреса туннелируемых устройств (см. «Настройка туннелирования» на стр. 220).

Сервер-маршрутизатор

В программе ViPNet Центр управления сетью или ViPNet Network Manager каждый создаваемый клиент регистрируется на координаторе. Этот координатор является для клиента сервером-маршрутизатором. Пользователь сетевого узла не может изменить заданный сервер-маршрутизатор на какой-либо другой.

Роль сервера-маршрутизатора в сети ViPNet состоит в доставке на сетевые узлы управляющих сообщений, обновлений ключей и программного обеспечения из программы ViPNet Центр управления сетью или ViPNet Network Manager, а также обмен прикладными транспортными конвертами между узлами (см. «Транспортный конверт» на стр. 492).

Маршрутизация прикладных и управляющих конвертов осуществляется с помощью транспортного модуля ViPNet MFTP, работающего на прикладном уровне. Транспортный модуль на координаторе принимает конверты от других узлов сети ViPNet и пересылает их на узел назначения.

Рисунок 10: Роль сервера-маршрутизатора в сети ViPNet

Маршрутизация данных между координаторами выполняется на основании межсерверных каналов, заданных для этих координаторов. Межсерверные каналы могут быть организованы по любой схеме. Если есть несколько маршрутов передачи конвертов между координаторами, передача информации осуществляется по кратчайшему из них. Передача информации из одной сети в другую выполняется через шлюзовые координаторы, с помощью которых происходит взаимодействие двух сетей.

При поступлении прикладного или управляющего конверта сервер-маршрутизатор в соответствии с маршрутными таблицами определяет дальнейший путь передачи этого конверта. Если конверт многоадресный, он дробится сервером на соответствующие части. Получив конверт, сервер-маршрутизатор выполняет одно из действий, в зависимости от заданных параметров:

- Устанавливает соединение с сетевым узлом (по умолчанию такая логика действует при отправке конверта на другой сервер-маршрутизатор).

- Ожидает, когда соединение установит получатель конверта (по умолчанию эта логика действует при наличии конвертов для клиентов).

Кроме того, можно задать период опроса других объектов независимо от наличия для них конвертов. При разрывах соединений передача информации всегда продолжается с точки разрыва, что особенно важно на коммутируемых каналах.

Подробнее о работе и настройке транспортного модуля ViPNet MFTP см. документ «ViPNet MFTP. Руководство администратора».

Межсетевой экран

Координатор выполняет фильтрацию открытых IP-пакетов на каждом сетевом интерфейсе по адресам, протоколам и портам в соответствии с настроенными сетевыми фильтрами (см. «Основные принципы фильтрации трафика» на стр. 156). С помощью сетевых фильтров можно не только заблокировать нежелательные соединения, но и разрешить соединения с открытыми узлами, не входящими в сеть ViPNet.

Помимо настраиваемых фильтров в программе имеется система защиты от одной из распространенных сетевых атак — спуфинга (см. «Антиспуфинг» на стр. 192).

Рисунок 11: Роль межсетевого экрана в сети ViPNet

Координатор также может осуществлять трансляцию адресов (NAT) для проходящего через него открытого трафика (см. «Трансляция сетевых адресов (NAT)» на стр. 492).

Примечание. Трансляция адресов для защищенного трафика осуществляется автоматически (см. «Маршрутизатор VPN-пакетов» на стр. 34).

Функция NAT для открытого трафика позволяет задать правила трансляции адресов для решения двух основных задач:

- Для подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов. Таким образом, NAT позволяет компьютерам с локальными адресами получать доступ к Интернету от имени публичного адреса координатора.

  Для решения этой задачи используется трансляция адреса источника.

- Для организации доступа к внутренним ресурсам из внешней сети. В результате применения технологии NAT узлы локальной сети, имеющие частные адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

  Для решения этой задачи используется трансляция адреса назначения.

Подробнее об использовании NAT для открытого трафика см. раздел Трансляция сетевых адресов (NAT) (на стр. 206).

Сервер открытого Интернета

Технология «Открытый Интернет» (см. «Настройка сервера открытого Интернета» на стр. 225) позволяет разделить доступ защищенных узлов в Интернет и к ресурсам защищенной сети ViPNet. Таким образом обеспечивается доступ в Интернет с максимальным уровнем безопасности, возможным без физического отключения компьютера от корпоративной сети.

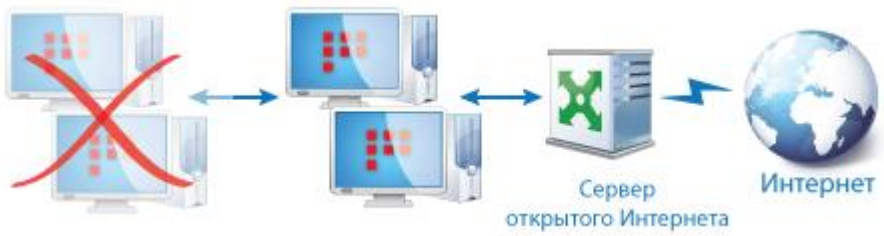


Рисунок 12: Роль сервера открытого Интернета в сети ViPNet

Клиенты, имеющие связь с сервером открытого Интернета, могут работать только в одном из двух режимов:

- Работа в Интернете, при этом ресурсы корпоративной защищенной сети недоступны, хотя компьютер не отключен от сети физически.

- Работа в локальной сети, при этом доступ в Интернет полностью заблокирован, но без физического отключения от внешней сети.

Такое разделение на два непересекающихся режима исключает любые атаки в реальном времени на компьютеры корпоративной сети через компьютеры, имеющие доступ к Интернету. Если же на компьютер, работающий в Интернете, попадет вредоносная программа, она будет обнаружена и блокирована модулем контроля приложений ViPNet (см. «ViPNet Контроль приложений» на стр. 19), при этом не получив доступа в корпоративную сеть.

Чтобы использовать на координаторе технологию «Открытый Интернет», в программе ViPNet Центр управления сетью для этого координатора следует включить функцию сервера открытого Интернета.

TCP-туннель

На координаторе может быть настроен TCP-туннель, через который будут осуществляться соединения клиентов, находящихся во внешних сетях, с другими узлами сети ViPNet, в том случае, если при подключении клиентов к внешним сетям провайдером услуг блокируется UDP-протокол.

Рисунок 13: Функция TCP-туннеля

Если удаленный клиент не может связаться с другими узлами по протоколу UDP, и на его координаторе соединений при этом настроен TCP-туннель, он автоматически начинает устанавливать с узлами соединение через TCP-туннель координатора соединений. На координаторе полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.

2

Установка, обновление и удаление ПО ViPNet Coordinator

Установка ПО ViPNet Coordinator

Внимание! На компьютере, где устанавливается ПО ViPNet Coordinator, не должны быть установлены сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT). Использование ViPNet Coordinator одновременно с такими программами может привести к конфликтам и вызвать проблемы с доступом в сеть.

Перед установкой ПО ViPNet Coordinator убедитесь, что на компьютере выполнены стандартные сетевые настройки, а также правильно заданы часовой пояс, дата и время.

Если ViPNet Coordinator устанавливается на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе ViPNet Coordinator нужно изменить региональные настройки Windows (см. «Региональные настройки» на стр. 426).

Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

Для установки ViPNet Coordinator требуются:

- Установочный файл программы.
- Дистрибутив ключей (на стр. 484) для сетевого узла (файл *.dst). Если на узле планируется работа нескольких пользователей, для каждого из них нужен отдельный дистрибутив ключей.
- Пароль пользователя сетевого узла или внешнее устройство аутентификации (см. «Внешние устройства» на стр. 438).

  Дистрибутив ключей и пароль пользователя (либо внешнее устройство) можно получить у администратора сети ViPNet.

Для установки ViPNet Coordinator выполните следующие действия:

1. Запустите установочный файл  . Дождитесь завершения подготовки к установке ViPNet Coordinator.

Примечание. После запуска файла установки может появиться предупреждение системы безопасности о невозможности проверить сертификат подписи файла установки. В этом случае см. указания раздела Невозможно проверить сертификат, которым подписан файл установки программы (на стр. 369).

2 Ознакомьтесь с условиями лицензионного соглашения. В случае согласия установите соответствующий флажок. Затем нажмите кнопку **Продолжить**.

3 Если вы хотите, чтобы после завершения установки компьютер был перезагружен автоматически, установите соответствующий флажок.

4 Если вы хотите настроить параметры установки, нажмите кнопку **Настроить** и укажите:

- компоненты ViPNet Coordinator, которые необходимо установить;
- путь к папке установки компонентов ViPNet Coordinator на компьютере;
- имя пользователя и название организации;
- название папки для программы ViPNet Coordinator в меню **Пуск**.

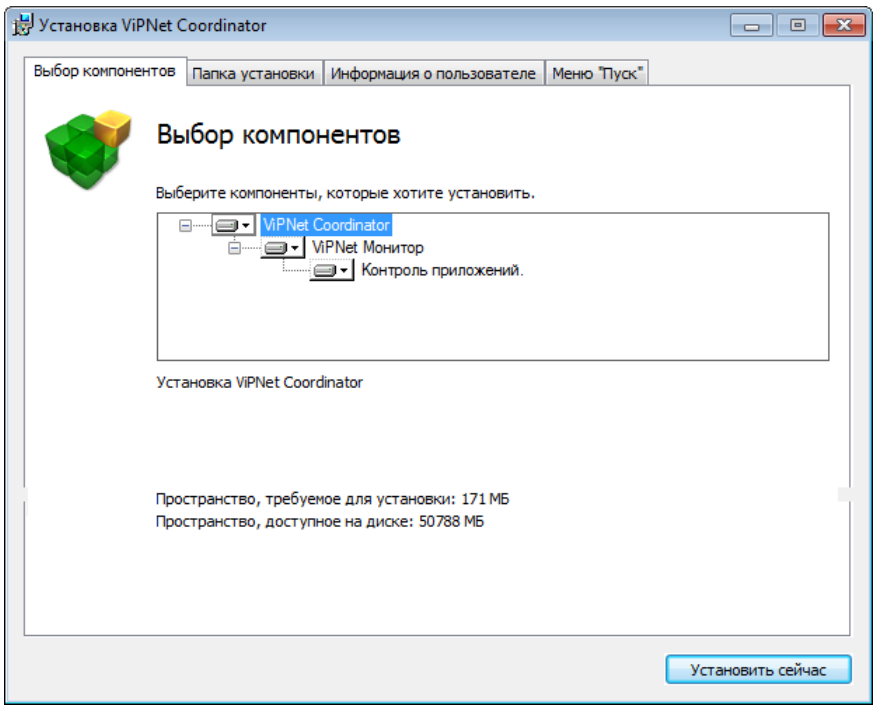


Рисунок 14: Выбор способа установки

5 Чтобы начать установку ViPNet Coordinator, нажмите кнопку **Установить сейчас**.

Примечание. ViPNet Coordinator можно установить в неинтерактивном режиме (см. «Установка в неинтерактивном режиме» на стр. 45). В этом случае процесс установки не будет отображаться на экране.

6 В зависимости от наличия на компьютере справочников и ключей, установленных ранее, выполните одно из действий:

- Если справочники и ключи еще не установлены на компьютере, выполните их установку (см. «Установка справочников и ключей» на стр. 59).
- Если на компьютере уже имеется ПО ViPNet, для которого ранее были установлены справочники и ключи, при запуске программы ViPNet Монитор укажите путь к папке ключей пользователя и папке ключей сетевого узла (см. «Использование справочников и ключей, установленных ранее» на стр. 69).

Внимание! В данном случае получать новый файл дистрибутива ключей для ПО ViPNet Coordinator у администратора сети ViPNet и устанавливать ключи из этого файла крайне не рекомендуется, поскольку это может привести к сбоям в работе программного обеспечения ViPNet.

7 При первом запуске программы ViPNet Монитор стандартный сетевой экран Windows будет автоматически отключен. Не включайте сетевой экран Windows во время использования программы ViPNet Coordinator, так как эти программы могут конфликтовать.

Установка в неинтерактивном режиме

В неинтерактивном режиме процесс установки ViPNet Coordinator не отображается на экране компьютера. Установку в данном режиме можно запустить с помощью командной строки Windows. Параметры, которые обычно могут быть заданы в процессе установки, в неинтерактивном режиме следует указать заранее в командной строке.

Использование неинтерактивного режима позволяет вам выполнять удаленную установку ПО или создавать программы, которые обращаются к командной строке Windows и запускают автоматическую установку ПО с заданными параметрами.

Например, вы можете создать сценарий входа в систему (logon script), который запустит автоматическую установку ПО после загрузки системы (информацию о создании сценариев входа в систему можно найти на сайте компании Microsoft http://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx).

Чтобы запустить программу установки ПО в неинтерактивном режиме, в командной строке Windows выполните одну из команд:

- `<название установочного файла> /qn` — для установки в неинтерактивном режиме (без отображения процесса установки на экране);
- `<название установочного файла> /qb` — установка в неинтерактивном режиме с отображением индикатора выполнения установки.

При необходимости можно задать дополнительные параметры установки ViPNet Coordinator в командной строке (см. «Дополнительные параметры установки в неинтерактивном режиме» на стр. 46). После начала установки изменить параметры установки уже нельзя.

Примечание. Если после начала установки в неинтерактивном режиме по прошествии нескольких минут не появляется признаков завершения установки (появление ярлыка установленной программы на рабочем столе, перезагрузка компьютера), см. указания раздела Установка программы не выполняется в неинтерактивном режиме (на стр. 370).

В неинтерактивном режиме ПО ViPNet Coordinator устанавливается в следующие папки:

- Если ПО ViPNet Coordinator устанавливается на данный компьютер впервые:
  - В папку `C:\Program Files\InfoTeCS\ViPNet Coordinator` при использовании 32-разрядных версий ОС Windows.
  - В папку `C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator` при использовании 64-разрядных версий ОС Windows.
- В текущую папку установки, если ПО ViPNet Coordinator уже было установлено на компьютере.

Дополнительные параметры установки в неинтерактивном режиме

При необходимости в командной строке укажите дополнительные параметры установки:

- Если вы хотите установить только часть компонентов ПО ViPNet Coordinator, в командной строке задайте список нужных компонентов. Для этого используйте параметр

  `ADDLOCAL="<список компонентов>"`

  Компоненты ПО ViPNet Coordinator:
  - Core — базовый компонент ПО.
  - Monitor — ViPNet Монитор.
  - RF — ViPNet Контроль приложений. Данный компонент может быть установлен только вместе с компонентом ViPNet Монитор.

Внимание! Компонент `Core` является обязательным для установки.

  Если вы не зададите компоненты ПО с помощью команды `ADDLOCAL`, будут установлены все компоненты.
- В командной строке вы также можете указать параметры перезапуска компьютера после завершения установки:
  - `/forcerestart` — принудительная перезагрузка компьютера по окончании установки (в неинтерактивном режиме выполняется по умолчанию);

- `/norestart` — отключение принудительной перезагрузки компьютера по окончании установки.

Пример команды для установки в неинтерактивном режиме без перезагрузки и без установки компонента ViPNet Контроль приложений:

```
<название установочного файла> /qn /norestart ADDLOCAL="Core,Monitor"
```

Обновление ПО ViPNet Coordinator

Если выпущена новая версия программы ViPNet Coordinator, вы можете обновить программу, установленную на сетевом узле.

Внимание! Обновить программу до версии 4.x вы можете только с версии 3.2.x и выше. Если у вас установлена программа более ранней версии, то выполните следующие действия:

- Сначала обновите программу до версии 3.2.x.
- Запустите и войдите в программу, сконвертировав ключи на устройстве, если таковые используются.
- После этого закройте и обновите программу до версии 4.x.

При несоблюдении указанных действий корректное обновление программы ViPNet Coordinator до версии 4.x будет невозможно.

Перед началом обновления убедитесь, что ваша лицензия на сеть ViPNet разрешает использовать новую версию программного обеспечения. Если вы установите на сетевом узле недопустимую версию программного обеспечения, его невозможно будет запустить. В этом случае для восстановления работоспособности сетевого узла удалите новую версию программного обеспечения, затем установите версию, использование которой разрешено лицензией.

Вы можете выполнить обновление несколькими способами:

- Прием обновления, отправленного централизованно на сетевые узлы администратором сети ViPNet с помощью программы ViPNet Центр управления сетью или ViPNet Network Manager. Такое обновление принимается автоматически (см. «Обновление, отправленное из ЦУСа или ViPNet Network Manager» на стр. 49).
- Обновление групповых политик Windows (см. «Обновление с помощью групповых политик» на стр. 49) либо обновление с помощью центра обновления Windows (на стр. 49). Обновления данного типа централизованно отправляются на сетевые узлы администратором сети ViPNet с помощью средств создания групповых политик Windows.
- Обновление вручную с помощью нового установочного файла (см. «Обновление с помощью установочного файла» на стр. 50).

Примечание. На компьютере с операционной системой Windows XP или Windows Vista после начала обновления может появиться предупреждение системы безопасности о невозможности проверить сертификат подписи файла установки. В этом случае см. указания раздела Невозможно проверить сертификат, которым подписан файл установки программы (на стр. 369).

Обновление, отправленное из ЦУСа или ViPNet Network Manager

Обновление ПО ViPNet Coordinator, отправленное из ViPNet Administrator или ViPNet Network Manager, можно принять на сетевом узле с помощью системы обновления ViPNet (см. «О системе обновления ViPNet» на стр. 95). В зависимости от настроек системы обновления, обновление ПО принимается на сетевом узле автоматически, либо вам необходимо принять его вручную (см. Установка обновлений вручную (на стр. 99)).

Обновление с помощью групповых политик

Администратор сети ViPNet может отправить на ваш сетевой узел обновление ПО ViPNet Coordinator в виде обновления групповых политик. Для этого администратор использует средства управления групповыми политиками.

Полученные таким образом обновления ПО ViPNet Coordinator устанавливаются в рамках обновления групповых политик в вашей сети и не требуют от вас каких-либо дополнительных действий.

Чтобы узнать о том, что такое групповые политики и для чего их можно использовать, перейдите по ссылке http://technet.microsoft.com/ru-ru/windowsserver/bb310732.aspx.

Обновление с помощью Центра обновления Windows

Администратор сети ViPNet может отправить на ваш сетевой узел обновление ViPNet Coordinator, устанавливаемое с помощью Центра обновления Windows. Для этого администратор использует средства управления обновлениями (например, Microsoft System Center Essentials).

Чтобы установить полученные обновления, выполните следующие действия:

1. В меню **Пуск** выберите **Все программы > Центр обновления Windows**.
2. В открывшемся окне **Центр обновления Windows** проверьте наличие обновлений. При наличии обновлений будет отображаться кнопка **Установить обновления**.

3 Чтобы обновить ПО ViPNet Coordinator, выберите для установки обновления ViPNet Coordinator и ViPNet CSP. Затем нажмите кнопку **Установить обновления.**

4 Дождитесь завершения процесса обновления. При необходимости перезагрузите компьютер.

Обновление с помощью установочного файла

Получите установочный файл новой версии ПО. Затем выполните следующие действия:

1 Запустите установочный файл  . Дождитесь завершения подготовки к установке ViPNet Coordinator.

2 В окне **Обновление ViPNet Coordinator** задайте настройки обновления:

- Если версия установленной на сетевом узле программы ViPNet CSP совпадает с версией в файле установки, в окне будет также отображен флажок **Восстановить ViPNet CSP**. Если вы установите данный флажок, то при обновлении ПО будет переустановлена программа ViPNet CSP.

Совет. Если программа ViPNet CSP на сетевом узле работает без сбоев, данный флажок можно не устанавливать. В этом случае обновление ПО будет выполнено быстрее.

  Если версия программы ViPNet CSP на сетевом узле не совпадает с версией в файле установки, то указанный флажок будет отсутствовать, и программа ViPNet CSP будет автоматически переустановлена.

- Если вы хотите, чтобы после обновления ViPNet Coordinator была автоматически выполнена перезагрузка компьютера, установите соответствующий флажок.

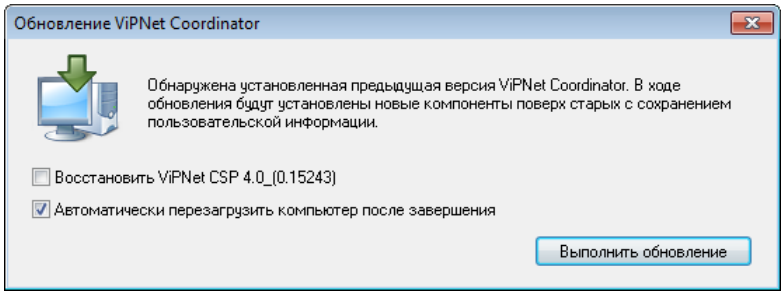


Рисунок 15: Параметры обновления ПО

3 Нажмите кнопку **Выполнить обновление.**

4 Если с некоторыми приложениями ViPNet работа не была завершена, может появиться сообщение о невозможности их обновления. В этом случае завершите работу с ними, после чего вы сможете продолжить обновление.

5 Дождитесь завершения обновления ПО.

Если ранее вы выбрали автоматическую перезагрузку компьютера, то после завершения установки компьютер будет автоматически перезагружен. В противном случае в окне завершения установки нажмите кнопку **Закрыть**, затем самостоятельно перезагрузите компьютер.

Добавление, удаление и восстановление компонентов ПО ViPNet Coordinator

При необходимости вы можете установить или удалить компоненты ПО ViPNet Coordinator, а также восстановить ПО при обнаружении повреждений. Для этого вам необходимо получить установочный файл версии программы, с которой вы работаете.

Примечание. При удалении компонентов ПО ViPNet Coordinator пользовательские данные (справочники и ключи ViPNet, настройки параметров работы программы и другие данные) сохраняются и могут использоваться после повторной установки соответствующего ПО.

Для установки, удаления компонентов и для восстановления ПО ViPNet Coordinator выполните следующие действия:

1. Запустите установочный файл  . Дождитесь завершения подготовки к установке компонентов ViPNet Coordinator.
2. В окне **Изменение установленных компонентов** выберите нужный пункт:
   - для установки или удаления компонентов выберите **Добавить или удалить компоненты**;
   - для восстановления ПО выберите **Восстановить**.

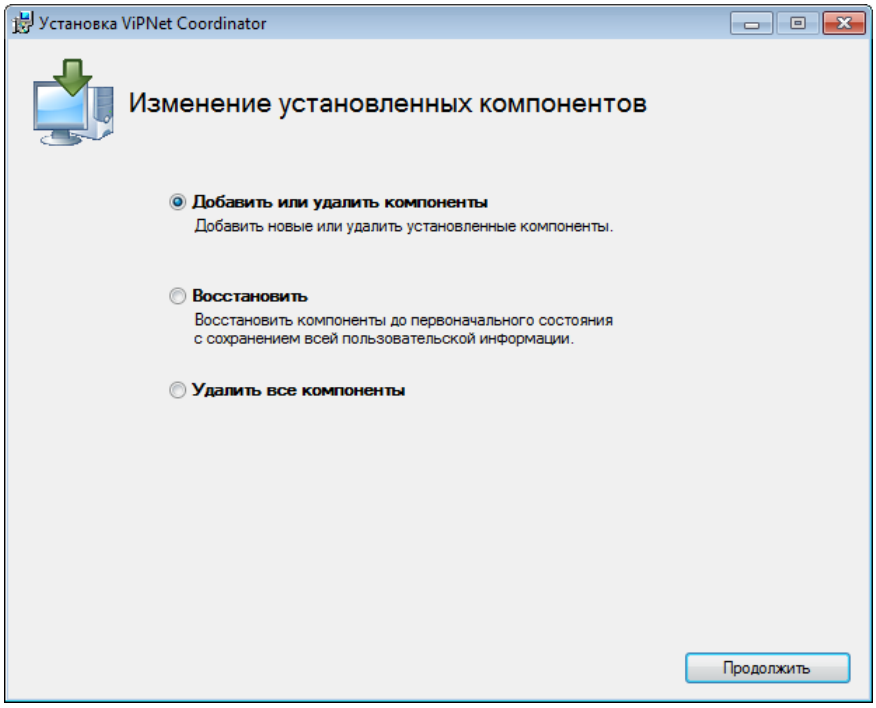


Рисунок 16: Изменение установленных компонентов

Затем нажмите кнопку **Продолжить**.

3 Если вы устанавливаете или удаляете компоненты ПО, на странице выбора компонентов укажите те, которые необходимо добавить или удалить. Затем нажмите кнопку **Продолжить**.

4 Дождитесь завершения установки (восстановления, удаления) компонентов ПО ViPNet Coordinator. Затем нажмите кнопку **Закрыть**.

Удаление ПО ViPNet Coordinator

При необходимости вы можете полностью удалить с компьютера программу ViPNet Coordinator и все ее компоненты.

При удалении программы ViPNet Coordinator вы можете сохранить пользовательские данные, сформированные и используемые во время работы: справочники и ключи ViPNet, настройки параметров работы программы и другие.

Чтобы полностью удалить ПО ViPNet Coordinator с компьютера, выполните следующие действия:

1. Запустите установочный файл. Дождитесь завершения подготовки к удалению ViPNet Coordinator.
2. На странице изменения установленных компонентов выберите пункт **Удалить все компоненты**.
3. Нажмите кнопку **Продолжить**.
4. В зависимости от того, хотите ли вы сохранить пользовательские данные, установите или снимите флажок **Удалить пользовательские данные**.
5. Для продолжения нажмите кнопку **Удалить**.
6. Дождитесь завершения удаления программного обеспечения.

Совет. Вы также можете полностью удалить ViPNet Coordinator, в меню **Пуск** выбрав **Все программы** > **ViPNet** > **ViPNet Coordinator** > **Удаление ViPNet Coordinator**. При этом пользовательские данные будут сохранены.

Перенос сетевого узла на другой компьютер

Чтобы перенести функционирующий узел сети ViPNet с одного компьютера на другой (например, в случае замены устаревшего компьютера), сохранив при этом текущие настройки программы ViPNet Монитор, необходимо скопировать на новый компьютер справочники, ключи и другие данные из папки программы ViPNet Coordinator.

Путем переноса справочников и ключей также можно восстановить сетевой узел после переустановки операционной системы.

Внимание! Не следует использовать данный сценарий для переноса сетевого узла с 32-разрядной версии операционной системы Windows на 64-разрядную версию Windows и наоборот, поскольку в этом случае возможна некорректная работа программного обеспечения ViPNet. Если есть потребность в подобном переносе, то в корректной форме его можно осуществить только путем установки на узле ПО ViPNet и справочников и ключей с помощью дистрибутива ключей.

После переноса справочников и ключей следует удалить их исходный экземпляр. Недопустима ситуация, когда на разных компьютерах установлены одни и те же ключи.

Для переноса справочников и ключей выполните следующие действия:

1. Скопируйте на съемный носитель или в другое надежное место следующие папки и файлы, находящиеся в папке установки программы ViPNet Coordinator:
   - `\d_station`;
   - `\databases`;
   - `\Protocol` (если требуется скопировать сохраненные протоколы сеансов обмена сообщениями);
   - `\TaskDir` (если требуется сохранить файлы, принятые по файловому обмену);
   - Папки ключей пользователей, обычно `\user_AAAA` (где AAAA — шестнадцатеричный идентификатор пользователя ViPNet без номера сети).

     В некоторых случаях папка ключей пользователя может совпадать с папкой установки программы ViPNet Coordinator, тогда следует скопировать папку `\key_disk`.

- \out;
- NMATRIX.DAT;
- NODEXXXX.MAP (где XXXX — шестнадцатеричный идентификатор сетевого узла без номера сети);
- файлы AP*.TXT: APAXXXX.TXT, APCXXXX.TXT, APIXXXX.TXT, APLXXXX.TXT, APNXXXX.CRC, APNXXXX.CRG, APNXXXX.TXT, APSXXXX.TXT, APUXXXX.TXT (где XXXX — шестнадцатеричный идентификатор сетевого узла без номера сети);
- infotecs.re;
- iplir.cfg, iplirmain.cfg;
- ipliradr.do$;
- linkXXXX.txt, nodeXXXX.tun (где XXXX — шестнадцатеричный идентификатор сетевого узла без номера сети);
- mftp.ini.

Примечание. По умолчанию программа ViPNet Coordinator устанавливается в папку C:\Program Files\InfoTeCS\ViPNet Coordinator в 32-битных версиях Windows и в папку C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator — в 64-битных версиях.

Некоторые из перечисленных файлов и папок могут отсутствовать в папке программы ViPNet Coordinator.

2 Перед переносом справочников и ключей на новый компьютер установите на этот компьютер программу ViPNet Coordinator, но не выполняйте установку справочников и ключей.

3 При переносе справочников и ключей на компьютер, на котором уже установлена программа ViPNet Coordinator, убедитесь, что на этом компьютере не установлены справочники и ключи другого сетевого узла. Если эти данные присутствуют, удалите их, как это описано в разделе Удаление справочников и ключей (на стр. 74) либо вручную удалите следующие папки и файлы:

- папки ключей пользователей \user_BBBB (где BBBB — шестнадцатеричный идентификатор пользователя ViPNet без номера сети).
- файлы AP*.TXT, APNYYYY.CRC, APNYYYY.CRG (где YYYY — шестнадцатеричный идентификатор сетевого узла без номера сети).

4 Файлы и папки, скопированные на шаге **1**, поместите в новую папку установки программы ViPNet Coordinator с заменой файлов.

5 Если требуется, в файле `mftp.ini` укажите путь к новой папке установки программы ViPNet Coordinator в значениях всех параметров, где он встречается.

6 Удалите файл `certlist.sst`, находящийся в подпапке `\d_station\abn_AAAA` (где AAAA — шестнадцатеричный идентификатор пользователя ViPNet без номера сети).

7 Запустите программу ViPNet Монитор. В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и выберите пункт **Папка ключей пользователя.** Укажите путь к папке ключей пользователя.

8 Выполните вход в программу ViPNet Монитор.

9 В окне **Настройка параметров безопасности** на вкладке **Ключи** установите контейнер ключей. Для этого:

- Нажмите кнопку **Установить контейнер.**
- В окне **ViPNet CSP - инициализация контейнера ключей** укажите путь к папке, в которой находится контейнер, например `C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator\user_AAAA\key_disk\dom`.
- В списке **Имя контейнера** выберите контейнер (имя контейнера начинается с символов `sgn`).
- Нажмите кнопку **OK**.

10 На компьютере, с которого вы осуществили перенос сетевого узла, удалите исходные экземпляры справочников и ключей (см. «Удаление справочников и ключей» на стр. 74).

После выполнения перечисленных действий программа ViPNet Coordinator готова к работе.

3

Установка и обновление справочников и ключей

Установка справочников и ключей

Установка справочников и ключей выполняется при развертывании ПО ViPNet на сетевом узле, при добавлении новых пользователей ViPNet на сетевой узел, а также в других случаях, когда справочники и ключи, установленные на узле, были повреждены или являются устаревшими.

Если вы хотите выполнить первоначальную установку справочников и ключей на сетевом узле с одним пользователем, выполните рекомендации раздела Установка справочников и ключей одного пользователя (на стр. 60).

В случаях, описанных ниже, перед установкой дополнительно ознакомьтесь с соответствующими разделами:

- Если вы хотите организовать работу нескольких пользователей на одном сетевом узле или добавить нового пользователя на сетевой узел, на котором уже работают другие пользователи, см. раздел Установка справочников и ключей нескольких пользователей на одном сетевом узле (на стр. 63).
- Если вы хотите самостоятельно задать папки, в которых будут храниться справочники и ключи, см. раздел Расширенный режим установки справочников и ключей (на стр. 63).
- Если на сетевом узле имеется несколько программ ViPNet, но ни для одной из них не установлены справочники и ключи, см. раздел Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet (на стр. 66).

Примечание. Если на узле уже установлены справочники и ключи для какой-либо программы ViPNet, выполните указания раздела Использование справочников и ключей, установленных ранее (на стр. 69).

- Если вы хотите установить справочники и ключи с использованием командной строки Windows, см. раздел Установка справочников и ключей в неинтерактивном режиме (на стр. 67).
- Если в результате программного или системного сбоя вы не можете войти в программу ViPNet Монитор и необходимо выполнить повторную установку справочников и ключей, см. раздел Повторная установка справочников и ключей после сбоя программы (на стр. 68).

В составе первоначального дистрибутива ключей каждому пользователю сети ViPNet передается резервный набор персональных ключей (РНПК) (на стр. 489). Файл, в котором содержится резервный набор ключей, имеет вид `AAAA.pk` (где `AAAA` — идентификатор пользователя в сети ViPNet). Во время установки справочников и ключей он помещается в папку ключей пользователя (см. «Папка ключей пользователя» на стр. 487).

Из соображений безопасности после первичной установки справочников и ключей рекомендуется переместить файл резервного набора из папки ключей пользователя на внешнее устройство для хранения в безопасном месте, не доступном для посторонних лиц (например, в сейфе). После получения резервного набора ключей пользователи сети ViPNet несут личную ответственность за его хранение.

Внимание! Если обнаружен факт доступа посторонних лиц к вашему резервному набору ключей либо если вы подозреваете, что такой факт имел место, следуйте рекомендациям раздела Действия при компрометации ключей (на стр. 75).

Установка справочников и ключей одного пользователя

Для установки справочников и ключей выполните следующие действия:

1. Получите дистрибутив ключей у администратора сети ViPNet.
2. Завершите работу всех компонентов программы ViPNet Coordinator (см. «Завершение работы с программой ViPNet Монитор» на стр. 87).
3. Запустите программу установки ключей сети ViPNet одним из двух способов:
   - Дважды щелкните файл дистрибутива ключей.
   - Запустите программу ViPNet Монитор. Затем в окне ввода пароля щелкните значок  справа от кнопки **Настройка** и в меню выберите пункт **Установить ключи**.

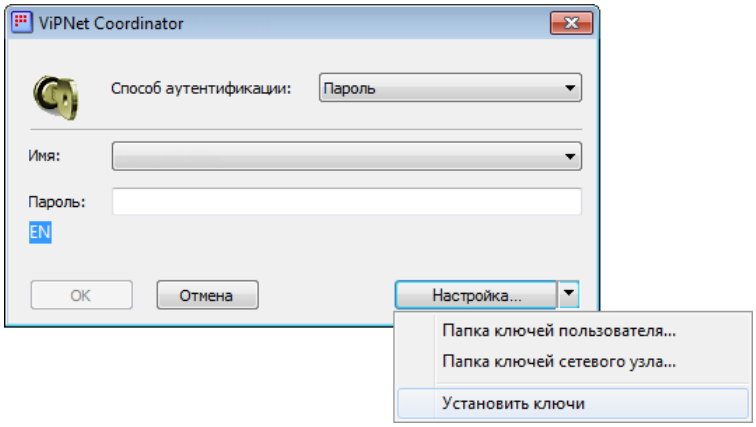


Рисунок 17: Запуск установки ключей

4 Если при запуске программы установки ключей будут обнаружены работающие приложения ViPNet, будет выведено сообщение о необходимости завершить их работу. Закройте указанные приложения и нажмите кнопку **Повтор**.

5 Если на странице **Укажите файл дистрибутива ключей** не указано местоположение файла дистрибутива, задайте его с помощью кнопки **Обзор**.

6 Убедитесь, что выбран дистрибутив ключей, предназначенный именно для текущего сетевого узла. Имя сетевого узла и имя пользователя отображаются ниже поля для указания пути к файлу дистрибутива. При необходимости укажите другой дистрибутив ключей.

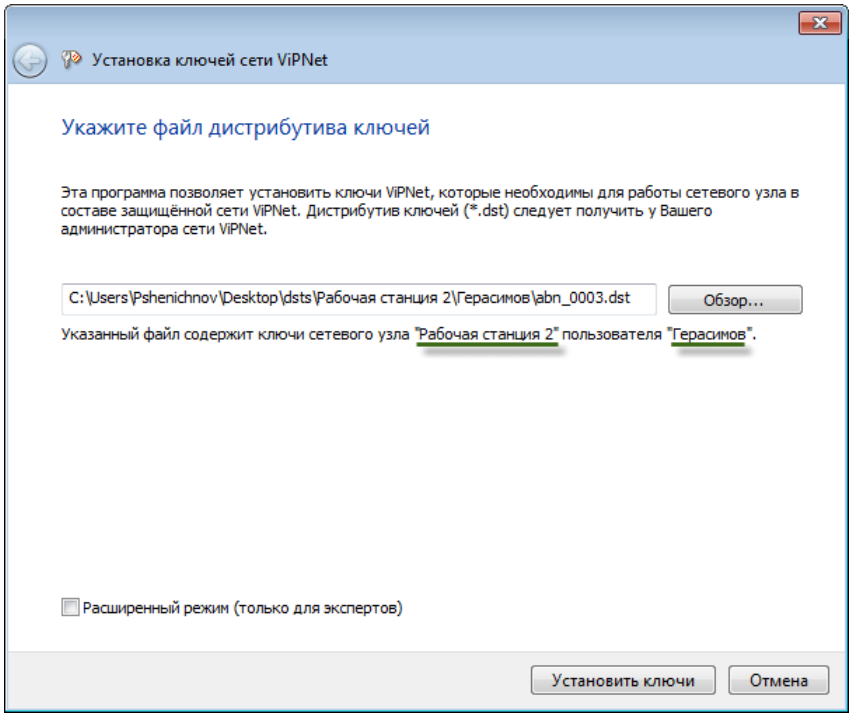


Рисунок 18: Выбор файла дистрибутива ключей

По умолчанию справочники и ключи устанавливаются в ту же папку, что и программа ViPNet Coordinator. При необходимости вы можете указать другие папки для их установки (см. «Расширенный режим установки справочников и ключей» на стр. 63).

7 Нажмите кнопку **Установить ключи**.

Примечание. Кнопка **Установить ключи** может быть скрыта в том случае, если на сетевом узле установлено несколько программ ViPNet (см. «Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet» на стр. 66).

---

8 Если установка ключей прошла успешно, появится соответствующее сообщение.

9 Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

После успешной установки ключей можно запустить ПО ViPNet Coordinator.

Установка справочников и ключей нескольких пользователей на одном сетевом узле

Если на сетевом узле планируется работа нескольких пользователей, установите ключи для каждого пользователя.

Если на сетевом узле уже работают пользователи, и вы хотите добавить на узел новых пользователей, для установки вам понадобятся только ключи новых пользователей.

Для установки справочников и ключей нескольких пользователей на одном компьютере выполните следующие действия:

1. Для каждого нового пользователя получите дистрибутив ключей у администратора сети ViPNet.
2. Последовательно выполните установку справочников и ключей (см. «Установка справочников и ключей одного пользователя» на стр. 60) с использованием дистрибутива каждого нового пользователя.

В результате в окне входа в программу в списке учетных записей будут отображаться пользователи, справочники и ключи которых вы установили.

Расширенный режим установки справочников и ключей

По умолчанию справочники и ключи устанавливаются в папку установки программы. При необходимости вы можете использовать расширенный режим установки, который позволяет вам самостоятельно задать папки для установки справочников и ключей. Такая необходимость может возникнуть, если:

- из соображений безопасности вы хотите хранить справочники и ключи на специальном съемном носителе;
- у вас нет прав на изменение и запись файлов в папке `C:\Program Files\` или `C:\Program Files (x86)\` (в том числе в папке установки программы).

Папки, в которые производится установка справочников и ключей в расширенном режиме установки, должны отвечать следующим требованиям:

- В папках не должны находиться справочники и ключи другой программы ViPNet.

- У вас должно быть право на изменение и запись файлов в данных папках.
- Информационная защита папок должна отвечать требованиям безопасности вашей организации.
- ПО ViPNet Coordinator должно иметь постоянный доступ к данным папкам.

Внимание! Неправильно заданные параметры установки могут привести к сбоям в работе программы. Не рекомендуется использовать данный режим без необходимости.

Для установки ключей в расширенном режиме выполните следующие действия:

1. Получите новый дистрибутив ключей у администратора сети ViPNet.
2. Следуйте указаниям раздела Установка справочников и ключей одного пользователя (на стр. 60).

   На странице указания файла дистрибутива ключей (см. Рисунок 18 на стр. 62) установите флажок **Расширенный режим (только для экспертов)** и нажмите кнопку **Далее**.
3. На следующей странице мастера:
   - В поле **Папка ключей сетевого узла** (на стр. 488) укажите папку для установки справочников и ключей сетевого узла.
   - В поле **Папка ключей пользователя** (на стр. 487) укажите папку для установки ключей пользователя.

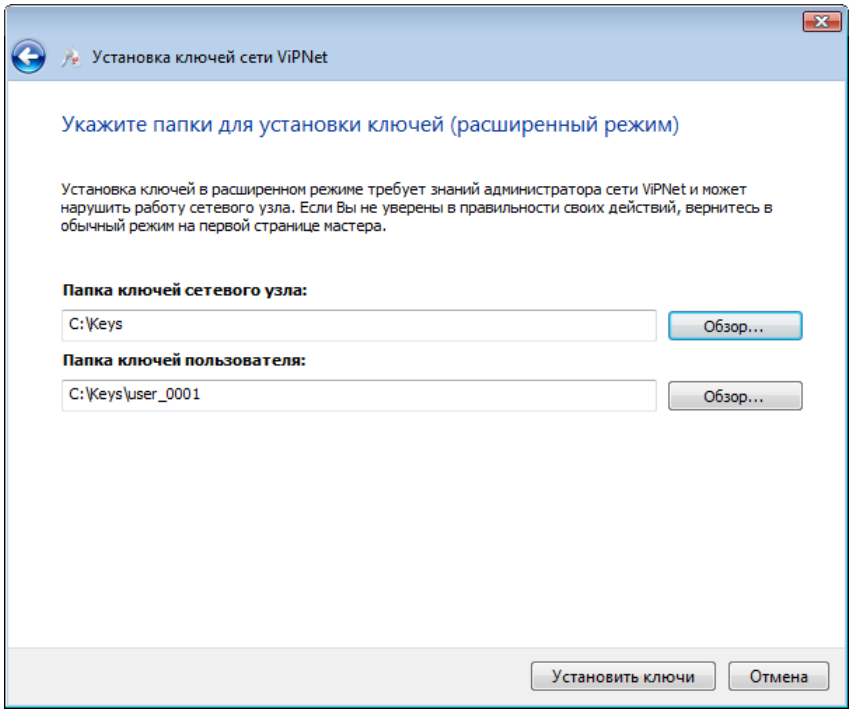


Рисунок 19: Указание папок для установки ключей узла и ключей пользователя в расширенном режиме

4 Для начала установки нажмите кнопку **Установить ключи**.

5 Если установка ключей прошла успешно, в завершающем окне будет выведено соответствующее сообщение. Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях**. Для завершения установки ключей нажмите кнопку **Закрыть**.

Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

6 При первом запуске программы ViPNet Coordinator укажите папки, в которые были установлены ключи сетевого узла и пользователя:

- В окне ввода пароля щелкните значок справа от кнопки **Настройка** и выберите пункт **Папка ключей сетевого узла**. В окне **Обзор папок** укажите путь к папке ключей узла.
- Снова щелкните значок справа от кнопки **Настройка** и выберите пункт **Папка ключей пользователя**. Укажите путь к папке ключей пользователя.

Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet

Если на сетевом узле установлено несколько программ ViPNet, но при этом ни для одной из них не установлены справочники и ключи, то необходимо указать приложение, в папке установки которого будут храниться справочники и ключи.

Внимание! Если на узле уже имеются справочники и ключи для какой-либо из программ ViPNet, устанавливать новые справочники и ключи нельзя. В этом случае выполните указания раздела Использование справочников и ключей, установленных ранее (на стр. 69).

Для установки справочников и ключей выполните следующие действия:

1. Начните установку справочников и ключей (см. «Установка справочников и ключей одного пользователя» на стр. 60). После указания файла дистрибутива ключей нажмите кнопку **Далее**.
2. В окне выбора приложения ViPNet выберите **ViPNet Coordinator**. В результате для установки справочников и ключей будет использована папка установки ПО ViPNet Coordinator.

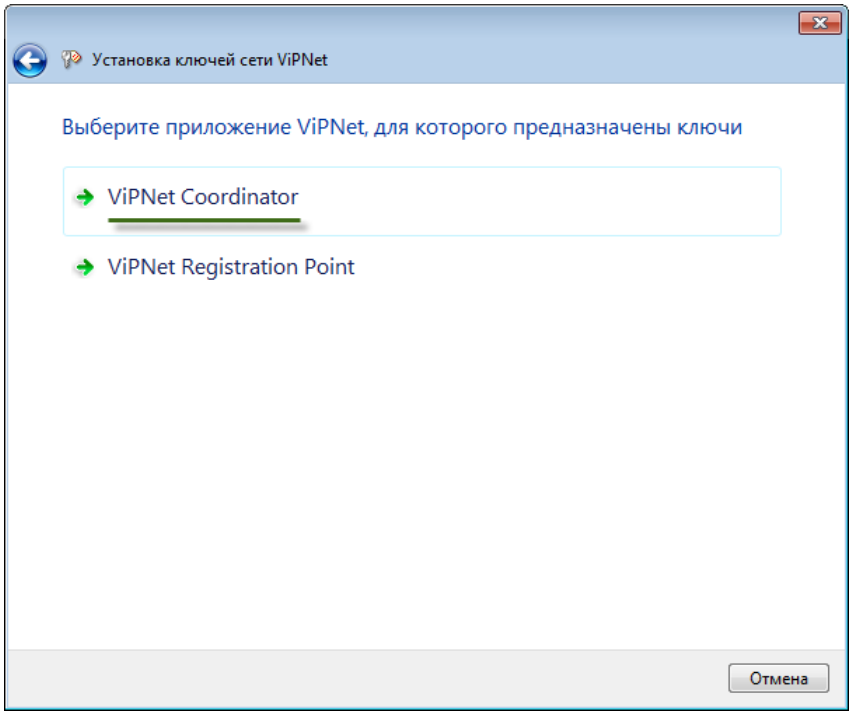


Рисунок 20: Выбор программы, для которой устанавливаются ключи

Примечание. В расширенном режиме установки ключей (см. «Расширенный режим установки справочников и ключей» на стр. 63) данное окно не отображается.

3 Если установка ключей прошла успешно, в завершающем окне будет выведено соответствующее сообщение. Для просмотра информации о выполненной установке ключей щелкните ссылку **Подробнее о произведенных действиях.** Для завершения установки ключей нажмите кнопку **Закрыть.**

   Если выполнить установку ключей не удалось, внимательно ознакомьтесь с сообщением о возникших ошибках и обратитесь к администратору сети ViPNet для их устранения.

4 При первом запуске других программ ViPNet, установленных на узле, в качестве папки ключей узла укажите папку установки программы ViPNet Coordinator.

После успешной установки ключей можно запустить ПО ViPNet Coordinator.

Установка справочников и ключей в неинтерактивном режиме

В неинтерактивном режиме процесс установки справочников и ключей не отображается на экране компьютера. Установку в данном режиме можно запустить с помощью командной строки Windows. Параметры установки, которые обычно могут быть заданы в процессе установки (см. «Установка справочников и ключей одного пользователя» на стр. 60), в неинтерактивном режиме следует указать заранее в командной строке.

Использование неинтерактивного режима позволяет вам выполнять удаленную установку справочников и ключей или создавать программы, которые обращаются к командной строке Windows и запускают автоматическую установку справочников и ключей с заданными параметрами.

Например, вы можете создать сценарий входа в систему (logon script), который запустит автоматическую установку справочников и ключей после загрузки системы (информацию о создании сценариев входа в систему можно найти на сайте компании Microsoft http://technet.microsoft.com/en-us/library/cc758918(v=ws.10).aspx).

Чтобы запустить программу установки справочников и ключей в неинтерактивном режиме, в командной строке Windows выполните команду:

```
keysetup <файл *.dst> /td <путь к папке для установки справочников и ключей>
/term /check
```

Например:

```
"C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator\keysetup"
"C:\keys\abn_0002.dst" /td "C:\Program Files (x86)\InfoTeCS\ViPNet
Coordinator" /term /check
```

Внимание! В качестве папки для установки справочников и ключей можно указывать только существующую папку. При указании несуществующей папки установка ключей произведена не будет.

После успешного выполнения данной команды можно запустить ПО ViPNet Coordinator.

Совет. Чтобы узнать больше о возможностях использования командной строки Windows для установки справочников и ключей, выполните команду:

```
keysetup /?
```

Повторная установка справочников и ключей после сбоя программы

Если в результате программного или системного сбоя вы не можете войти в программу ViPNet Монитор, рекомендуется обратиться в службу поддержки для восстановления доступа к программе. В исключительных случаях вы можете получить у администратора сети ViPNet новый дистрибутив ключей и выполнить повторную установку справочников и ключей.

Внимание! Крайне не рекомендуется проводить повторную установку ключей без особой необходимости, поскольку в этом случае может быть нарушена связь между сетевыми узлами, зарегистрированными на координаторе.

Для повторной установки справочников и ключей на сетевом узле выполните следующие действия:

1. Получите у администратора сети ViPNet новый дистрибутив ключей.
2. Установите справочники и ключи (см. «Установка справочников и ключей одного пользователя» на стр. 60), используя полученный дистрибутив.

Использование справочников и ключей, установленных ранее

В момент установки программы ViPNet Coordinator на сетевом узле уже могут иметься другие программы ViPNet, для работы которых установлены справочники, ключи сетевого узла и транспортный модуль MFTP. В этом случае задайте в программе ViPNet Coordinator папку ключей сетевого узла (см. «Папка ключей сетевого узла» на стр. 488), которую используют установленные ранее программы ViPNet.

Примечание. Если на сетевом узле не установлены справочники и ключи ни для одной из программ ViPNet, выполните указания раздела Установка справочников и ключей на сетевом узле с несколькими установленными программами ViPNet (на стр. 66).

Чтобы указать папку ключей сетевого узла, выполните следующие действия:

1. Запустите программу ViPNet Монитор.
2. В окне ввода пароля щелкните значок справа от кнопки **Настройка** и выберите пункт **Папка ключей сетевого узла**.
3. В окне **Обзор папок** укажите путь к нужной папке ключей узла.

Примечание. По умолчанию папка ключей сетевого узла совпадает с папкой установки программного обеспечения ViPNet.

После задания папки ключей сетевого узла вы можете приступать к работе с программой ViPNet Coordinator.

Обновление справочников, ключей и политик безопасности

Для поддержания работоспособности узла следует регулярно обновлять справочники, ключи и политики безопасности.

Если администратор сети ViPNet вносит какие-либо изменения в структуру сети или настройки отдельных сетевых узлов, например, создает новые связи между сетевыми узлами, то автоматически изменяются справочники и ключи для сетевых узлов. Обновления справочников и ключей создаются администратором сети в программе ViPNet Administrator или ViPNet Network Manager.

При изменениях правил безопасности в сети ViPNet администратор безопасности рассылает на сетевые узлы обновленные политики безопасности. Политика безопасности, полученная сетевым узлом из программы ViPNet Policy Manager, определяет текущую политику безопасности узла, совместно с сетевыми фильтрами, настроенными на самом узле (см. «Общие сведения о сетевых фильтрах» на стр. 159). Текущая политика безопасности узла действительна для всех пользователей, зарегистрированных на узле, и для всех конфигураций программы ViPNet Монитор. При добавлении новых пользователей или конфигураций к ним также применяется текущая политика.

Обновления справочников, ключей и политик безопасности могут быть приняты на сетевом узле с помощью системы обновления ViPNet (см. «О системе обновления ViPNet» на стр. 95). Если по каким-либо причинам обновление справочников и ключей с помощью системы обновления не может быть выполнено, вы можете выполнить его вручную с помощью дистрибутива ключей (см. «Обновление справочников и ключей с помощью дистрибутива ключей» на стр. 71).

Прием централизованных обновлений

Обновления справочников и ключей передаются на сетевые узлы из программы ViPNet Administrator или ViPNet Network Manager, а обновления политик безопасности — из программы ViPNet Policy Manager.

Обновления справочников, ключей и политик безопасности можно принять на сетевом узле с помощью системы обновления ViPNet (см. «О системе обновления ViPNet» на стр. 95). В зависимости от настроек системы обновления, данные обновления могут быть приняты на сетевом узле автоматически сразу после их получения либо обновление потребуется выполнить вручную.

Обновление справочников и ключей с помощью дистрибутива ключей

Если по каким-либо причинам обновление справочников и ключей не может быть принято по сети (см. «Обновление справочников, ключей и политик безопасности» на стр. 70), вы можете выполнить обновление вручную с помощью дистрибутива ключей. Для этого:

1 Получите новый дистрибутив ключей у администратора сети ViPNet.

Следуйте указаниям раздела Установка справочников и ключей одного пользователя (на стр. 60) с использованием нового дистрибутива.

При указании дистрибутива ключей (см. Рисунок 18 на стр. 62) автоматически проверяется соответствие между установленными ранее ключами и новыми ключами, которые находятся в указанном файле дистрибутива ключей (например, предназначены ли данные ключи для одного и того же сетевого узла).

Внимание! При установке ключей в расширенном режиме (см. «Расширенный режим установки справочников и ключей» на стр. 63) данное сопоставление ключей производиться не будет.

2 Для установки справочников и ключей нажмите кнопку **Установить ключи** (см. Рисунок 18 на стр. 62).

Если кнопка недоступна, это значит, что обнаружены несоответствия между новыми и установленными ранее ключами. Для получения информации о выявленных несоответствиях нажмите кнопку **Далее**. В зависимости от характера несоответствия появится сообщение одного из двух типов:

- Если выбранный дистрибутив содержит ключи другого сетевого узла, формат ключей в дистрибутиве отличается от формата текущих ключей, а также в ряде других случаев будет выведено предупреждение, содержащее описание выявленного несоответствия.

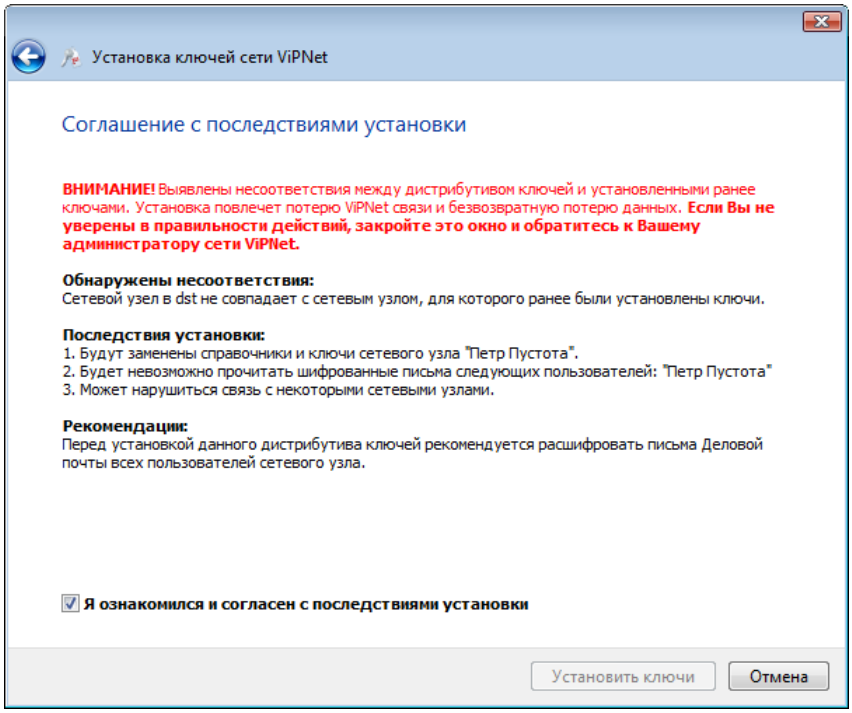


Рисунок 21: Обнаружено несоответствие между дистрибутивом и текущими ключами на узле

- Чтобы отказаться от установки ключей, нажмите кнопку **Отмена**, затем в окне подтверждения нажмите кнопку **Да**.

Внимание! Если вы хотите продолжить установку, ознакомьтесь с информацией о возможных последствиях и проконсультируйтесь у администратора вашей сети ViPNet. Перед продолжением установки рекомендуется завершить работу мастера с помощью кнопки **Отмена**, расшифровать письма программы ViPNet Деловая почта и затем повторно запустить мастер установки ключей.

- Для продолжения установите флажок **Я ознакомился и согласен с последствиями установки**, затем нажмите кнопку **Установить ключи**.

- Если выбранный дистрибутив не может быть установлен (например, он создан для другой программы ViPNet), будет выведено сообщение об ошибке, и дальнейшая установка будет невозможна. Ознакомьтесь с информацией о выявленном несоответствии и нажмите кнопку **Закрыть**.

В случае отказа от установки в результате несоответствий новых и установленных ранее ключей обратитесь за помощью к администратору сети ViPNet.

3 Завершите установку согласно указаниям раздела Установка справочников и ключей одного пользователя (на стр. 60).

После успешного обновления ключей можно запустить ПО ViPNet.

Удаление справочников и ключей

Удаление справочников и ключей может потребоваться при переносе сетевого узла на другой компьютер (см. «Перенос сетевого узла на другой компьютер» на стр. 55).

Чтобы удалить справочники и ключи, завершите работу с программой (см. «Завершение работы с программой ViPNet Монитор» на стр. 87), затем в командной строке Windows выполните команду:

```
keysetup /clean /td <папка, в которой находятся справочники и ключи>
```

Например:

```
"C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator\keysetup" /clean / td
"C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator"
```

В результате выполнения данной команды все справочники и ключи, находящиеся в указанной папке, будут удалены.

Если вы хотите удалить ключи только одного из пользователей сетевого узла с сохранением возможности работы на узле для других пользователей, то в параметрах удаления укажите папку ключей данного пользователя, например:

```
"C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator\keysetup" /clean / td
"C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator\user_0003"
```

Действия при компрометации ключей

Под компрометацией ключей подразумевается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Различают явную и неявную компрометацию ключей:

- Явной называют компрометацию, факт которой становится известным в течение срока действия данного ключа.
- Неявной называют компрометацию ключа, факт которой остается неизвестным для лиц, являющихся законными пользователями данного ключа. Неявная компрометация представляет наибольшую опасность.

Основные события, при которых ключи можно считать скомпрометированными, перечислены ниже:

1. Посторонним лицам мог стать доступным файл дистрибутива ключей.
2. Посторонним лицам могло стать доступным внешнее устройство с ключами пользователя.
3. Посторонним лицам мог стать доступным пароль пользователя, и эти лица могли иметь доступ к компьютеру пользователя.
4. Посторонние лица могли получить неконтролируемый физический доступ к ключам пользователя, хранящимся на компьютере.
5. На компьютере, подключенном к сети, не установлена программа ViPNet Монитор или в программе была отключена защита трафика. При этом:
   - в локальной сети возможно присутствие посторонних лиц;
   - на границе локальной сети отсутствует (отключен) межсетевой экран.
6. Был уволен сотрудник, имевший доступ к ключам.
7. Входящий документ подписан сертификатом, находящимся в списке отозванных сертификатов.
8. Случаи, когда нельзя достоверно установить, что произошло с внешними устройствами (например, внешнее устройство вышло из строя, и существует

возможность того, что это произошло в результате несанкционированных действий злоумышленника).

К событиям, требующим проведения расследования и принятия решения на предмет произошла ли компрометация, также относится возникновение подозрений в утечке информации или ее искажение в системе конфиденциальной связи.

При наступлении любого из перечисленных выше событий:

- Немедленно прекратите работу на сетевом узле и сообщите о факте компрометации (или предполагаемом факте компрометации) администратору сети ViPNet.
- Если скомпрометированы только ключи подписи, прекратите использование этих ключей для подписи документов и сообщите администратору сети ViPNet.
- Если есть подозрение, что посторонние лица могут знать пароль пользователя ViPNet, но эти посторонние лица не имеют доступа к компьютеру, смените пароль и продолжайте работу. Если доступ посторонних лиц к компьютеру пользователя возможен, то следует считать ключи скомпрометированными.

В сети ViPNet CUSTOM на случай компрометации ключей пользователя предусмотрена возможность дистанционного обновления ключей с помощью резервного набора персональных ключей (РНПК). Файл резервного набора (`AAAA.pk`, где AAAA — идентификатор пользователя в сети ViPNet) входит в состав первоначального дистрибутива ключей и при установке справочников и ключей помещается в папку ключей пользователя (см. «Установка справочников и ключей» на стр. 59).

Если текущий персональный ключ пользователя оказался скомпрометирован, администратор программы ViPNet Удостоверяющий и ключевой центр высылает пользователю новые ключи, защищенные с помощью очередного варианта персонального ключа, который не нужно передавать по сети, так как он уже содержится в резервном наборе. Если при обновлении файл резервного набора не найден, требуется указать путь к этому файлу. Если резервный набор персональных ключей отсутствует или не подходит пароль, откажитесь от ввода данных и обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр, чтобы получить его копию.

Начало работы с программой ViPNet Coordinator

Запуск программы ViPNet Монитор

По умолчанию ViPNet-драйвер активирует защиту трафика во время загрузки операционной системы Windows.

Внимание! Работа ViPNet-драйвера до аутентификации пользователя ViPNet определяется предустановленными фильтрами защищенной сети и фильтрами открытой сети, которые использовались в предыдущем сеансе работы.

Перед окончанием загрузки Windows появится окно входа в программу ViPNet Монитор. Для запуска программы введите пароль или подключите внешнее устройство аутентификации (см. «Способы аутентификации пользователя» на стр. 80). Чтобы отказаться от запуска программы ViPNet Монитор, нажмите кнопку **Отмена**, в этом случае защита трафика будет отключена.

Примечание. Чтобы выполнить аутентификацию в программе ViPNet Монитор во время загрузки Windows, вы можете использовать экранную клавиатуру. Для этого нажмите кнопку  и в меню выберите пункт **Экранная клавиатура**.

Если вы вышли из программы (см. «Завершение работы с программой ViPNet Монитор» на стр. 87) или отказались от аутентификации при загрузке Windows, то для запуска программы ViPNet Монитор:

1. Выполните одно из действий:
   - В меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Coordinator** > **Монитор** (во время установки положение программы в меню **Пуск** могло быть изменено).
   - Дважды щелкните ярлык  на рабочем столе (ярлык отображается на рабочем столе, если при установке программы была выбрана соответствующая опция).

   Откроется окно входа в программу.

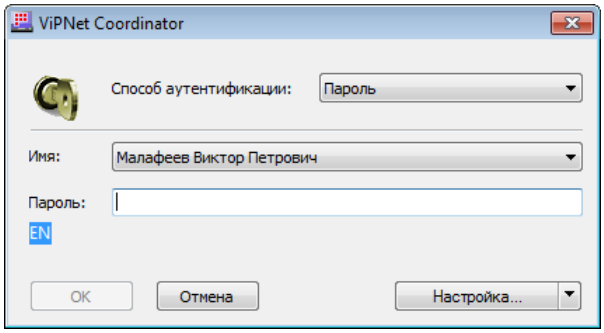


Рисунок 22: Окно входа в программу

2 Выберите способ аутентификации для входа в программу (см. «Способы аутентификации пользователя» на стр. 80) и в зависимости от выбранного способа введите пароль пользователя либо подключите внешнее устройство и введите ПИН-код.

Если на вашем компьютере работает несколько пользователей ViPNet Coordinator и для аутентификации вы используете пароль, в списке **Имя** выберите ваше имя пользователя.

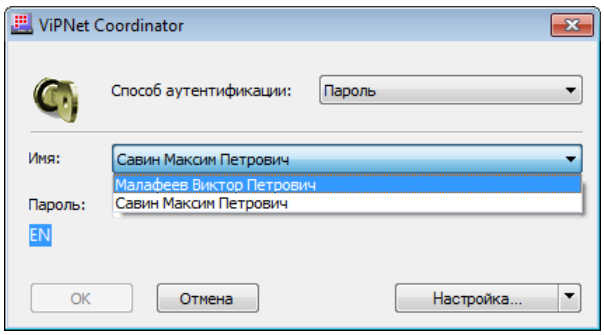


Рисунок 23: Выбор учетной записи пользователя

3 После ввода необходимых для аутентификации данных нажмите кнопку **OK**. Откроется окно программы ViPNet Монитор (см. «Интерфейс программы ViPNet Монитор» на стр. 88).

Особенности запуска ViPNet Coordinator на терминальных серверах в консольной и удаленной сессии

Терминальный сервер (например, Windows Server 2008) позволяет осуществить запуск нескольких пользовательских сессий. По соображениям безопасности и в целях обеспечения стабильной работы ПО ViPNet Монитор позволяет запустить только одну

копию программы, поэтому успешный запуск программы ViPNet Монитор в любой из сессий автоматически запрещает его запуск в любой другой сессии.

Для загрузки программы ViPNet Монитор в удаленной сессии необходимо удостоверится, что запуск программы удаленно разрешен:

1. Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304).
2. В разделе **Администратор** удостоверьтесь, что установлен флажок **Разрешить запуск монитора в удалённой сессии.**

Способы аутентификации пользователя

В программе ViPNet Монитор предусмотрено три способа аутентификации:

- Пароль (на стр. 82). Для входа в программу вам следует ввести свой пароль. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу.
- Пароль на устройстве (на стр. 83). Для входа в программу вам следует подключить устройство и ввести ПИН-код.

  Как правило, использование этого способа аутентификации предполагает, что ваш пароль хранится на устройстве и вам не известен. Однако если вы знаете пароль, то помимо аутентификации с помощью внешнего устройства для входа в программу можно использовать аутентификацию по паролю. Данная возможность обеспечивает вход в программу в случае неисправности внешнего устройства (для этого вам понадобится узнать свой пароль у администратора сети ViPNet).

Внимание! Способ аутентификации **Пароль на устройстве** не отвечает требованиям безопасности, и возможность его использования оставлена исключительно для совместимости с программным обеспечением ViPNet более ранних версий. В связи с этим, если программа ViPNet Монитор была обновлена до версии 4.x и в ней используется данный способ аутентификации, то настоятельно рекомендуется его изменить на **Пароль** или **Устройство.**

- Устройство (на стр. 84). Для входа в программу вам следует подключить устройство и ввести ПИН-код (и в некоторых случаях пароль).

По умолчанию установлен способ аутентификации **Пароль.** В режиме администратора можно изменить способ аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 312).

При использовании способов **Пароль на устройстве** и **Устройство** аутентификация пользователя осуществляется с помощью внешних устройств (см. «Внешние устройства» на стр. 438). Чтобы использовать какое-либо устройство для аутентификации пользователя, на компьютер необходимо установить драйверы этого устройства и затем записать ключи на это устройство. Записать ключи на внешнее устройство можно при изменении способа аутентификации пользователя или в программе ViPNet Удостоверяющий и ключевой центр при создании дистрибутива ключей (в программе ViPNet Network Manager работа с внешними устройствами невозможна).

Внимание! Если при использовании способов аутентификации **Пароль на устройстве** или **Устройство** внешнее устройство будет отключено, может произойти автоматическая блокировка компьютера — в соответствии с настройками, заданными в режиме администратора (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305). Для продолжения работы необходимо вновь подключить это внешнее устройство.

На схеме ниже представлены факторы аутентификации, используемые при выборе каждого способа аутентификации в зависимости от типа внешнего устройства.

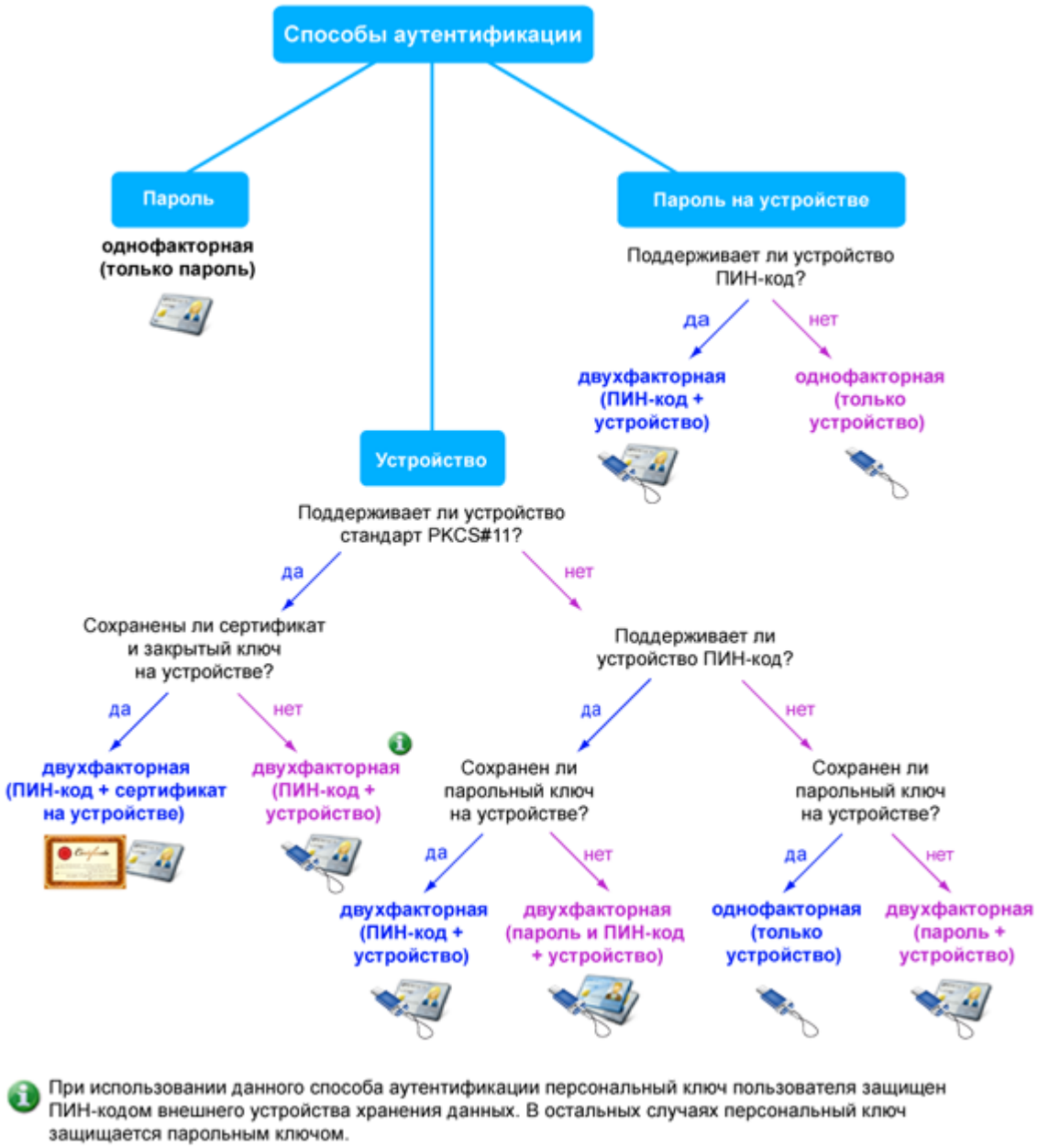


Рисунок 24: Схема соответствия между факторами и способами аутентификации

Пароль

Для входа в программу ViPNet Монитор с помощью пароля в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Пароль**.

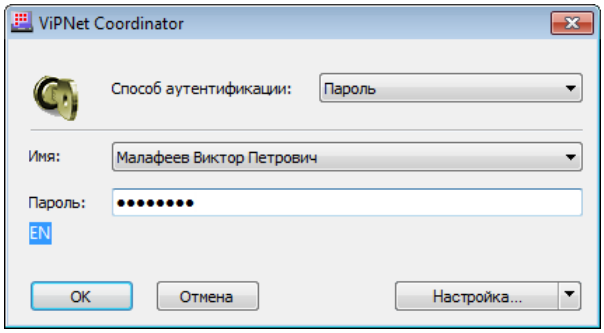


Рисунок 25: Способ аутентификации «Пароль»

2 При необходимости в списке **Имя** выберите ваше имя пользователя ViPNet.

Примечание. В данном списке отображаются имена всех пользователей, ключи которых были установлены на данном сетевом узле (см. «Установка справочников и ключей» на стр. 59). Если на узле не установлены ключи ни одного пользователя, список будет пуст.

3 В поле **Пароль** введите ваш пароль.

Если сохранение пароля в реестре разрешено настройками программы (см. «Дополнительные настройки параметров безопасности» на стр. 311), для сохранения пароля можно установить соответствующий флажок.

4 Нажмите кнопку **OK**.

Пароль на устройстве

Внимание! Во избежание неполадок в работе ПО ViPNet не следует использовать способ аутентификации **Пароль на устройстве**. При использовании данного способа аутентификации рекомендуется его изменить на **Пароль** или **Устройство** (см. «Изменение способа аутентификации пользователя» на стр. 312).

Для входа в программу ViPNet Монитор с помощью пароля на устройстве в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Пароль на устройстве**.

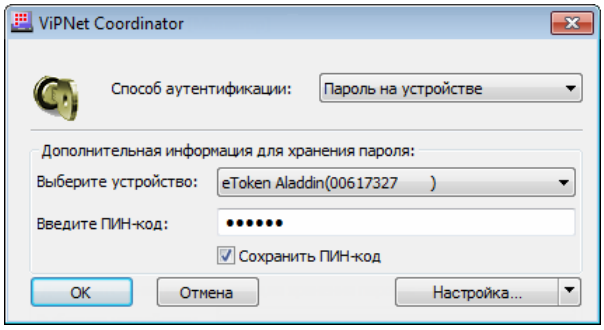


Рисунок 26: Способ аутентификации «Пароль на устройстве»

2 Подключите внешнее устройство, на котором находится ваш пароль.

3 В списке **Выберите устройство** выберите внешнее устройство.

4 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства (см. Рисунок 24 на стр. 82).

Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, установите соответствующий флажок.

5 Нажмите кнопку **OK**.

Устройство

Для входа в программу ViPNet Монитор с помощью устройства в окне аутентификации выполните следующие действия:

1 В списке **Способ аутентификации** выберите **Устройство**.

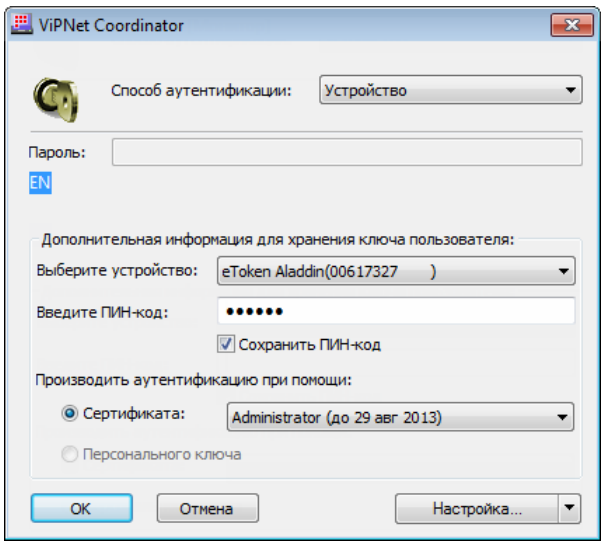


Рисунок 27: Способ аутентификации «Устройство»

2 Подключите внешнее устройство.

3 Если требуется, в списке ниже выберите ваше имя пользователя и в поле **Пароль** введите свой пароль. Необходимость ввода пароля зависит от типа используемого внешнего устройства (см. Рисунок 24 на стр. 82).

4 В списке **Устройство** выберите внешнее устройство, на котором находится ваш персональный ключ или сертификат с закрытым ключом подписи.

5 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства. Чтобы сохранить ПИН-код и в дальнейшем не вводить его при аутентификации, установите соответствующий флажок.

6 В списке **Производить аутентификацию при помощи** установите переключатель в одно из следующих положений:

- **Сертификата** — чтобы выполнить аутентификацию с помощью вашего сертификата и соответствующего ему закрытого ключа, хранящегося в контейнере ключей на используемом устройстве. В списке сертификатов, обнаруженных на устройстве, выберите нужный сертификат. В случае возникновения затруднений при аутентификации с помощью сертификата см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 371).

Примечание. Для аутентификации с помощью сертификата должны быть выполнены следующие условия:

- Внешнее устройство хранения данных поддерживает стандарт PKCS#11, в том числе операции подписи и шифрования. В текущий момент внешние устройства с поддержкой алгоритма ГОСТ 34.10-2001 использоваться не могут, поскольку они поддерживают только операцию вычисления подписи.
- Сертификат действителен (срок действия сертификата не истек).
- Сертификат не отозван.
- Сертификат имеет назначение «Проверка подлинности клиента». Это назначение отображается в окне **Сертификат**, на вкладке **Состав**, в поле **Расширенное использование ключа**.
- Сертификат издателя установлен в системное хранилище **Доверенные корневые центры сертификации**.

- **Персонального ключа** — чтобы выполнить аутентификацию с помощью персонального ключа (который входит в состав ключей пользователя и хранится на используемом устройстве).

7 Нажмите кнопку **OK**.

Смена пользователя

Если на сетевом узле зарегистрировано несколько пользователей, сменить пользователя можно, не выходя из программы ViPNet Монитор. Для этого выполните следующие действия:

1 В главном меню программы выберите пункт **Файл** > **Сменить пользователя**. Откроется окно входа в программу.

2 Выберите способ аутентификации для входа в программу (см. «Способы аутентификации пользователя» на стр. 80) и в зависимости от выбранного способа введите пароль пользователя либо подключите внешнее устройство и введите ПИН-код.

Если на вашем компьютере работает несколько пользователей ViPNet Coordinator и для аутентификации вы используете пароль, в списке **Имя** выберите ваше имя пользователя.

Примечание. На сетевом узле должны быть предварительно установлены ключи пользователя (см. «Установка справочников и ключей» на стр. 59), от имени которого выполняется вход в программу.

3 Нажмите кнопку **OK**.

Завершение работы с программой ViPNet Монитор

Существует несколько способов завершения работы с программой ViPNet Coordinator:

1. Чтобы свернуть окно программы, выполните одно из действий:
   - Нажмите кнопку **Закрыть**  в правом верхнем углу окна.
   - Нажмите сочетание клавиш **Alt+F4**.

   Чтобы снова развернуть окно программы, щелкните значок  в области уведомлений на панели задач.
2. Чтобы выйти из программы, в главном меню программы выберите пункт **Файл** > **Выход** либо в области уведомлений в контекстном меню программы ViPNet Coordinator выберите пункт **Выход**. В окне подтверждения нажмите **Да**.

Примечание. После выхода из программы ViPNet Coordinator работа ViPNet-драйвера продолжается: он фильтрует IP-трафик в соответствии с фильтрами, заданными в настройках интегрированного сетевого экрана.

Интерфейс программы ViPNet Монитор

Окно программы ViPNet Монитор представлено на рисунке ниже:

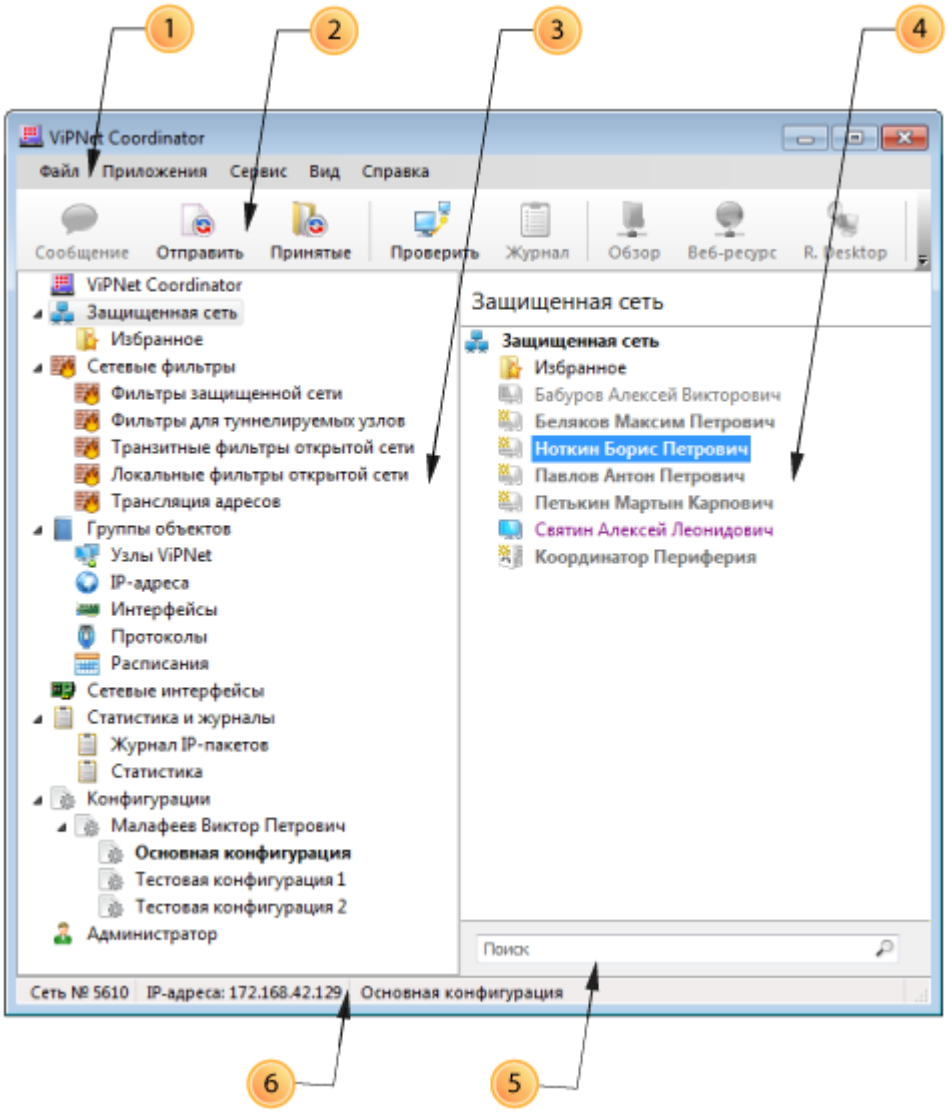


Рисунок 28: Окно программы ViPNet Coordinator Монитор

Цифрами на рисунке обозначены:

1. Главное меню программы.
2. Панель инструментов. Чтобы отобразить или скрыть панель инструментов, в меню **Вид** выберите пункт **Панель инструментов**. Добавить или удалить кнопки на панель инструментов вы можете с помощью кнопки  . Чтобы изменить расположение кнопок на панели инструментов, перетащите их в нужном порядке, удерживая нажатой клавишу **Alt**.
3. Панель навигации. Содержит перечень разделов, предназначенных для настройки различных параметров ViPNet Монитор:
   - **Защищенная сеть** (этот раздел выбран по умолчанию) — содержит список сетевых узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью или ViPNet Network Manager. Подробнее см. Работа со списком защищенных узлов ViPNet (на стр. 91).
   - **Сетевые фильтры**. Содержит подразделы с фильтрами IP-трафика:
     - **Фильтры защищенной сети** — предназначен для настройки фильтров защищенного трафика (см. «Создание фильтров для защищенной сети» на стр. 180).
     - **Фильтры для туннелируемых узлов** — предназначен для настройки фильтров трафика туннелируемых узлов (см. «Защита трафика открытых узлов (туннелирование)» на стр. 217).
     - **Транзитные фильтры открытой сети** — предназначен для настройки фильтров транзитного открытого трафика (см. «Создание транзитных фильтров для открытой сети» на стр. 184).
     - **Локальные фильтры открытой сети** — предназначен для настройки фильтров локального открытого трафика.
     - **Трансляция адресов** — предназначен для задания правил трансляции IP-адресов открытых узлов (см. «Трансляция сетевых адресов (NAT)» на стр. 206).
   - **Группы объектов** — содержит списки объектов, которые могут быть использованы при создании сетевых фильтров: группы узлов ViPNet, группы IP-адресов и так далее (см. «Использование групп объектов» на стр. 163).
   - **Сетевые интерфейсы** — содержит список сетевых интерфейсов, установленных на компьютере.
   - **Статистика и журналы**. Содержит подразделы:
     - **Журнал IP-пакетов** — предназначен для поиска записей в журнале IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 274).

- **Статистика —** предназначен для просмотра статистики фильтрации IP-пакетов (см. «Просмотр статистики фильтрации IP-пакетов» на стр. 289).

- **Конфигурации** — предназначен для управления конфигурациями программы ViPNet Монитор (см. «Управление конфигурациями программы» на стр. 291).
- **Администратор** — отображается только после входа в программу в режиме администратора и служит для настройки дополнительных параметров программы (см. «Работа в программе в режиме администратора» на стр. 304).

Примечание. Количество и порядок расположения разделов на панели навигации зависит от уровня полномочий пользователя, который определяется в ViPNet Центр управления сетью (в сетях ViPNet CUSTOM) (см. «Использование программы ViPNet Монитор в условиях ограниченных полномочий» на стр. 92). В сетях ViPNet VPN уровень полномочий для пользователей не задается.

---

4 Панель просмотра. Предназначена для отображения раздела, выбранного на панели навигации (**3**).

5 Строка поиска. Отображается в разделах **Защищенная сеть**, **Сетевые фильтры** и **Группы объектов**. Для поиска по разделу введите в этой строке часть адреса, имени сетевого узла или другие параметры.

В разделе **Защищенная сеть** поиск выполняется по следующим параметрам:

- Имя узла (отображается в разделе **Защищенная сеть** и в окне **Свойства узла** на вкладке **Общие**).
- Имя компьютера (окно **Свойства узла**, вкладка **Общие**).
- Псевдоним (окно **Свойства узла**, вкладка **Общие**).
- Реальные и виртуальные IP-адреса (окно **Свойства узла**, вкладка **IP-адреса**, список **IP-адреса**).
- DNS-имя (окно **Свойства узла**, вкладка **IP-адреса**, список **DNS-имя**).
- Идентификатор узла (окно **Свойства узла**, вкладка **Общие**).

Чтобы очистить строку поиска, нажмите кнопку **Показать все**.

6 Строка состояния. Содержит следующие сведения: номер сети ViPNet, IP-адреса, назначенные узлу, и текущая конфигурация программы. При изменении сетевых фильтров или групп объектов вместо указанных сведений в строке состояния появляется сообщение о том, что фильтры или группы объектов были изменены, но не применены.

Чтобы показать или скрыть строку состояния, в меню **Вид** выберите пункт **Строка состояния.** При изменении фильтров или групп объектов строка состояния отображается всегда, даже если она была ранее скрыта.

Работа со списком защищенных узлов ViPNet

Раздел **Защищенная сеть** (см. «Интерфейс программы ViPNet Монитор» на стр. 88) содержит список защищенных узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью или ViPNet Network Manager.

Значок рядом с именем сетевого узла, а также цвет имени обозначают тип сетевого узла и его текущий статус:

Таблица 3. Обозначение статуса сетевых узлов

Значок	Цвет имени	Статус сетевого узла
	Серый	Клиент в данный момент отключен от сети либо нет данных о его статусе
	Фиолетовый	Клиент в данный момент подключен к сети
	Серый или фиолетовый, полужирный	Новый клиент, с которым была создана связь
	Серый или фиолетовый, полужирный	Новый координатор, с которым была создана связь
	Серый	Координатор в данный момент отключен от сети либо нет данных о его статусе
	Фиолетовый	Координатор в данный момент подключен к сети

Примечание. Чтобы настроить параметры внешнего вида раздела **Защищенная сеть**, выберите в окне программы ViPNet Монитор в меню **Сервис** пункт **Настройка приложения** и далее перейдите к разделу **Общие**.

Для удобства просмотра списка и поиска сетевые узлы в разделе **Защищенная сеть** можно сгруппировать по папкам:

- Чтобы создать новую папку, в окне программы ViPNet Монитор на панели навигации или на панели просмотра в контекстном меню элемента **Защищенная сеть** выберите пункт **Создать папку**.

  Новая папка появится на панели навигации, а также в разделе **Защищенная сеть**.

- Чтобы перенести сетевые узлы в какую-либо папку, в разделе **Защищенная сеть** выберите один или несколько сетевых узлов и перетащите их в нужную папку.
- Чтобы переименовать папку, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Переименовать.**
- Чтобы удалить папки:
  - Убедитесь, что папки, которые требуется удалить, не содержат сетевых узлов. В противном случае перенесите сетевые узлы в другие папки.
  - Выберите одну или несколько папок на панели навигации или в разделе **Защищенная сеть.**
  - Нажмите клавишу **Delete** либо воспользуйтесь пунктом **Удалить** в контекстном меню.

Для поиска сетевого узла в списке введите в строку поиска часть имени, IP-адреса или другие параметры узла.

Для просмотра свойств сетевого узла дважды щелкните имя узла. Откроется окно **Свойства узла**, в котором приведены общие сведения о сетевом узле и содержатся параметры доступа к узлу (см. «Настройка доступа к узлам сети ViPNet» на стр. 121).

Чтобы проверить соединение с другим узлом, начать сеанс обмена защищенными сообщениями, отправить файл или использовать другие встроенные функции программы ViPNet Монитор (см. «Встроенные средства коммуникации» на стр. 251), выполните одно из действий:

- Выберите сетевой узел в списке и нажмите соответствующую кнопку на панели инструментов.
- Выберите соответствующий пункт в контекстном меню сетевого узла.

Использование программы ViPNet Монитор в условиях ограниченных полномочий

Возможности использования программы ViPNet Монитор и изменения ее параметров на узлах сетей ViPNet CUSTOM могут быть ограничены уровнем полномочий пользователя. Кроме этого, интерфейс программы ViPNet Монитор может быть ограничен в режиме администратора сетевого узла (см. «Работа в программе в режиме администратора» на стр. 304). В сетях ViPNet VPN уровень полномочий не задается: на координаторах всегда используется максимальный уровень полномочий, на клиентах — уровень полномочий, при котором интерфейс программы ограничен.

Если полномочия пользователя ограничены, могут быть скрыты определенные элементы интерфейса программы ViPNet Монитор, может быть заблокировано изменение параметров программы, сетевых фильтров и так далее. При входе в программу в режиме администратора все ограничения снимаются.

В данном документе возможности программы ViPNet Монитор описаны с точки зрения пользователя, полномочия которого не ограничены. Если для вас недоступны какие-либо функции или настройки программы, обратитесь к администратору вашей сети ViPNet.

Подробная информация о полномочиях пользователя содержится в документе «Классификация полномочий. Приложение к документации ViPNet CUSTOM».

5

Система обновления ViPNet

О системе обновления ViPNet

Система обновления ViPNet обеспечивает получение и установку обновлений следующих типов:

- обновления ПО ViPNet Coordinator, полученные из программы ViPNet Administrator или ViPNet Network Manager;
- обновления справочников и ключей, полученные из программы ViPNet Administrator или ViPNet Network Manager;
- обновления политик безопасности, полученные из программы ViPNet Policy Manager.

Установка обновлений может осуществляться как в автоматическом режиме (см. «Автоматическая установка обновлений» на стр. 97), так и вручную (см. «Установка обновлений вручную» на стр. 99).

Если на узле настроена установка обновлений вручную, то при поступлении файлов обновления в области уведомлений отображается значок **Система обновления ViPNet** и соответствующая информация.

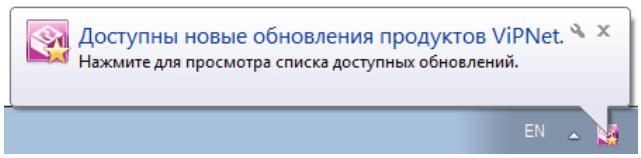


Рисунок 29: Отображение наличия обновлений в области уведомлений

Значок **Система обновления ViPNet** в области уведомлений может принимать следующий вид:

- — доступны новые обновления;
- — обновления успешно установлены;
- — обновления успешно установлены, необходима перезагрузка.

После установки обновлений, если не требуется перезагрузка, значок системы перестает отображаться в области уведомлений.

Если же на узле настроена автоматическая установка обновлений, то все операции система обновления ViPNet будет производить в «тихом» режиме без выдачи сообщений на экран. В области уведомлений значок системы будет отображаться только, если требуется перезагрузка компьютера (значок будет иметь вид ).

Автоматическая установка обновлений

Совет. Не рекомендуется настраивать автоматическое принятие обновлений в том случае, если вы планируете работу с защищенными контейнерами SafeDisk-V. Независимо от выбранного режима установки обновлений, в процессе работы с контейнерами SafeDisk-V поступающие обновления можно установить только вручную.

Если вы хотите, чтобы обновления устанавливались на узле автоматически, выполните следующие действия:

1. Войдите в операционную систему с правами администратора.

   Без прав администратора вы не сможете изменить настройки системы обновления ViPNet.

2. В меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления**.

3. В открывшемся окне на вкладке **Параметры** установите флажок **Устанавливать обновления автоматически**.

4. Если вы хотите, чтобы, когда это необходимо, после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.

5. Для сохранения настроек нажмите кнопку **OK.**

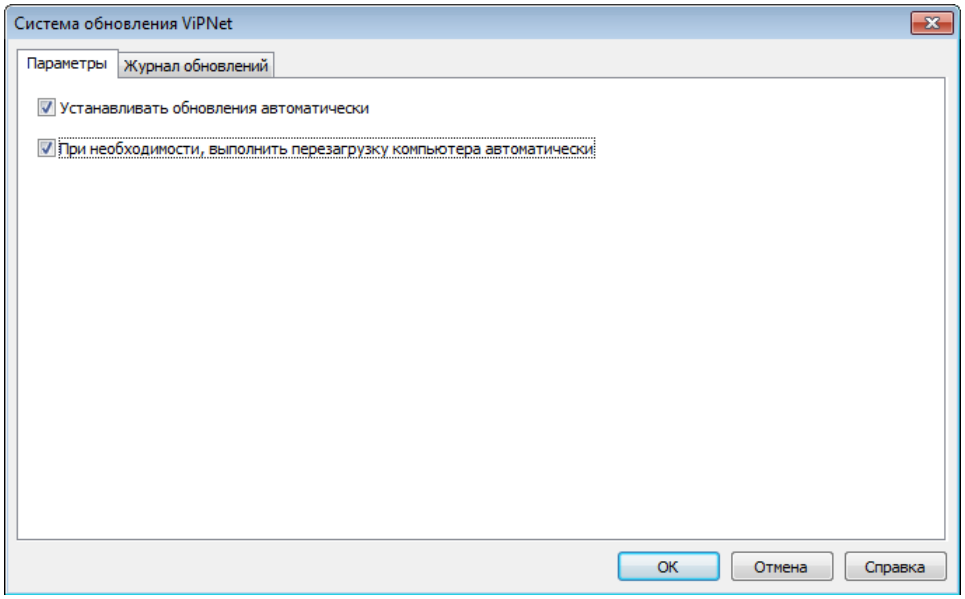


Рисунок 30: Настройка автоматической установки обновлений

Установка обновлений вручную

Если вы хотите самостоятельно контролировать установку обновлений на сетевом узле, отключите автоматическую установку обновлений. Для этого выполните следующие действия (см. Рисунок 30 на стр. 98):

1. Войдите в операционную систему с правами администратора.

   Без прав администратора вы не сможете изменить настройки системы обновления ViPNet.

2. В меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления**.

3. В открывшемся окне на вкладке **Параметры** снимите флажок **Устанавливать обновления автоматически**.

4. Если вы хотите, чтобы, когда это необходимо, после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.

5. Для сохранения настроек нажмите кнопку **OK**.

Если автоматическая установка обновлений отключена, то после получения обновлений выполните их установку вручную:

1. В области уведомлений щелкните значок **Система обновления ViPNet**.

2. В открывшемся окне проверьте список устанавливаемых обновлений (они отмечены флажком). Если какое-либо обновление устанавливать не нужно, снимите соответствующий флажок.

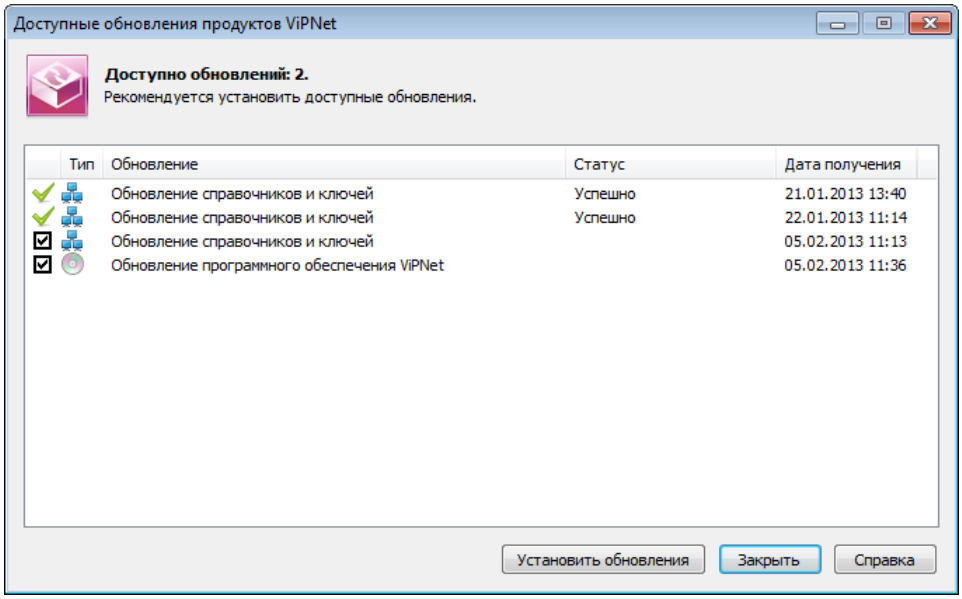


Рисунок 31: Просмотр полученных обновлений

3 Нажмите кнопку **Установить обновления**.

4 Если для продолжения установки обновлений должны быть закрыты какие-либо работающие приложения ViPNet, в окне **Установка обновлений продуктов ViPNet** появится соответствующее сообщение. Нажмите кнопку **Продолжить**. При этом нужные приложения будут автоматически закрыты, и установка обновлений будет продолжена.

После запуска установки ViPNet Монитор выгружается из памяти компьютера, и начинается процесс обновления. При этом в области уведомлений отображается соответствующая информация.

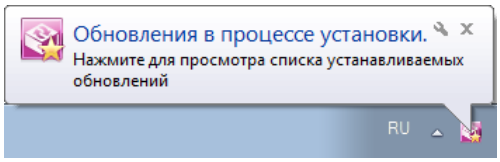


Рисунок 32: Отображение установки обновлений в области уведомлений

Внимание! Обновление ПО может длиться довольно долго. Не прерывайте процесс обновления и не выполняйте перезагрузку компьютера до окончания процесса обновления.

5 Если после завершения обновления необходимо выполнить перезагрузку, соответствующая информация появится в области уведомлений.

Просмотр журнала установленных обновлений

Информация об установленных обновлениях отображается в журнале обновлений. Для просмотра журнала обновлений выполните следующее:

1 В меню **Пуск** выберите **Все программы** > **ViPNet** > **ViPNet Система обновления**.

2 Выберите вкладку **Журнал обновлений**.

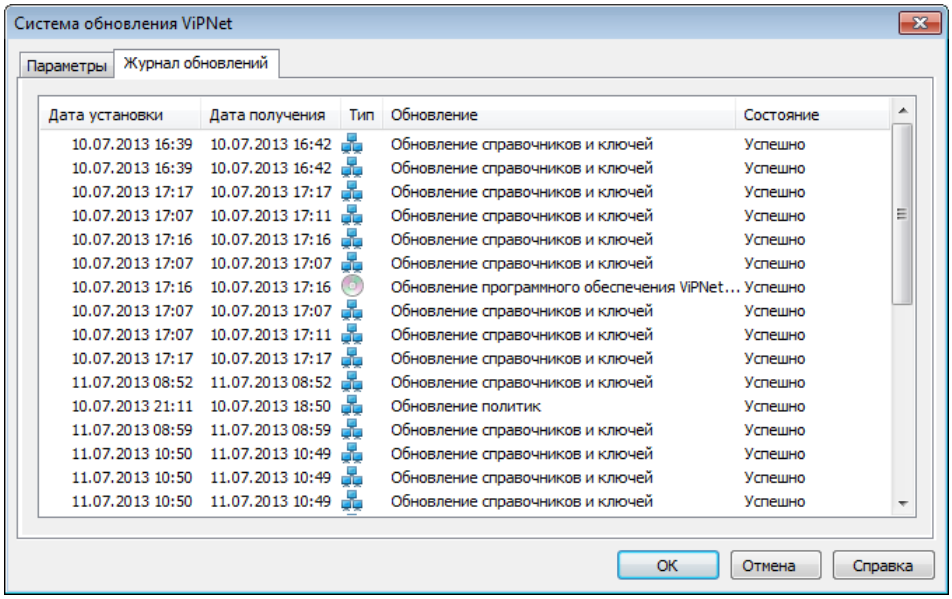


Рисунок 33: Журнал обновлений

6

Подключение к защищенной сети ViPNet

Протоколы соединений в защищенной сети

Сетевые узлы ViPNet могут располагаться в сетях любого типа, поддерживающих IP-протокол. Способ подключения к сети может быть любой: сеть Ethernet, PPPoE через XDSL-подключение, PPP через подключение Dial-up или ISDN, сеть сотовой связи GPRS или UMTS, устройства Wi-Fi, сети MPLS или VLAN. ПО ViPNet поддерживает разнообразные протоколы канального уровня. Для создания защищенных соединений между сетевыми узлами используются IP-протоколы трех типов (IP/241, UDP и TCP), в которые упаковываются пакеты любых других IP-протоколов.

При взаимодействии любых узлов ViPNet между собой, если они расположены в одном сегменте локальной сети и доступны по широковещательным адресам, используется протокол IP/241. Этот протокол более экономичен, так как не имеет UDP-заголовка размером 8 байт. Исходный пакет после шифрования упаковывается в пакет IP-протокола номер 241.

Рисунок 34: Сетевые узлы расположены в одном сегменте локальной сети

Если узлы ViPNet располагаются в разных сегментах сети, то автоматически используется протокол UDP, который позволяет IP-пакетам проходить через межсетевые экраны. Исходный пакет после шифрования упаковывается в UDP-пакет.

Рисунок 35: Сетевые узлы соединяются через межсетевой экран

Если на пути следования IP-пакета расположено устройство NAT, на этом устройстве должны быть настроены динамические или статические правила трансляции адресов, которые разрешают обмен UDP-трафиком с узлами сети ViPNet. При настройке

статических правил должен быть указан порт инкапсуляции UDP-пакетов. По умолчанию используется порт 55777, но при необходимости он может быть изменен на любой другой. Если пакеты проходят напрямую через координатор, то номер порта узлов, расположенных за этим координатором, значения не имеет. После прохождения через координатор пакетам присваиваются IP-адреса соответствующего сетевого интерфейса координатора, то есть осуществляется трансляция адресов.

Бывают случаи, когда взаимодействие защищенных узлов по UDP-протоколу невозможно, передача UDP-пакетов провайдером услуг запрещена. Например, при удаленном подключении к сети ViPNet из гостиниц или других общественных мест. В таком случае весь IP-трафик может передаваться через TCP-туннель, настроенный на координаторе соединений узла, являющегося инициатором соединения (см. «TCP-туннель» на стр. 40). При настройке TCP-туннеля на координаторе соединений может быть указан произвольный порт. По умолчанию используется порт 443.

Рисунок 36: Сетевые узлы соединяются через межсетевой экран

На координаторе полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узел назначения по UDP-протоколу.

Принципы осуществления соединений в защищенной сети

Клиентские узлы в сети ViPNet автоматически выполняют соединения с другими узлами по кратчайшим доступным маршрутам. Для установки соединений они используют координаторы соединений (см. «Координатор соединений» на стр. 485). Информацию о других узлах, параметрах доступа и их активности в данный момент клиенты получают от своего сервера IP-адресов (см. «Сервер IP-адресов» на стр. 490). По умолчанию сервер IP-адресов является координатором соединений для клиента, но при необходимости координатором соединений может быть назначен другой координатор. Параметры подключения к сети определяются клиентами автоматически также с помощью координаторов соединений.

Координаторы информацию о других узлах получают от других координаторов. К внешней сети они могут подключаться одним из следующих способов:

- Непосредственное подключение к внешней сети (см. «Подключение без использования межсетевого экрана» на стр. 109). В этом случае следует отключить использование межсетевого экрана.
- Подключение через другой координатор (см. «О подключении через координатор» на стр. 111).
- Подключение через межсетевой экран с динамической трансляцией адресов (см. «О подключении через межсетевой экран с динамической трансляцией адресов» на стр. 113).
- Подключение через межсетевой экран со статической трансляцией адресов (см. «О подключении через межсетевой экран со статической трансляцией адресов» на стр. 117).

Совет. Настройки параметров подключения координаторов рекомендуется задавать централизованно в программе ViPNet Центр управления сетью или ViPNet Network Manager.

Организация соединений между клиентскими узлами осуществляется следующим образом:

- Перед установкой соединения с другим узлом клиент определяет канал доступа к своему координатору соединений. Если клиент определил, что работает через устройство NAT, то он продолжает поддерживать канал путем периодической отправки на координатор IP-пакетов. Интервал отправки IP-пакетов на координатор соединений по умолчанию равен 25 секундам. Этого, как правило, достаточно для работы через большинство устройств NAT. При необходимости интервал (тайм-аут) может быть изменен.

- После того, как связь между клиентом и его координатором соединений будет установлена, клиент начинает устанавливать соединение с другим узлом. Он начинает передавать IP-пакеты удаленному узлу через свой координатор соединений. Одновременно с этим клиент проверяет возможность передачи IP-пакетов напрямую на удаленный узел или через координатор соединений удаленного узла путем отправки на него и его координатор соединений тестовых IP-пакетов.

- Если тестовые IP-пакеты дошли до удаленного узла, то удаленный узел регистрирует соединение и начинает ответный IP-трафик передавать напрямую. Клиент при получении ответного IP-трафика от удаленного узла свой последующий IP-трафик ему также начинает передавать напрямую.

  Если тестовые IP-пакеты дошли только до координатора соединений удаленного узла, то координатор соединений регистрирует это соединение и отправляет напрямую клиенту ответные IP-пакеты удаленного узла.

  То есть с удаленным узлом устанавливается прямое соединение или соединение через его координатор соединений. Если ответов на тестовые IP-пакеты не было получено, то клиент по-прежнему осуществляет соединение с удаленным узлом через свой координатор соединений.

Рисунок 37: Взаимодействие между сетевыми узлами

Таким образом, если существует возможность, узлы устанавливают взаимодействие друг с другом по кратчайшим маршрутам без участия координаторов, за счет чего повышается скорость обмена шифрованным IP-трафиком и снижается нагрузка на координаторы.

Примечание. Описанный порядок установления соединения применим в полном объеме только в том случае, если на всех узлах используется ПО ViPNet версии не ниже 4.2.x.

Кроме этого, существуют следующие особенности при установлении соединений в сети:

- Если узлы находятся в маршрутизируемой сети, то соединение между клиентами будет производиться в соответствии с заданными маршрутами через шлюзы сети, а не координаторы.
- Если удаленный узел, с которым устанавливается соединение, не расположен за устройством NAT, то информация о возможности прямого доступа к нему запоминается и при следующих соединениях с этим узлом, если не изменилось его местоположение, тестовые IP-пакеты не отправляются, IP-трафик начинает сразу передаваться по прямому маршруту.
- Если клиенты, между которыми устанавливается соединение, расположены за устройствами с динамической трансляцией адресов, то они также в состоянии соединиться друг с другом напрямую. Это происходит за счет того, что координаторы соединений передают клиентам информацию об IP-адресах и портах, по которым они могут получить доступ к другим узлам через устройства NAT.

Данную информацию координаторы определяют по полученным от клиентов IP-пакетам.

Имея эту информацию, клиенты отправляют друг другу тестовые IP-пакеты на зарегистрированные IP-адреса и порты. Если тестовые пакеты будут получены хотя бы одной стороной, весь IP-трафик начинает передаваться между клиентами напрямую. То есть технология установления прямого соединения между клиентами будет применена, если хотя бы одно из устройств NAT при отправке IP-пакетов от узла по разным адресам сохраняет для данного узла выделенный порт.

Прямое соединение между клиентами будет невозможно, если устройства NAT обоих клиентов при отправке IP-пакетов от них по разным адресам каждый раз выделяют случайный порт. Таким образом работает так называемый симметричный NAT. В этом случае соединение между двумя такими клиентами установится через один из координаторов соединений.

- Возможность прямого соединения с удаленным узлом, стоящим за устройством с динамической трансляцией адресов, сохраняется по умолчанию в течение 75 секунд (трех тайм-аутов или интервалов отправки IP-пакетов) с момента окончания предыдущего соединения.

- Если клиент расположен за устройством со статической трансляцией адресов, то в его настройках необходимо зафиксировать нужный порт инкапсуляции UDP-пакетов. В противном случае порт будет изменяться, а вследствии этого соединение клиента с другими узлами будет невозможно.

Подключение без использования межсетевого экрана

О подключении без использования межсетевого экрана

Данный тип подключения следует выбирать на координаторе в том случае, если ни один из его сетевых интерфейсов не стоит за устройством NAT, то есть когда координатор доступен из маршрутизируемой сети. Если координатор должен быть доступен для узлов, находящихся во внешних сетях, то тогда один из его интерфейсов должен иметь публичный IP-адрес.

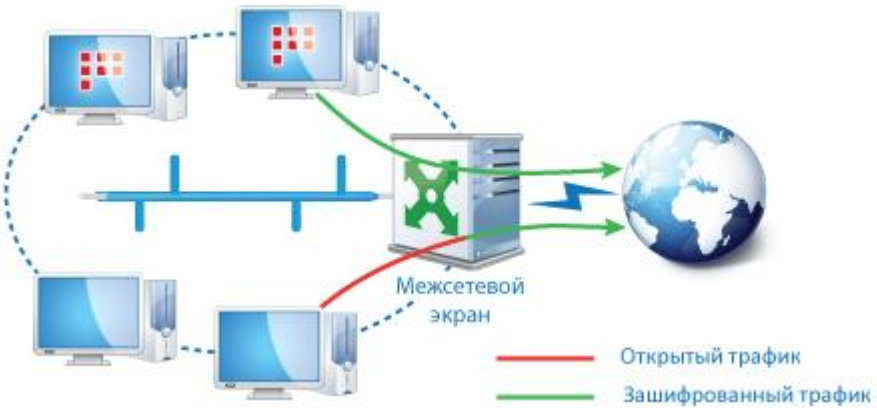


Рисунок 38: Подключение координатора без использования межсетевого экрана

Настройка подключения

Для настройки подключения координатора без использования межсетевого экрана выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. На панели навигации окна **Настройка** выберите раздел **Защищенная сеть**.

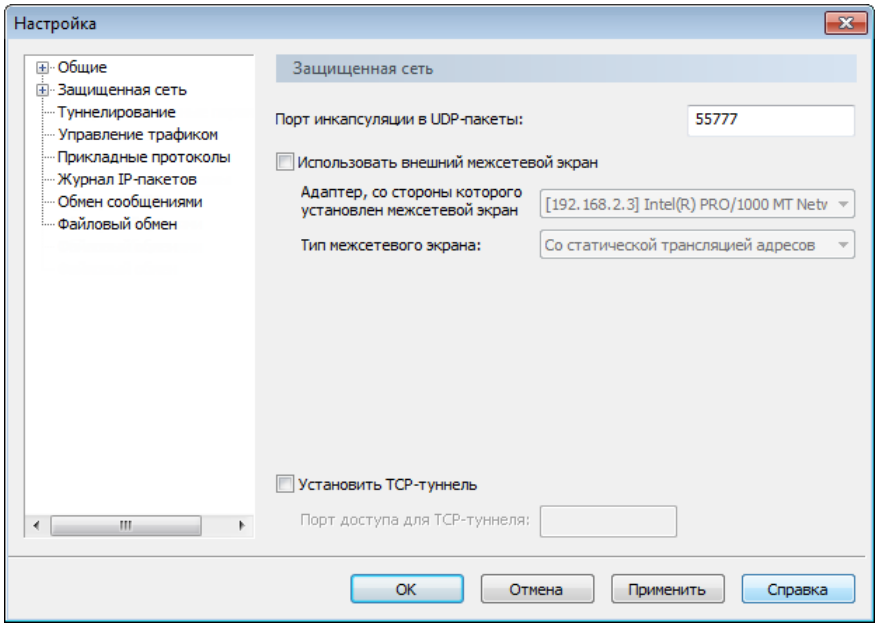


Рисунок 39: Подключение координатора без использования межсетевого экрана

3 Снимите флажок **Использовать внешний межсетевой экран** и нажмите кнопку **OK**.

Подключение через координатор

О подключении через координатор

Если необходимо защитить трафик отдельного сегмента локальной сети, на границе которой уже установлен ViPNet-координатор, выполняющий функции координатора соединений для клиентов этой локальной сети или внешних клиентов, то на границу такого сегмента может быть установлен второй ViPNet-координатор.

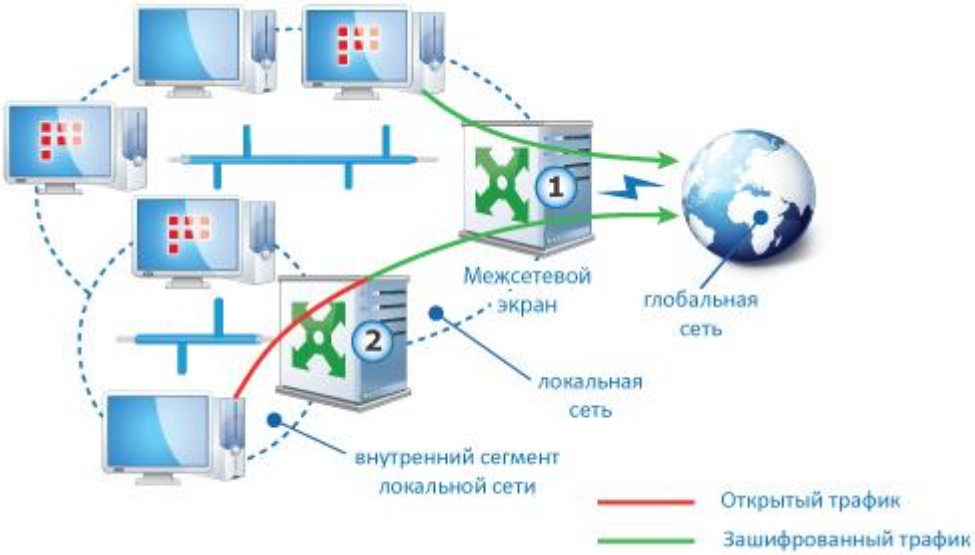


Рисунок 40: Подключение координатора через другой координатор

При этом координатор (1) (см. рисунок выше) должен быть выбран в качестве межсетевого экрана для координатора (2). Между двумя координаторами не должно быть никаких устройств, осуществляющих трансляцию адресов (NAT).

Такое включение координаторов называется каскадным включением. В результате для координаторов будет реализована автоматическая маршрутизация зашифрованного трафика из внутреннего сегмента сети как в локальную, так и в глобальную сеть.

Примечание. Количество координаторов при каскадном включении не ограничено.

Настройка подключения

Чтобы настроить подключение координатора через другой координатор, выполните следующие действия:

1 В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 На панели навигации окна **Настройка** выберите раздел **Защищенная сеть**.

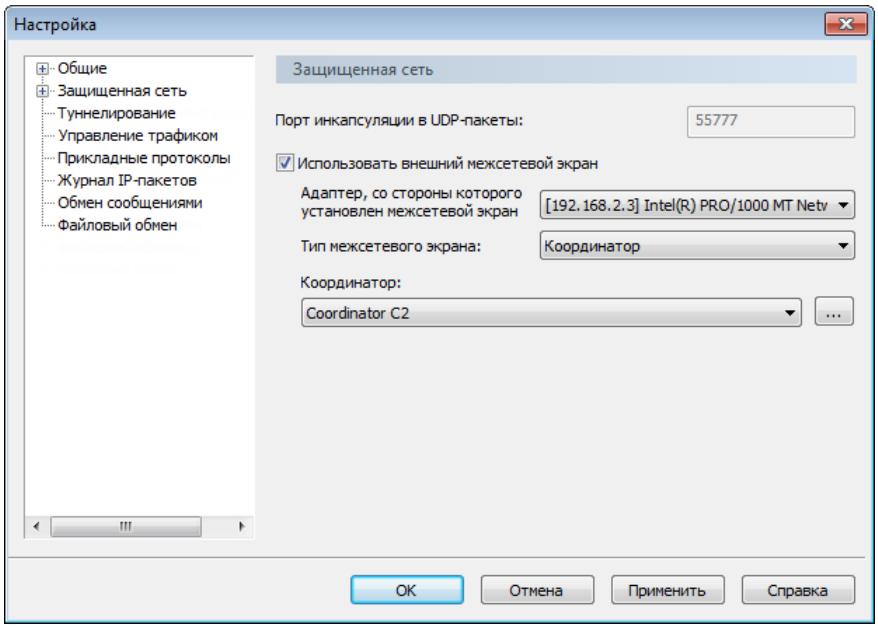


Рисунок 41: Подключение координатора через другой координатор

3 Установите флажок **Использовать внешний межсетевой экран**.

4 В списке **Адаптер, со стороны которого установлен межсетевой экран** выберите сетевой интерфейс, через который будет происходить подключение к другому координатору, выполняющему функции межсетевого экрана.

5 В списке **Тип межсетевого экрана** выберите **Координатор**.

6 В списке **Координатор** выберите координатор, который будет использоваться в качестве межсетевого экрана.

7 Нажмите кнопку **OK**.

Подключение через межсетевой экран с динамической трансляцией адресов

О подключении через межсетевой экран с динамической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT), и на нем затруднительно настроить статические правила трансляции, то для защиты IP-трафика локальной сети, в том числе и при инициативных соединениях снаружи, можно установить координатор с типом межсетевого экрана с динамической трансляцией адресов.

Для координатора с данным типом подключения должен существовать постоянно доступный ViPNet-координатор, расположенный во внешней сети, который будет являться координатором соединений.

Рисунок 42: Подключение через межсетевой экран с динамической трансляцией адресов

Координатор соединений должен быть доступен из внешней сети по публичному IP-адресу или через межсетевой экран со статической трансляцией адресов. Через него

удаленные узлы смогут устанавливать соединения с узлами локальной сети, в том случае если не смогут установить соединение напрямую.

Координатор, использующий подключение через межсетевой экран с динамической трансляцией адресов, взаимодействует с внешними узлами с помощью координатора соединений по тем же правилам, что и клиент. При этом он таким же образом взаимодействует и с клиентами, и с туннелируемыми узлами в своей локальной сети.

Настройка подключения

Чтобы настроить подключение через межсетевой экран с динамической трансляцией адресов:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. На панели навигации окна **Настройка** выберите раздел **Защищенная сеть**.
3. Установите флажок **Использовать внешний межсетевой экран**.
4. В списке **Тип межсетевого экрана** выберите **С динамической трансляцией адресов**.

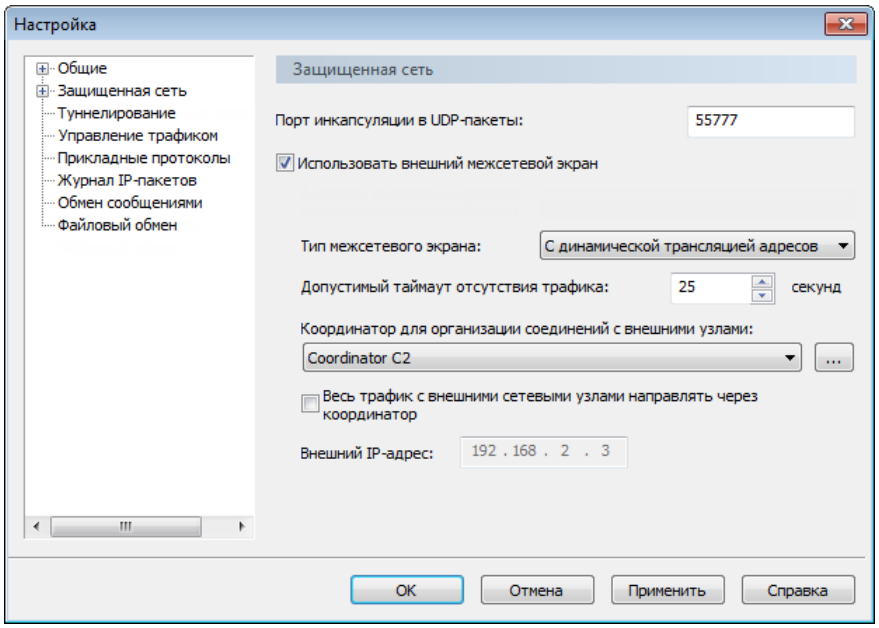


Рисунок 43: Подключение координатора через межсетевой экран с динамической трансляцией адресов

5 Из списка **Координатор для организации соединений с внешними узлами** выберите координатор соединений. Этот координатор должен быть доступен либо напрямую, либо через межсетевой экран со статической трансляцией адресов.

6 Если требуется изменить интервал отправки IP-пакетов координатору соединений, в поле **Допустимый таймаут отсутствия трафика** укажите новое значение. По умолчанию отправка IP-пакетов производится каждые 25 секунд. Как правило, этого интервала достаточно, чтобы поддерживать связь с координатором соединений при работе через большинство устройств NAT.

7 Если требуется направлять весь входящий и исходящий трафик через координатор соединений, установите флажок **Весь трафик с внешними сетевыми узлами направлять через координатор**.

Примечание. Направлять IP-трафик через координатор соединений может потребоваться в том случае, если есть необходимость в контроле всего передаваемого IP-трафика. При этом стоит учитывать, что передача IP-трафика через координатор соединений может привести к существенному снижению скорости обмена данными между узлами.

8 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Если при работе с некоторыми DSL-модемами не проходит передача длинных пакетов, в программе ViPNet Монитор в окне **Настройка** в подразделе **Защищенная сеть** > **Дополнительные параметры** можно уменьшить значение MSS (максимальный размер сегмента).

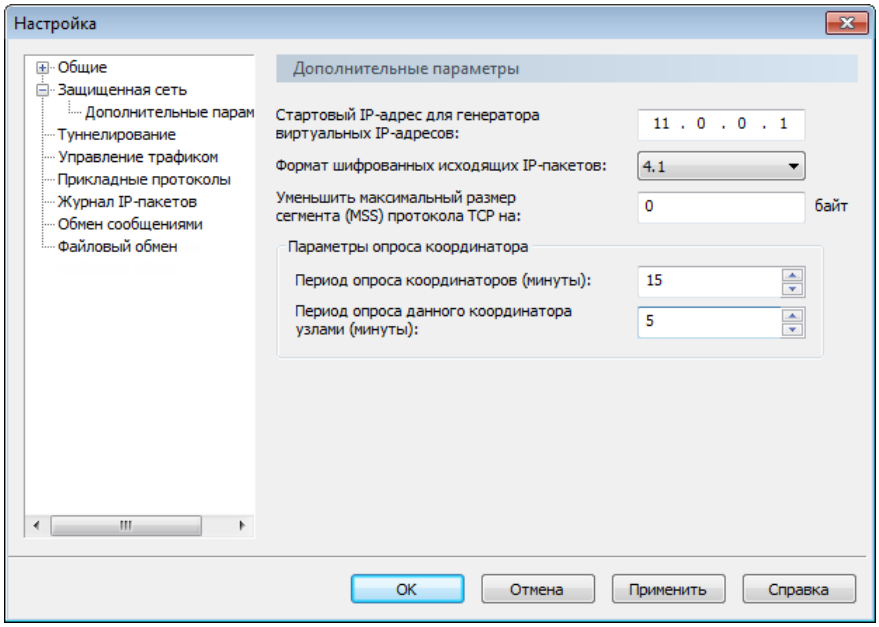


Рисунок 44: Настройка дополнительных параметров

Подключение через межсетевой экран со статической трансляцией адресов

О подключении через межсетевой экран со статической трансляцией адресов

Если на границе локальной сети установлен межсетевой экран, выполняющий трансляцию сетевых адресов (NAT) и позволяющий настроить статические правила трансляции, между этим межсетевым экраном и узлами локальной сети следует установить координатор. На координаторе в этом случае должны быть настроены параметры подключения через межсетевой экран со статической трансляцией адресов. Для клиентов локальной сети данный координатор следует использовать в качестве координатора соединений.

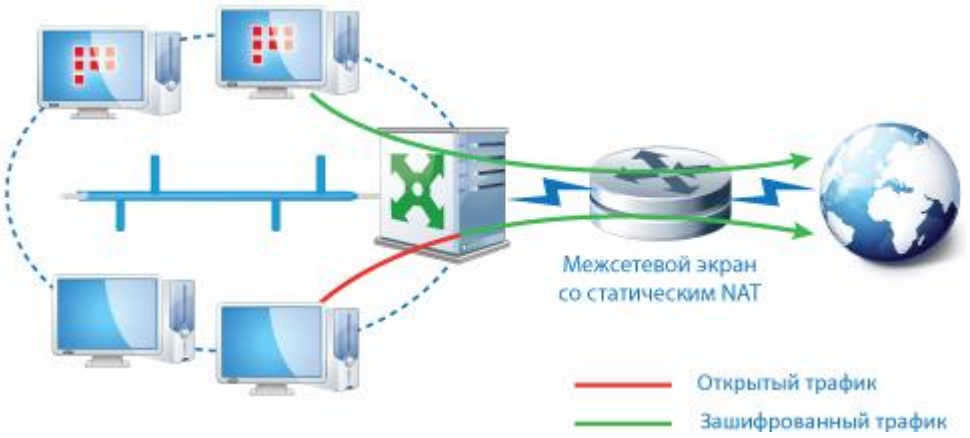


Рисунок 45: Подключение координатора через межсетевой экран со статической трансляцией адресов

Настройка подключения

Для обеспечения работы координатора через межсетевой экран со статической трансляцией адресов должны быть произведены настройки как на межсетевом экране, так и на координаторе.

Для настройки межсетевого экрана укажите следующие статические правила трансляции для каждого координатора, работающего через данный межсетевой экран:

- Пропускать исходящие UDP-пакеты от адреса координатора во внешнюю сеть.
- Пропускать и перенаправлять входящие UDP-пакеты с портом назначения, заданным в настройках вашего координатора.

Чтобы настроить подключение координатора через межсетевой экран со статической трансляцией адресов, выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. На панели навигации окна **Настройка** выберите раздел **Защищенная сеть**.

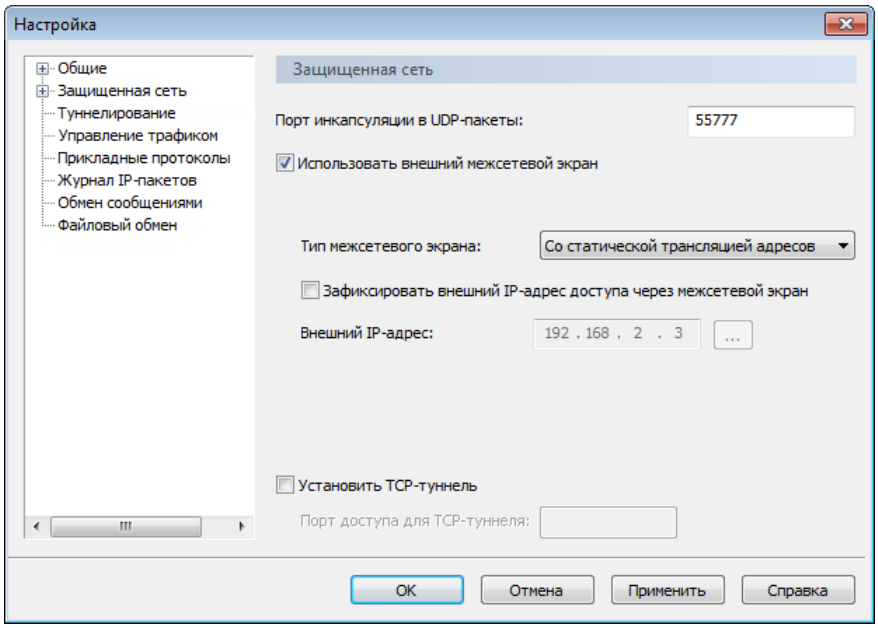


Рисунок 46: Подключение координатора через межсетевой экран со статической трансляцией адресов

3. Установите флажок **Использовать внешний межсетевой экран**.
4. В списке **Тип межсетевого экрана** выберите **Со статической трансляцией адресов**.
5. При необходимости измените значение в поле **Порт инкапсуляции в UDP-пакеты**. По умолчанию задан порт номер 55777. Изменять номер порта нужно в том случае, если несколько координаторов подключены через один межсетевой экран. Каждый из них должен иметь собственный номер порта.

6 Если требуется, чтобы входящие пакеты поступали на определенный адрес межсетевого экрана независимо от того, с какого адреса были отправлены исходящие пакеты (см. «Фиксирование внешнего IP-адреса доступа через межсетевой экран» на стр. 119), установите флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран** и выберите требуемый IP-адрес из списка **Внешний IP-адрес**. Кроме этого, в списке **Адаптер, со стороны которого установлен межсетевой экран** также укажите сетевой интерфейс координатора, со стороны которого находится межсетевой экран.

   Рекомендуется использовать эту настройку, только если межсетевой экран имеет несколько внешних адресов.

7 Чтобы сохранить настройки, нажмите кнопку **Применить.**

Фиксирование внешнего IP-адреса доступа через межсетевой экран

Если внешний IP-адрес доступа не зафиксирован, он определяется по внешним параметрам IP-пакета. Это значит, что внешние узлы будут отправлять ответные IP-пакеты на тот IP-адрес, с которого был принят исходный пакет. Если установлен флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран**, внешние узлы будут отправлять ответные пакеты для рассматриваемого сетевого узла на указанный IP-адрес независимо от внешних параметров пакета. IP-адрес отправителя пакета не учитывается и заменяется фиксированным IP-адресом доступа. При этом на межсетевом экране должны быть настроены правила трансляции адресов, обеспечивающие доставку ответных пакетов получателю.

Внимание! Рекомендуется фиксировать внешний IP-адрес доступа только в том случае, если межсетевой экран имеет несколько внешних IP-адресов и по какой-либо причине необходимо направлять все входящие пакеты через определенный адрес межсетевого экрана.

Рассмотрим следующий пример. IP-пакет имеет параметры:

IP-адрес отправителя: 192.168.2.1

IP-адрес получателя: 79.15.89.11

При прохождении пакета через межсетевой экран IP-адрес отправителя будет заменен на публичный адрес межсетевого экрана, например 68.89.90.110.

Если флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран** снят, ответный IP-пакет будет иметь следующие параметры:

IP-адрес отправителя: 79.15.89.11

IP-адрес получателя: 68.89.90.110

Когда ответный пакет будет принят на межсетевом экране, адрес получателя будет заменен на 192.168.2.1.

Если флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран** установлен и в поле **Внешний IP-адрес** указан адрес 78.56.89.43, то ответный пакет будет иметь следующие параметры:

IP-адрес отправителя: 79.15.89.11

IP-адрес получателя: 78.56.89.43

На межсетевом экране следует настроить правила трансляции адресов, направляющие такие ответные пакеты на локальный адрес получателя (192.168.2.1).

Настройка доступа к узлам сети ViPNet

Виртуальные IP-адреса

Использование виртуальных IP-адресов

В различных локальных сетях и сетях интернет-провайдеров довольно часто возникает проблема с пересечением IP-адресов. Технология виртуальных адресов позволяет эффективно решить эту проблему при организации защищенных соединений.

Виртуальные адреса также можно использовать, чтобы установить правила доступа к ресурсу на основе виртуальных адресов. Для чего это нужно? Известно, что если IP-адрес используется для идентификации пользователя, то одной из сетевых угроз является подделка IP-адреса. Однако в сети ViPNet подделка адреса невозможна. В момент приема пакета из сети ViPNet-драйвер подставляет вместо реального адреса отправителя соответствующий виртуальный адрес, затем пакет передается приложению. Это происходит только в случае успешной расшифровки пакета на ключах отправителя, то есть после идентификации отправителя пакета. Это обеспечивает защиту от подмены адреса отправителя и надежное разграничение доступа к ресурсам на основе виртуальных адресов.

Каждый сетевой узел ViPNet автоматически формирует один или несколько виртуальных IP-адресов для каждого сетевого узла ViPNet и туннелируемого узла, с которым он связан. Каждому реальному адресу узла ставится в соответствие виртуальный IP-адрес. То есть число формируемых виртуальных адресов зависит от числа реальных адресов узла и числа туннелируемых этим узлом адресов.

У каждого сетевого узла собственный список виртуальных адресов для других узлов. Все приложения при работе в сети могут использовать эти виртуальные адреса для соединения с соответствующими узлами. ViPNet-драйвер подменяет адреса в момент отправки и получения IP-пакетов (включая пакеты служб DNS, WINS, NetBIOS, SCCP, SIP и другие).

По умолчанию сетевой узел автоматически использует виртуальные адреса для соединения с другими сетевыми узлами, если эти узлы недоступны по широковещательным IP-адресам. Для туннелируемых узлов по умолчанию используются реальные IP-адреса. При необходимости можно принудительно установить для любых узлов реальную или виртуальную видимость.

Общие принципы назначения виртуальных адресов

По умолчанию начальный адрес для генератора виртуальных адресов — 11.0.0.1 (маска подсети: 255.0.0.0). Начальный адрес можно изменить в окне **Настройка**, в разделе **Защищенная сеть > Дополнительные параметры**. Автоматическое формирование виртуальных IP-адресов для сетевых узлов ViPNet и одиночных туннелируемых адресов начинается с этого адреса.

Для диапазонов туннелируемых адресов начальным виртуальным адресом по умолчанию является 12.0.0.1 либо адрес, в котором значение первого октета на 1 больше, чем значение первого октета начального адреса для генератора виртуальных адресов.

Примечание. Одиночный туннелируемый адрес — это адрес, который явно (а не в составе диапазона адресов) указан в настройках туннелируемых адресов узла.

Следует учитывать, что по умолчанию для виртуальных адресов используется один из интернет-диапазонов. Поэтому при взаимодействии узла с открытыми ресурсами Интернета может возникнуть конфликт, если у некоторого открытого ресурса IP-адрес совпадет с используемым виртуальным адресом. Соединение с таким открытым ресурсом будет невозможно. Если доступ к открытому ресурсу все же необходим, следует либо сменить диапазон назначаемых виртуальных адресов или работать с этим ресурсом через прокси-сервер.

Виртуальные адреса сетевых узлов отображаются на вкладке **IP-адреса** в окне **Свойства узла** для каждого сетевого узла. Виртуальные адреса туннелируемых узлов отображаются на вкладке **Туннель** в окне **Свойства узла** для координатора, осуществляющего туннелирование.

Виртуальные адреса для сетевых узлов закрепляются не за конкретными реальными адресами, а за уникальными идентификаторами сетевых узлов, присвоенными в ViPNet Центр управления сетью или ViPNet Network Manager. Виртуальные адреса для одиночных туннелируемых узлов закрепляются за каждым реальным туннелируемым IP-адресом. Виртуальные адреса закрепляются за сетевыми узлами и одиночными туннелируемыми адресами до тех пор, пока сетевые узлы или туннелируемые адреса не будут удалены.

Внимание! Чтобы избежать ошибок при назначении начальных адресов для генератора виртуальных адресов, следует иметь в виду следующее:

- Значение первого (младшего) октета должно быть в диапазоне 1–254.
- Значение четвертого октета должно быть в диапазоне 1–239.
- Значение второго и третьего октетов должно быть в диапазоне 0–255.

Вновь добавленным сетевым узлам, реальным IP-адресам узлов и одиночным туннелируемым адресам ставятся в соответствие новые свободные виртуальные адреса. 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.

Настройка доступа к защищенным узлам

Для установления соединения между двумя координаторами нужно на каждом из координаторов указать IP-адрес или DNS-имя того координатора, с которым устанавливается связь.

Если IP-адреса и параметры подключения координаторов были заданы в программе ViPNet Administrator или ViPNet Network Manager, то в программе ViPNet Монитор на сетевом узле никаких дополнительных настроек выполнять не требуется. Если предварительных настроек не было сделано, то на сетевом узле настройте параметры доступа к нужному координатору вручную. Для этого выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** дважды щелкните нужный сетевой узел.
3. В окне **Свойства узла** на вкладке **IP-адреса** добавьте в список реальный IP-адрес сетевого узла. Автоматически новому адресу будет сопоставлен виртуальный IP-адрес (см. «Виртуальные IP-адреса» на стр. 122).

   Если вам не известен IP-адрес узла, то вы можете определить его по имени компьютера. Для этого нажмите кнопку  и в появившемся окне выполните поиск IP-адреса по указанному имени.

   При добавлении IP-адреса будет автоматически выполнена его проверка на наличие конфликта с IP-адресами, уже заданными в списке, и IP-адресами других сетевых узлов (в том числе, туннелируемых), если для узлов не установлена виртуальная видимость. Данная проверка позволит избежать задания одинаковых IP-адресов. Если в ходе проверки будет обнаружен конфликт IP-адресов, появится соответствующее сообщение. Устраните конфликт IP-адресов (см. «Обнаружен конфликт IP-адресов» на стр. 375).

   Вы также можете выполнить проверку на конфликт IP-адресов вручную. Для этого нажмите кнопку  .

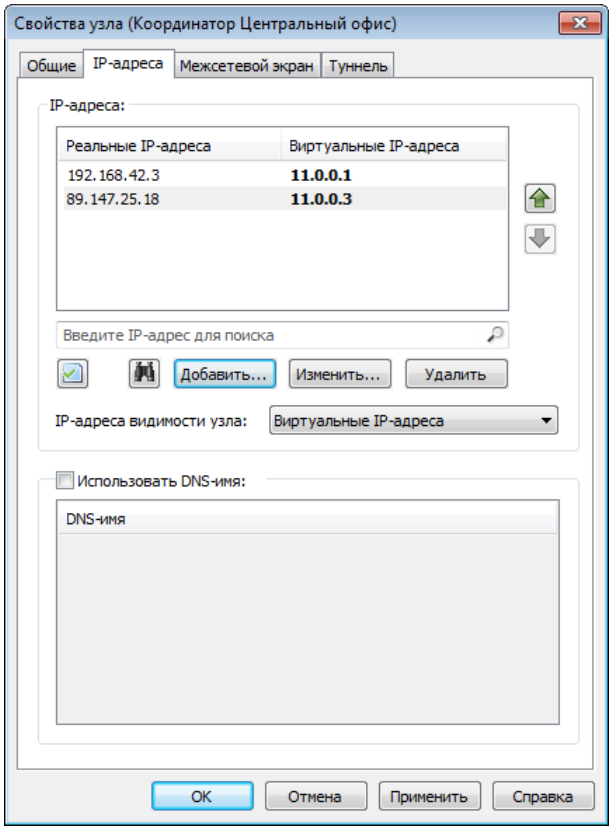


Рисунок 47: Задание IP-адреса сетевого узла

4 В списке **IP-адреса видимости узла** укажите, по каким адресам должен быть доступен сетевой узел. По умолчанию IP-адреса видимости выбираются автоматически. Если возможен конфликт реальных IP-адресов с адресами других узлов в сети, в списке выберите **Виртуальные IP-адреса**.

При изменении IP-адресов видимости в свойствах координатора вам будет предложено установить аналогичные IP-адреса видимости на всех узлах, использующих данный координатор в качестве координатора соединений.

5 Если для доступа к сетевому узлу необходимо использовать DNS-имя, установите флажок **Использовать DNS-имя** и добавьте в список DNS-имя сетевого узла.

Для любого сетевого узла можно задать несколько DNS-имен. При настройке параметров доступа к координатору DNS-имена узлов, туннелируемых этим координатором, также следует добавить в список на вкладке **IP-адреса** (см. «Настройка доступа к узлам, туннелируемым другим координатором» на стр. 129).

Для клиента порядок DNS-имен в списке не имеет значения. Для координатора в первой строке списка нужно указать DNS-имя, соответствующее IP-адресу координатора. Подробная информация об использовании службы DNS в сети ViPNet

см. в разделе Настройка и использование служб имен DNS и WINS в сети ViPNet (на стр. 139).

6 При настройке параметров доступа к координатору на вкладке **Межсетевой экран** добавьте IP-адрес межсетевого экрана, если он используется. При необходимости укажите дополнительные IP-адреса. Если будет указано несколько IP-адресов доступа через межсетевой экран, то вы можете указать приоритет этих адресов с помощью метрик (см. «Настройка приоритета IP-адресов доступа к координатору» на стр. 132).

В поле **Порт UDP** укажите порт доступа через межсетевой экран.

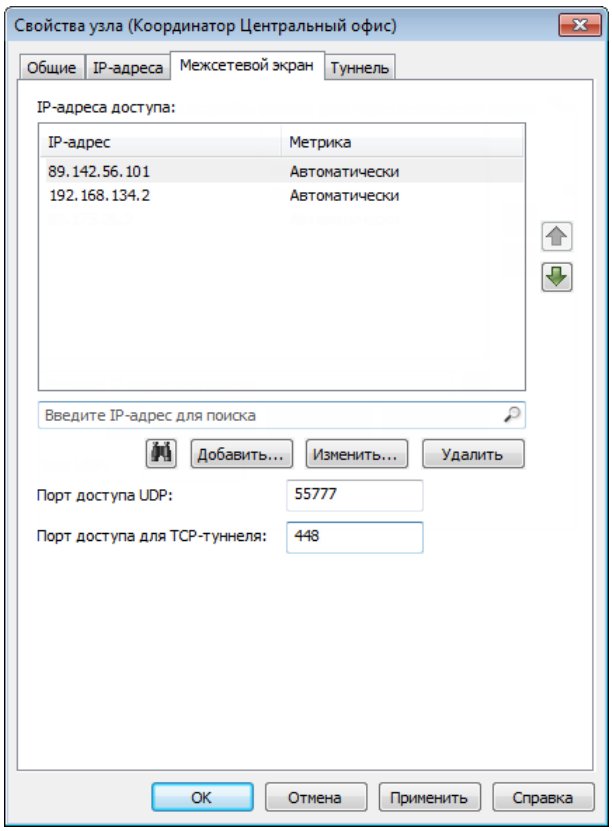


Рисунок 48: Настройка доступа к координатору через межсетевой экран

7 При настройке параметров доступа к координатору на вкладке **Межсетевой экран** в поле **Порт доступа для TCP-туннеля** вы можете указать порт, по которому ваш узел сможет соединяться с координатором по TCP-протоколу (через TCP-туннель). Порт рекомендуется задавать в том случае, если в свойствах координатора он не задан, но при этом известно, что на данном координаторе развернут TCP-туннель для соединений по TCP-протоколу.

Как правило, информация о номере порта доступа по TCP-протоколу поступает на сетевой узел автоматически сразу после развертывания на координаторе TCP-

туннеля. Поэтому если в свойствах координатора порт доступа по TCP-протоколу указан, изменять его не следует.

8 Чтобы сохранить указанные настройки, нажмите кнопку **Применить**.

Настройка доступа к узлам, туннелируемым другим координатором

Для возможности соединения с узлами, которые уже туннелируются другим координатором, в программе ViPNet Монитор на вашем узле должны быть настроены параметры доступа к ним. Если в программе ViPNet Administrator или ViPNet Network Manager были сделаны настройки параметров туннелирования для всех координаторов, то в данном случае ничего дополнительно настраивать не требуется. Доступ вашего узла к туннелируемым узлам других координаторов будет организован автоматически.

Чтобы настроить соединение вашего узла с туннелируемыми узлами другого координатора вручную, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** дважды щелкните координатор, который осуществляет туннелирование требуемых открытых узлов.
3. В окне **Свойства узла** на вкладке **Туннель** установите флажок **Использовать IP-адреса для туннелирования** и с помощью соответствующих кнопок сформируйте список IP-адресов туннелируемых узлов. Заданным адресам автоматически будут сопоставлены виртуальные IP-адреса (на стр. 122).

   Если вам не известен IP-адрес туннелируемого узла, то вы можете определить его по имени компьютера. Для этого нажмите кнопку  и в появившемся окне выполните поиск IP-адреса по указанному имени.

Примечание. Если необходимо указать DNS-имена туннелируемых узлов, эти имена следует добавить в список DNS-имен туннелирующего координатора (см. «Настройка доступа к защищенным узлам» на стр. 125). Следует иметь в виду, что на первом месте в этом списке должно стоять зарегистрированное на DNS-сервере имя координатора.

При добавлении IP-адреса будет автоматически выполнена его проверка на пересечение с IP-адресами, уже заданными в списке, и IP-адресами других сетевых

узлов (в том числе, туннелированных). Данная проверка позволит исключить возможность задания одинаковых IP-адресов. Если в ходе проверки будет обнаружено пересечение IP-адресов, появится соответствующее сообщение. Устраните пересечение IP-адресов (см. «Обнаружен конфликт IP-адресов» на стр. 375).

Вы также можете выполнить проверку на пересечение IP-адресов вручную. Для этого нажмите кнопку  .

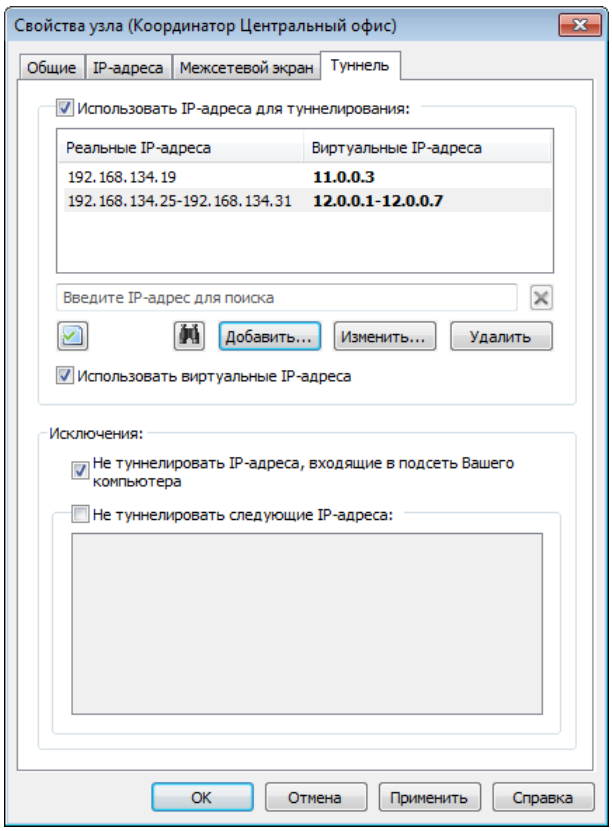


Рисунок 49: Задание адресов туннелируемых узлов

4 Если возможен конфликт IP-адресов в подсетях, установите флажок **Использовать виртуальные IP-адреса**.

5 Если туннелируемый узел находится в одной подсети с вашим узлом и на нем не настроена специальная маршрутизация, убедитесь, что установлен флажок **Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера**. Иначе соединение с туннелируемым узлом будет невозможно.

6 Если при соединении с какими-либо туннелированными узлами шифрование данных не требуется, рекомендуется установить флажок **Не туннелировать следующие IP-адреса** и добавить в список ниже IP-адреса этих узлов.

7 Выполнив необходимые настройки, нажмите кнопку **Применить**.

Настройки, описанные в данном разделе, должны быть выполнены на сетевом узле для всех координаторов, с туннелируемыми узлами которых требуется устанавливать соединения.

Настройка приоритета IP-адресов доступа к координатору

Если координатор имеет несколько адресов доступа (например, по разным каналам связи), то можно настроить приоритет каналов для установления соединения с координатором. Если самый приоритетный канал по каким-то причинам недоступен, то канал связи будет выбран в соответствии с приоритетами оставшихся каналов. Когда самый приоритетный канал станет доступен, соединение с координатором вновь будет установлено через него.

Примечание. Следует учитывать, что эффективной данная настройка может быть только в случае, если узел связывается с координатором по нескольким разным каналам, например, через Интернет и выделенную сеть (то есть при маршрутизации через разные шлюзы).

Приоритет каналов задается с помощью метрики для каждого адреса доступа координатора. По умолчанию метрика назначается автоматически. При назначении метрик нужно придерживаться следующих принципов:

- Метрика определяет задержку (в миллисекундах) отправки тестовых IP-пакетов при выполнении опроса для определения доступности адреса. Соединение устанавливается по тому адресу, доступность которого быстрее определяется в результате опроса.
- Опросы осуществляются в следующих случаях:
  - При запуске программы ViPNet Монитор.
  - При проверке соединения с узлом вручную.
  - Периодически. Период опросов задается на координаторе в окне **Настройка** в разделе **Защищенная сеть > Дополнительные параметры**. По умолчанию период опроса координаторами других координаторов равен 15 минутам, период опроса своего координатора клиентами равен 5 минутам.
- Адрес с наименьшей метрикой считается самым приоритетным. Соединение с координатором устанавливается по адресу с наименьшей метрикой всегда, когда этот адрес доступен.

- Если для всех адресов доступа узла метрика назначена автоматически, то значение метрики равно 0. Если для части адресов метрика назначена вручную, а для остальных — автоматически, то значение автоматически назначенной метрики всегда на 100 миллисекунд больше максимального значения метрики, присвоенной вручную.

- Чем больше разница между наименьшей метрикой и остальными метриками, тем меньше вероятность того, что в случае кратковременного сбоя самого приоритетного канала будет выбран менее приоритетный канал. При использовании менее приоритетного канала сетевой узел быстрее сможет вернуться к работе через самый приоритетный канал, когда он станет доступен.

- Если все метрики равны, то для работы будет выбран тот канал, через который соединение с координатором будет установлено быстрее. После того как канал выбран, определение доступности других каналов связи выполняется только при потере соединения по текущему каналу. Этот же механизм действует в случае, если выбран канал связи с наименьшей метрикой.

- Если хотя бы для одного адреса доступа значение метрики задано вручную и выбран не самый приоритетный канал, то определение доступности других каналов связи с целью возвращения к каналу с наименьшей метрикой начнется одновременно с периодическим опросом по выбранному каналу.

- После определения канала доступа текущий адрес доступа отобразится в окне свойств координатора в первой строке списка IP-адресов на вкладке **Межсетевой экран**.

Чтобы назначить метрики для адресов доступа к координатору, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.

2. В разделе **Защищенная сеть** дважды щелкните координатор, для которого требуется задать приоритет IP-адресов доступа.

3. В окне **Свойства узла** откройте вкладку **Межсетевой экран**.

4. В случае необходимости настройте параметры доступа к координатору через межсетевой экран (см. «Настройка доступа к защищенным узлам» на стр. 125).

5. Чтобы назначить IP-адресу доступа метрику, выберите в списке адрес и нажмите кнопку **Изменить**.

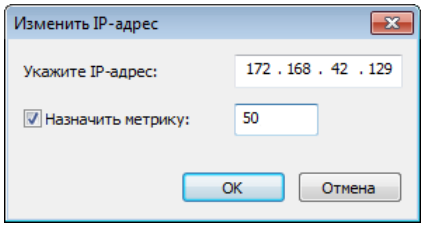


Рисунок 50: Назначение метрики

6 В появившемся окне установите флажок **Назначить метрику** и в поле рядом введите значение метрики в миллисекундах (допустимые значения от 1 до 9999), после чего нажмите кнопку **OK.**

Рассмотрим пример использования метрики. Предположим, координатор имеет четыре адреса доступа по каналам связи A, B, C и D. Требуется задать метрики для этих каналов.

Пусть каналы имеют следующий приоритет:

1 A — самый быстрый и безопасный канал. Используется в первую очередь.

2 C и D — безопасные, но менее быстрые каналы. Используются, если канал A недоступен.

3 B — менее безопасный канал. Используется в последнюю очередь.

Чтобы канал A стал самым приоритетным, зададим для него самую маленькую метрику, например 1. Для канала B зададим максимальную метрику 9999, так как работа через этот канал нежелательна. Для каналов C и D зададим одинаковую метрику, причем такую, чтобы разница с метрикой для канала A была небольшой, например 500.

При указанных значениях метрик канал A будет использоваться всегда, когда доступен. Если в момент проверки он недоступен или его качество ухудшилось (он стал медленнее), то соединение с координатором будет установлено по каналу C или D. И только в крайнем случае, если в момент проверки каналы A, C или D недоступны или их качество значительно ухудшилось, для работы может быть выбран канал B.

Если для соединения с координатором используются каналы B, C или D, то по истечении периода опроса, при перезапуске программы ViPNet Монитор или при проверке соединения с координатором сетевой узел будет пытаться установить соединение с координатором по каналу A. Чем меньше период опроса, тем быстрее происходит переход на другой канал в случае сбоев и возвращение на более приоритетный канал.

Настройка TCP-туннеля

При удаленном подключении клиентов к сетям ViPNet может возникать проблема с передачей IP-пакетов по протоколу UDP из-за того, что данный протокол блокируется некоторыми провайдерами услуг. Для решения подобной проблемы можно организовать взаимодействие клиентов через TCP-туннель по протоколу TCP. Для этого на координаторе соединений этих клиентов требуется настроить TCP-туннель (см. «TCP-туннель» на стр. 40).

Примечание. TCP-туннель можно настроить только на координаторе, который не установлен за межсетевой экран или установлен за межсетевой экран со статической трансляцией адресов (см. «Подключение к защищенной сети ViPNet» на стр. 102).

Чтобы настроить TCP-туннель на координаторе, выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. На панели навигации окна **Настройка** выберите раздел **Защищенная сеть**.

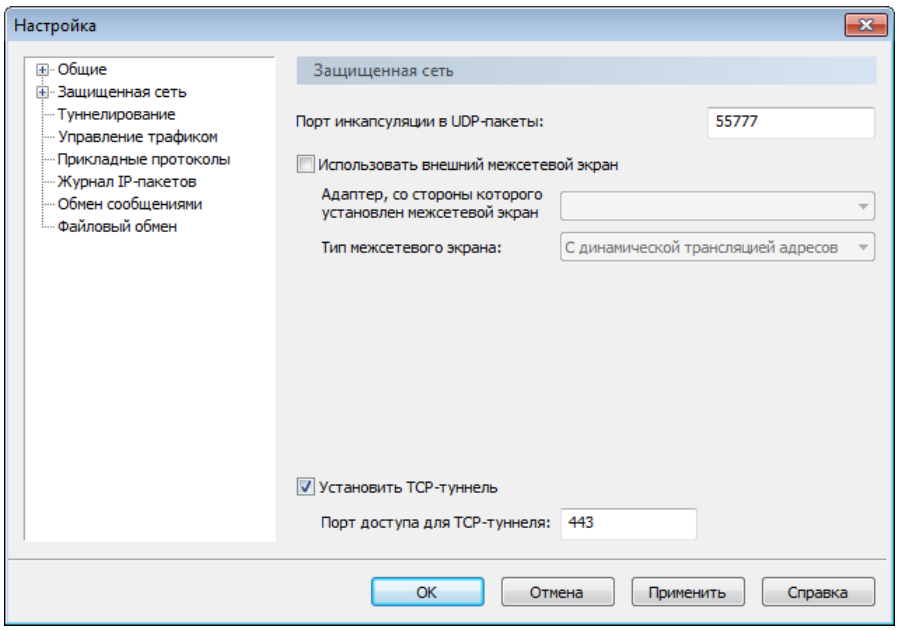


Рисунок 51: Настройка TCP-туннеля

3 Установите флажок **Установить TCP-туннель**.

4 В поле **Порт доступа для** укажите номер порта, на который будут поступать TCP-пакеты от защищенных узлов.

5 Чтобы сохранить настройки, нажмите кнопку **Применить**.

В результате на координаторе будет настроен TCP-туннель. Информация о том, что был настроен TCP-туннель, с номером порта для передачи TCP-пакетов будет отправлена на все сетевые узлы, для которых данный координатор является координатором соединений.

В дальнейшем, если удаленный клиент не сможет связаться с другими узлами сети ViPNet по протоколу UDP, он автоматически начнет устанавливать с ними соединение через TCP-туннель, настроенный на своем координаторе соединений. На координаторе полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узлы назначения по UDP-протоколу.

Использование псевдонимов для защищенных узлов

Чтобы улучшить восприятие в разделе **Защищенная сеть** для любого сетевого узла можно задать произвольный псевдоним. Этот псевдоним будет отображаться вместо имени сетевого узла в разделе **Защищенная сеть**. Чтобы найти сетевой узел в списке, в строку поиска можно ввести как псевдоним, так и имя сетевого узла.

Чтобы задать псевдоним для сетевого узла:

1. В программе ViPNet Монитор выберите раздел **Защищенная сеть** и дважды щелкните узел, для которого требуется задать псевдоним.
2. В окне **Свойства узла** на вкладке **Общие** в поле **Псевдоним** введите имя, которое нужно присвоить данному сетевому узлу.
3. Нажмите кнопку **OK**.
4. При необходимости добавьте псевдонимы для других защищенных сетевых узлов.

Примечание. Если после добавления псевдонима в списке по-прежнему указано имя сетевого узла, включите функцию отображения псевдонимов. Для этого:

- В программе ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
- В окне **Настройка** в разделе **Общие** установите флажок **Отображать псевдонимы ViPNet-пользователей**.

Просмотр информации о сетевом узле

При организации доступа к узлу или при возникновении проблем с доступом, администратор сети ViPNet или служба технической поддержки может запросить информацию об этом сетевом узле, а также о вашем сетевом узле.

Чтобы просмотреть информацию о чужом сетевом узле ViPNet, выполните следующие действия:

1. В окне программы ViPNet Монитор в разделе **Защищенная сеть** дважды щелкните нужный сетевой узел.
2. В окне **Свойства узла** перейдите на вкладку **Общие**.
3. Если необходимо, скопируйте нужный текст, чтобы передать его администратору или службе технической поддержки.

Для просмотра информации о своем сетевом узле в главном окне программы в меню **Файл** выберите пункт **Свойства моего узла.**

8

Настройка и использование служб имен DNS и WINS в сети ViPNet

Службы DNS и WINS

К компьютерам удобнее обращаться не по цифровым адресам, а по каким-либо осмысленным именам, которые соответствуют функциям и местоположению компьютеров. Людям проще запомнить буквенное имя, чем последовательность цифр. Локальные сети и Интернет объединяют огромное количество компьютеров, поэтому необходимы специализированные службы имен, обеспечивающие сопоставление имен компьютеров с их IP-адресами. В настоящее время в сетях используются две службы имен — DNS и WINS.

DNS

В сетях TCP/IP используется система доменных имен (Domain Name System, DNS), которая служит для преобразования IP-адреса в доменное имя и наоборот: например, 79.11.15.23 — в `www.company.ru`.

Следующий рисунок иллюстрирует использование DNS, то есть обнаружение IP-адреса компьютера по его имени.

Рисунок 52: Общий принцип работы службы DNS

Компьютер-клиент запрашивает у DNS-сервера IP-адрес компьютера с доменным именем `www.company.ru`. Поскольку DNS-сервер может ответить на запрос с помощью своей локальной базы данных, он возвращает ответ, содержащий запрашиваемую информацию, то есть запись об узле, в которой содержится IP-адрес, соответствующий имени `www.company.ru`.

Этот пример демонстрирует простой запрос DNS от клиента к DNS-серверу. На практике запросы DNS могут потребовать привлечения других серверов и выполнения дополнительных шагов, не показанных в этом примере.

Система именования, используемая DNS, носит иерархический характер. Доменное имя складывается из нескольких частей, расположенных справа налево. Первая часть (домен верхнего уровня) является фиксированной и назначается централизованно Сетевым Информационным Центром (Network Information Center, NIC). Домены остальных уровней присваиваются на серверах доменных имен произвольно.

WINS

Аналогично DNS работает служба WINS (Windows Internet Name Service, служба имен сети Интернет для Windows), которая преобразует IP-адрес в NetBIOS-имя и наоборот: например, 192.168.1.20 — в HOST-A. Служба WINS является наиболее удобным средством разрешения имен NetBIOS в маршрутизируемых сетях, использующих NetBIOS через стек TCP/IP.

Примечание. NetBIOS (Network Basic Input Output System, сетевая базовая система ввода-вывода) — протокол сеансового уровня для работы в локальных сетях, обеспечивающий доступ компьютера как к собственным локальным ресурсам, так и к ресурсам удаленных компьютеров. Поскольку NetBIOS применяет рассылку широковещательных сообщений, он не поддерживает передачу информации через маршрутизаторы. Но с другой стороны, усовершенствования, внесенные в NetBIOS, позволяют этой системе работать поверх протоколов маршрутизации, таких как IP и IPX.

Служба WINS упрощает управление пространством имен NetBIOS в сетях на основе стека протоколов TCP/IP. Следующий рисунок иллюстрирует типичную последовательность событий, связанных с клиентами и серверами WINS.

Рисунок 53: Общий принцип работы службы WINS

Этот пример демонстрирует следующие события:

- (1) WINS-клиент HOST-A регистрирует любое из своих локальных имен NetBIOS на своем WINS-сервере WINS-A.

  В случае, если компьютер HOST-A не имеет в своем распоряжении IP-адреса WINS-сервера, он передает в широковещательной рассылке свое имя NetBIOS, объявляя тем самым о своем присутствии в сети. Когда происходит подобное событие, локальный WINS-сервер принимает такое широковещательное сообщение и вводит содержащееся в нем имя и соответствующий IP-адрес в свою базу данных.

- (2) Другой WINS-клиент HOST-B запрашивает сервер WINS-A найти IP-адрес компьютера HOST-A в сети.

- (3) Сервер WINS-A возвращает 192.168.1.20 — IP-адрес компьютера HOST-A.

Службы WINS и DNS могут бесконфликтно работать в пределах одной сети. Пространства имен той и другой службы не совпадают. DNS использует иерархическую структуру именования, в то время как WINS — одноранговую. Служба WINS особенно актуальна для сетей, на узлах которых установлены ОС Windows XP или Windows Server 2003. В сетях, в которых применяются и доменные имена, и имена NetBIOS, рекомендуется использовать обе службы.

Службы DNS и WINS в сети ViPNet

В сетях ViPNet приложения могут использовать виртуальные IP-адреса (на стр. 122), реально не существующие в сети и уникальные на каждом сетевом узле, что позволяет избежать конфликтов при наличии пересекающихся адресов в разных сетях.

Для обеспечения работы служб DNS и WINS в сети ViPNet с виртуальными адресами программное обеспечение ViPNet автоматически выполняет специальную обработку IP-пакетов этих служб. Такая обработка требуется для того, чтобы на защищенных узлах приложения, которые обращаются к службам DNS и WINS, использовали для доступа к другим защищенным и туннелируемым узлам правильные IP-адреса (реальные или виртуальные).

Если на DNS (WINS) сервере, к которому обращаются приложения, установлено ПО ViPNet или этот сервер туннелируется координатором, поддержка DNS (NetBIOS) имен для виртуальных адресов обеспечивается без дополнительных настроек ПО ViPNet при соблюдении определенных правил (см. «DNS (WINS) сервер на защищенном или туннелируемом узле» на стр. 144).

DNS-имена для защищенных узлов можно задать вручную в программе ViPNet Монитор на сетевом узле либо в программе ViPNet Центр управления сетью или ViPNet Network Manager. В этом случае при использовании службы DNS появляются дополнительные возможности:

- Обеспечивается безопасная работа приложений с удаленными защищенными узлами ViPNet по DNS-именам при использовании открытых (публичных) DNS-серверов (см. «Незащищенный DNS (WINS) сервер» на стр. 147).
- Появляется возможность взаимодействия защищенного узла ViPNet со своим координатором по DNS-имени путем публикации на DNS-сервере IP-адреса, не принадлежащего координатору (например, IP-адреса доступа к координатору через NAT-устройство). При автоматической публикации адреса доступа к координатору на публичном DNS-сервере (технология динамического DNS, или DYN DNS) можно организовать безопасный доступ к координатору, адрес доступа к которому динамически изменяется.

DNS (WINS) сервер на защищенном или туннелируемом узле

Особенности использования

Использование DNS (WINS) сервера, расположенного на защищенном или туннелируемом узле, имеет следующие особенности:

- Для обеспечения работоспособности служб имен DNS и WINS не нужно выполнять никаких дополнительных настроек ПО ViPNet.
- Если DNS (NetBIOS) имена и соответствующие им IP-адреса защищенных и туннелируемых узлов автоматически регистрируются на DNS (WINS) сервере, то технология ViPNet обеспечивает автоматическую публикацию на этом сервере требуемых реальных или виртуальных IP-адресов защищенных и туннелируемых узлов. ViPNet-драйвер на DNS (WINS) сервере (или на координаторе, туннелирующем этот сервер) выполняет подмену адреса в IP-пакете на виртуальный или реальный IP-адрес.
- Если к DNS (WINS) серверу обращается защищенный или туннелируемый узел, к ответу добавляется идентификатор запрашиваемого узла в сети ViPNet (или идентификатор координатора, который туннелирует запрашиваемый узел). По этому идентификатору программное обеспечение ViPNet на узле, с которого был отправлен запрос (или на координаторе, его туннелирующем), определяет правильный адрес доступа к запрашиваемому узлу — реальный или виртуальный.
- Если к защищенному DNS (WINS) серверу обращается открытый компьютер, программное обеспечение ViPNet на DNS (WINS) сервере или на туннелирующем координаторе обрабатывает ответ таким образом, чтобы сообщить открытому компьютеру реальные IP-адреса защищенных и туннелируемых узлов, даже если для них опубликованы виртуальные IP-адреса.

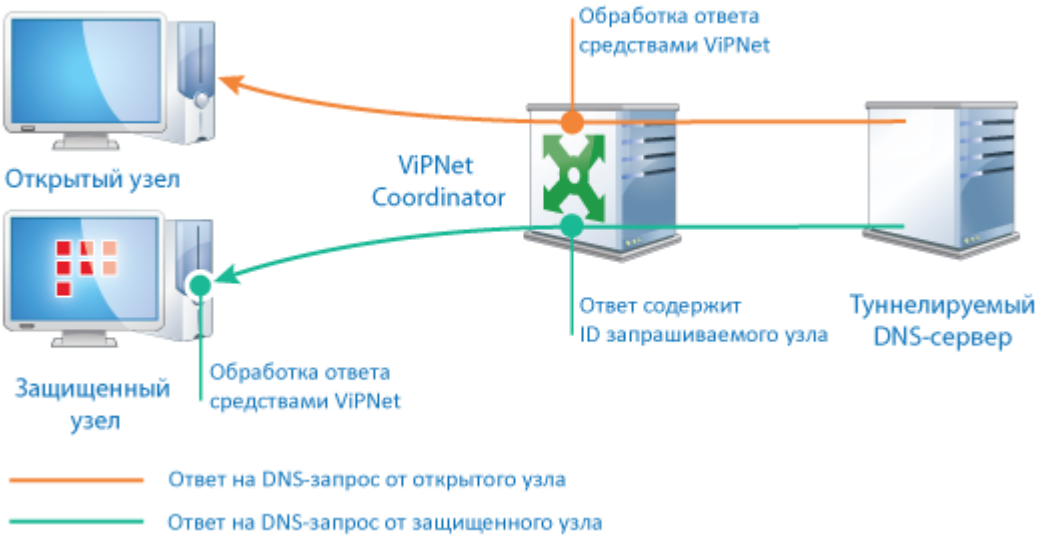


Рисунок 54: DNS-сервер на защищенном или туннелируемом узле

Рекомендации по настройке

При использовании DNS (WINS) сервера, расположенного на защищенном или туннелируемом узле, и при необходимости публикации виртуальных IP-адресов следует соблюдать следующие рекомендации:

- При регистрации вручную на DNS (WINS) сервере IP-адресов защищенных и туннелируемых узлов следует указывать их виртуальные или реальные IP-адреса, по которым эти узлы видны в программе ViPNet Монитор, установленной на DNS (WINS) сервере, или на координаторе, осуществляющем туннелирование этого сервера.

- Если DNS (WINS) сервер расположен на узле с ПО ViPNet, то в подсети этого сервера не следует размещать туннелируемые каким-либо координатором узлы, с которых будут поступать запросы на сервер (или адреса которых будут запрашиваться другими узлами). Если сервер расположен на координаторе, то данное требование относится к туннелируемым узлам других координаторов.

- Если DNS (WINS) сервер туннелируется координатором, то в подсети этого сервера не следует размещать узлы с ПО ViPNet, с которых будут поступать запросы на сервер (или адреса которых будут запрашиваться другими узлами).

- Если возникает необходимость размещения узлов в нарушение приведенных рекомендаций, то на узлах с ПО ViPNet следует снять флажок **Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера** (см. «Настройка доступа к

узлам, туннелируемым другим координатором» на стр. 129), а на туннелируемых узлах настроить частный маршрут на узлы с ПО ViPNet через координатор.

Незащищенный DNS (WINS) сервер

Особенности использования

Часто возникает задача получения доступа к координатору с динамически изменяющимся внешним адресом доступа (например, координатор подключен к сети через DSL-модем) со стороны других защищенных узлов. Для решения данной задачи можно опубликовать адрес этого координатора на публичном DNS-сервере, расположенном в Интернете, и задать DNS-имя координатора в программе ViPNet Монитор на других узлах. В корпоративной сети может возникнуть необходимость в использовании публичного DNS-сервера и в других случаях.

Однако публичные DNS-серверы могут быть подвержены различным сетевым атакам, в результате которых происходит подмена IP-адреса запрашиваемого сетевого ресурса с целью заставить защищенный компьютер обратиться на атакующий компьютер. Если такая атака удастся, при обращении к защищенному узлу по DNS-имени он установит с атакующим компьютером открытое соединение, так как IP-адрес атакующего компьютера не известен ViPNet-драйверу. В результате злоумышленник может получить интересующую его информацию с защищенного компьютера.

Рисунок 55: Атака на публичный DNS-сервер

Чтобы предотвратить атаки подобного рода, для защищенных прикладных серверов, регистрируемых на публичном DNS-сервере и доступных с защищенного узла, в

программе ViPNet Монитор на этом узле следует указать DNS-имена (см. «Настройка доступа к защищенным узлам» на стр. 125). Тогда при обращении к серверу по DNS-имени независимо от адреса, подставленного злоумышленником, при приеме ответа на DNS-запрос ViPNet-драйвер подставит уже известный ему IP-адрес видимости узла (реальный или виртуальный), соответствующий заданному в программе ViPNet Монитор DNS-имени.

Рекомендации по настройке

При использовании открытого DNS-сервера следует выполнять следующие рекомендации:

- Если внешний IP-адрес доступа к координатору может изменяться, для организации доступа к этому координатору по DNS-имени, зарегистрированному на открытом DNS-сервере, в программе ViPNet Монитор на защищенных узлах для данного координатора следует указать DNS-имя.

- Если на узле с установленным ПО ViPNet другие защищенные узлы доступны по виртуальным IP-адресам, и необходимо обеспечить доступ к этим узлам по DNS-именам, зарегистрированным на открытом DNS-сервере, то эти DNS-имена следует указать в программе ViPNet Монитор. При этом на открытом DNS-сервере может быть зарегистрирован любой адрес (реальный или виртуальный). Технология ViPNet обеспечит защищенное соединение по виртуальному адресу видимости (см. «Адреса видимости» на стр. 482) узла вне зависимости от типа опубликованного адреса.

- Как было сказано выше, даже если доступ к защищенным узлам обеспечивается по реальным адресам, для обеспечения безопасности важно указать их DNS-имена в программе ViPNet Монитор.

Во всех описанных случаях DNS-имена защищенных узлов могут быть заданы вручную на каждом сетевом узле (см. «Настройка доступа к защищенным узлам» на стр. 125), однако рекомендуется указывать DNS-имена централизованно в программе ViPNet Центр управления сетью или ViPNet Network Manager.

Использование защищенного DNS (WINS) сервера для удаленной работы с корпоративными ресурсами

Удаленные пользователи подключаются к сети ViPNet через Интернет. Они могут работать дома, в интернет-кафе, в гостинице или других местах, где IP-адреса и используемые DNS (WINS) серверы определяются поставщиком услуг Интернета. Однако для работы со многими корпоративными приложениями требуется использовать DNS (WINS) сервер корпоративной сети. Использование корпоративного DNS (WINS) сервера позволяет обращаться к серверам и другим узлам корпоративной сети по их именам, а не по IP-адресам. При этом преобразование DNS (WINS) имен в IP-адреса обеспечивается как для адресов корпоративной сети, так и для адресов Интернета.

Автоматическая регистрация DNS (WINS) серверов

Для удаленного доступа к корпоративным ресурсам по DNS-именам должны быть выполнены следующие условия:

- В системном файле `hosts`, который устанавливает соответствие между IP-адресами и именами компьютеров, не должно быть записей об узлах корпоративной сети. Этот файл расположен в папке `%systemroot%\System32\drivers\etc\` (по умолчанию это `C:\Windows\System32\drivers\etc\`).
- В программе ViPNet Монитор должно быть настроено подключение через межсетевой экран с динамической трансляцией адресов (см. «О подключении через межсетевой экран с динамической трансляцией адресов» на стр. 113).
- В свойствах подключения к сети должен быть указан адрес корпоративного DNS (WINS) сервера.

Вы можете указать адрес корпоративного DNS-сервера в свойствах подключения к сети вручную. Однако рекомендуется задать адреса корпоративных DNS-серверов централизованно. Для этого администратору сети ViPNet следует указать сетевые узлы или туннелируемые узлы, на которых расположены DNS-серверы, в программе ViPNet Центр управления сетью или ViPNet Network Manager. В этом случае список корпоративных DNS-серверов будет передан на сетевые узлы ViPNet вместе с ключами и

справочниками. На сетевых узлах программа ViPNet Монитор будет определять текущие IP-адреса видимости корпоративных DNS-серверов (реальные или виртуальные) и автоматически изменять адреса DNS-серверов в настройках сетевых интерфейсов компьютера.

Рассмотрим следующий пример. Сотрудник, работающий в главном офисе на ноутбуке с установленным ПО ViPNet Client, подключается к защищенному корпоративному DNS-серверу по одному адресу (например, 10.0.0.25). В какой-то момент времени этот сотрудник отправляется со своим ноутбуком в командировку в другой офис, и DNS-сервер главного офиса становится доступен по другому IP-адресу (например, 11.0.0.3). При этом сотруднику нужно подключиться через Интернет к корпоративным ресурсам главного офиса.

При регистрации DNS-сервера средствами операционной системы сотруднику потребуется на ноутбуке изменять настройки подключения к сети, что неудобно, поскольку после возвращения в главный офис эти настройки нужно будет вернуть в исходное состояние. Если узлы, на которых расположены DNS-серверы, заданы в программе ViPNet Центр управления сетью или ViPNet Network Manager, изменять настройки подключения к сети вручную не требуется.

Если по какой-либо причине адреса корпоративных DNS-серверов не заданы в программе ViPNet Центр управления сетью или ViPNet Network Manager, на сетевом узле вы можете задать список защищенных DNS-серверов вручную, как описано ниже.

Создание списка DNS (WINS) серверов вручную

Если список корпоративных DNS (WINS) серверов не был задан централизованно в программе ViPNet Центр управления сетью или ViPNet Network Manager (см. «Автоматическая регистрация DNS (WINS) серверов» на стр. 149), вы можете создать такой список вручную на вашем сетевом узле. В этом случае программа ViPNet Монитор также будет определять текущие IP-адреса видимости корпоративных DNS-серверов и автоматически изменять настройки сетевых интерфейсов компьютера.

Для регистрации корпоративного DNS (WINS) сервера вручную выполните следующие действия:

1. В любом текстовом редакторе (лучше «Блокнот») создайте пустой текстовый файл `DNS.TXT`.
2. Внесите в него запись о корпоративном DNS (WINS) сервере. О том, как указать информацию о сервере, см. в разделах ниже. Формат записей в файле `DNS.TXT` отличается в зависимости от того, установлен ли корпоративный DNS (WINS) сервер на защищенном узле или туннелируется координатором.

3 Сохраните файл в папке \DATABASES\DNSWINSLIST, находящейся в папке установки ПО ViPNet (если папка не существует, создайте ее).

Примечание. Все операции по созданию и редактированию файла DNS.TXT можно производить без выгрузки программы ViPNet Монитор из памяти компьютера.

В файле DNS.TXT можно зарегистрировать сразу несколько DNS (WINS) серверов. В этом случае на всех сетевых интерфейсах компьютера списки IP-адресов DNS (WINS) серверов будут дополнены IP-адресами, по которым в данный момент доступны указанные серверы. Одновременно в настройках сетевых интерфейсов сохранятся IP-адреса, полученные по DHCP или заданные на сетевых интерфейсах вручную, если эти IP-адреса не принадлежат указанным в DNS.TXT серверам.

Примечание. Если используемые DNS (WINS) серверы перечислены в файле DNS.TXT, задавать их адреса в сетевых настройках Windows не требуется.

Если корпоративный DNS (WINS) сервер установлен непосредственно на сетевом узле ViPNet

Если корпоративный DNS (WINS) сервер установлен на защищенном сетевом узле, то в файле DNS.TXT укажите следующую информацию:

- Для DNS-сервера:

  ```
  [DNSLIST]
  ID00=<идентификатор>;
  ```

- Для WINS-сервера:

  ```
  [WINSLIST]
  ID00=<идентификатор>;
  ```

  где: <идентификатор> — шестнадцатеричный идентификатор сетевого узла ViPNet, на котором установлен DNS (WINS) сервер, с номером сети;

Примечание. Чтобы узнать идентификатор узла, в программе ViPNet Монитор в разделе **Защищенная сеть** дважды щелкните сетевой узел, на котором установлен DNS (WINS) сервер. Откроется окно **Свойства узла**. На вкладке **Общие** в первой строке будет указан идентификатор сетевого узла.

`ID00` — идентификатор номера строки, где после ID допустимы любые цифры.

В разделе ниже вы можете ознакомиться с примером составления файла `DNS.TXT` (см. «Пример составления файла DNS.TXT» на стр. 153).

Если корпоративный DNS (WINS) сервер туннелируется координатором

Если корпоративный DNS (WINS) сервер туннелируется координатором, то в файле `DNS.TXT` укажите следующую информацию:

- Для DNS-сервера:

  ```
  [DNSLIST]
  ID00=<идентификатор>-<IP-адрес>;
  ```

- Для WINS-сервера:

  ```
  [WINSLIST]
  ID00=<идентификатор>-<IP-адрес>;
  ```

  где: `<идентификатор>` — шестнадцатеричный идентификатор координатора, туннелирующего DNS (WINS) сервер, с номером сети;

Примечание. Чтобы узнать идентификатор координатора, который туннелирует DNS (WINS) сервер, в программе ViPNet Монитор дважды щелкните его в разделе **Защищенная сеть**. Откроется окно **Свойства узла**. На вкладке **Общие** в первой строке будет указан идентификатор координатора.

`ID00` — идентификатор номера строки, где после ID допустимы любые цифры.

В отличие от ситуации, когда корпоративный DNS (WINS) сервер установлен непосредственно на сетевом узле ViPNet, здесь указывается идентификатор координатора, который туннелирует DNS (WINS) сервер, и через дефис непосредственно IP-адрес DNS (WINS) сервера. Если имеется несколько DNS (WINS) серверов, которые туннелируются одним координатором, их IP-адреса можно перечислить в одной строке через точку с запятой без пробелов после идентификатора координатора:
`ID00=<идентификатор>-<IP-адрес 1>;<IP-адрес 2>`.

При этом следует убедиться, что в списке туннелируемых адресов данного координатора эти IP-адреса также присутствуют.

В разделе ниже вы можете ознакомиться с примером составления файла DNS.TXT (см. «Пример составления файла DNS.TXT» на стр. 153).

Пример составления файла DNS.TXT

Ниже приведен пример того, как может быть составлен файл DNS.TXT:

```
[DNSLIST]
ID00=000100CA-10.0.0.25;
ID01=0001000b;
ID02=000110bc-10.0.0.20;10.0.0.21;10.0.2.132;
[WINSLIST]
ID00=0001000b;
ID01=000101fa-10.0.1.132;10.0.1.133;10.0.1.134;
```

Обратите внимание, что в одном файле DNS.TXT могут содержаться записи как для DNS (WINS) серверов, установленных на сетевых узлах ViPNet, так и туннелируемых тем или иным координатором. Число записей не ограничивается.

Использование DNS-серверов на контроллерах домена

Если в сети ViPNet вашей организации используется служба Active Directory и при этом защищенные контроллеры домена с DNS-серверами, которые в рамках домена синхронизируются между собой, защищены разными узлами ViPNet, то могут возникнуть проблемы разрешения IP-адресов при обращении к ним с других защищенных узлов. Для предотвращения проблем в этом случае необходимо обеспечить регистрацию на всех резервируемых DNS-серверах одного и того же адреса каждого узла.

Воспользуйтесь одним из следующих вариантов:

- Разместите DNS-серверы без установленного ПО ViPNet за отдельным сетевым интерфейсом координатора и настройте туннелирование этих серверов данным координатором (см. «Если корпоративный DNS (WINS) сервер туннелируется координатором» на стр. 152). Другие защищенные и открытые узлы, которые обращаются к DNS-серверам, во избежание конфликтов не должны находиться со стороны данного интерфейса координатора.

  Если регистрация IP-адресов узлов осуществляется на защищенном DNS-сервере автоматически, будут зарегистрированы IP-адреса, соответствующие видимости узлов с данного координатора. Если регистрация IP-адресов узлов осуществляется на DNS-сервере вручную, на каждом DNS-сервере зарегистрируйте IP-адреса видимости узлов (виртуальные или реальные) с этого координатора. Открытые узлы, которые обращаются к DNS-серверу за IP-адресом защищенного узла через координатор, получат реальный IP-адрес этого узла.

- Если размещение DNS-серверов за одним координатором затруднительно или на них установлена программа ViPNet Client, на координаторах, за которыми расположены DNS-серверы, или в программе ViPNet Client настройте видимость узлов (туннелируемых узлов, клиентов и координаторов), зарегистрированных на этих DNS-серверах, по реальным IP-адресам.

  Чтобы изменить IP-адрес видимости всех клиентов, стоящих за координатором, достаточно изменить IP-адрес видимости координатора на одном из клиентов в программе ViPNet Client Монитор, после чего появится сообщение с предложением изменить аналогичным образом IP-адреса видимости клиентов, расположенных за данным координатором.

9

Интегрированный сетевой экран

Основные принципы фильтрации трафика

Фильтрации подвергается весь трафик, который проходит через сетевой узел:

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

Рисунок 56: Виды IP-трафика

Наибольшую опасность представляет трафик из открытой сети, поскольку в случае атаки достаточно сложно обнаружить ее источник и принять оперативные меры по ее пресечению.

И открытый, и защищенный трафик может быть локальным или широковещательным. Под локальным трафиком понимается входящий или исходящий трафик конкретного узла (то есть когда сетевой узел является отправителем или получателем IP-пакетов). Под широковещательным трафиком имеется в виду передача узлом IP-пакетов, у которых IP-адрес или MAC-адрес назначения является широковещательным адресом (то есть передача пакетов всем узлам определенного сегмента сети).

Кроме этого, через координатор может проходить транзитный трафик. Координатор не является ни отправителем, ни получателем транзитных IP-пакетов, которые следуют через координатор на другие узлы.

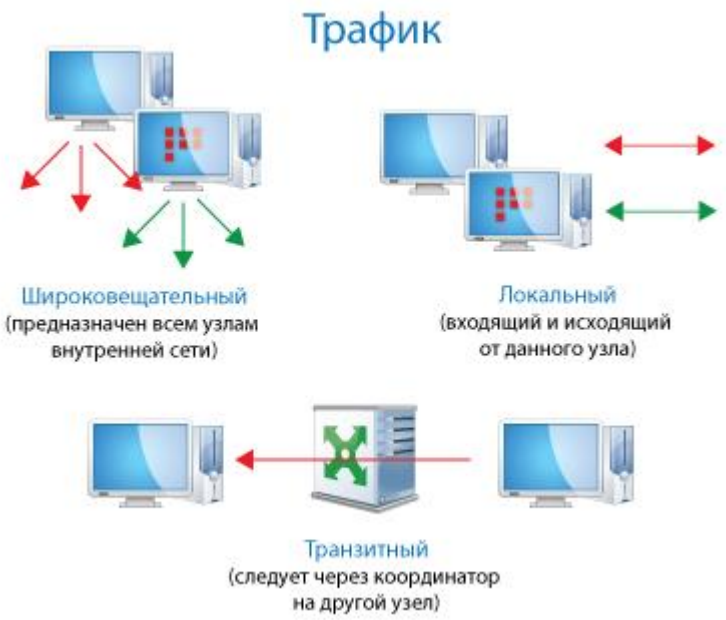


Рисунок 57: Виды защищенного и открытого трафика

Для того чтобы правильно настроить сетевые фильтры, необходимо понимать основные принципы фильтрации трафика.

Все входящие и исходящие открытые и защищенные IP-пакеты проходят комплексную фильтрацию в следующей последовательности:

1 Проверка в соответствии с правилами антиспуфинга (см. «Антиспуфинг» на стр. 192).

> **Примечание.** Данная проверка применяется только при фильтрации открытого трафика, в том числе трафика между координатором и его туннелируемыми устройствами.

Если IP-пакет имеет адрес, разрешенный правилом антиспуфинга, пакет пропускается. В противном случае — блокируется.

2 Проверка в соответствии с сетевыми фильтрами (см. «Общие сведения о сетевых фильтрах» на стр. 159). 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.

Схематично последовательность фильтрации IP-пакетов представлена ниже:

Рисунок 58: Уровни фильтрации трафика

Такой принцип фильтрации обеспечивает высокий уровень безопасности, разрешая соединения только с нужными узлами по заданным протоколам и портам. IP-пакет последовательно проходит ряд фильтров, пока не будет пропущен или заблокирован одним из них. Как только пакет пропускается или блокируется, все последующие фильтры уже не действуют. Если пакет не был обработан ни одним фильтром, то он блокируется.

Сетевые фильтры к зашифрованным IP-пакетам применяются только после их успешной расшифровки и идентификации сетевого узла-источника. В этом случае IP-адреса сетевых узлов не имеют никакого значения.

Примечание. В ПО ViPNet Coordinator версии 3.2 и ниже принцип фильтрации определялся выбранным режимом безопасности.

Общие сведения о сетевых фильтрах

Сетевые фильтры создаются отдельно для защищенного, открытого и туннелируемого трафика. Они выполняют следующие функции:

- Фильтры открытой сети на защищенном узле могут разрешать либо запрещать обмен IP-трафиком с открытыми узлами. Они могут быть созданы отдельно для локального трафика и транзитного трафика.

Примечание. Под открытыми узлами понимаются узлы, на которых не установлено программное обеспечение ViPNet с функцией шифрования трафика. К ним относятся также компьютеры с программным обеспечением ViPNet CryptoService и ViPNet Registration Point.

- Фильтры защищенной сети могут ограничивать обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел имеет связь.
- Фильтры для туннелируемого трафика определяют правила для IP-пакетов, передаваемых между туннелируемыми узлами и узлами сети ViPNet, с которыми данный координатор имеет связь.

Все сетевые фильтры делятся на следующие категории:

- Фильтры, поступившие в составе политик безопасности (см. «Политика безопасности» на стр. 488) из программы ViPNet Policy Manager.

  С помощью специальной опции в режиме администратора можно исключить данные фильтры из списков сетевых фильтров (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305).

- Предустановленные фильтры и фильтры, заданные пользователем.

  В том случае если программа ViPNet Монитор была обновлена до версии 4.x с версии 3.x, предустановленных фильтров не будет. В списках сетевых фильтров будут присутствовать только фильтры, которые действовали в программе до обновления (в сконвертированном формате).

- Фильтры по умолчанию.

Фильтры, поступившие из ViPNet Policy Manager, имеют более высокий приоритет, чем все остальные фильтры, и применяются в первую очередь. После них размещаются предустановленные фильтры и фильтры, заданные пользователем в программе ViPNet Монитор. При определенных полномочиях их всегда можно изменить или удалить. Самыми последними фильтрами являются фильтры по умолчанию. Данная категория представлена одним сетевым фильтром, блокирующим IP-трафик, который не соответствует ни одному из сетевых фильтров из категорий выше.

Последовательность применения сетевых фильтров согласно приоритету изображена на схеме ниже.

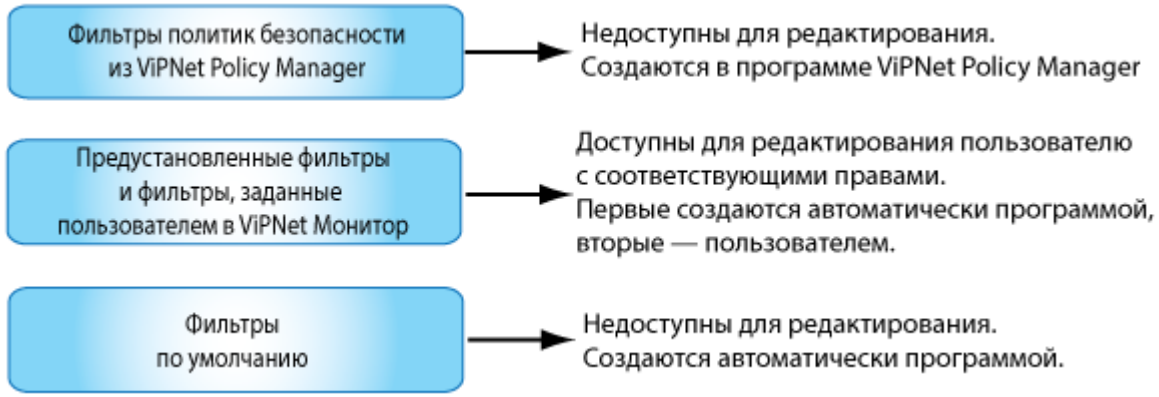


Рисунок 59: Приоритет применения сетевых фильтров

Списки сетевых фильтров представлены на панели просмотра в окне программы ViPNet Coordinator Монитор в разделах **Фильтры защищенной сети**, **Фильтры для туннелируемых узлов**, **Транзитные фильтры открытой сети** и **Локальные фильтры открытой сети**.

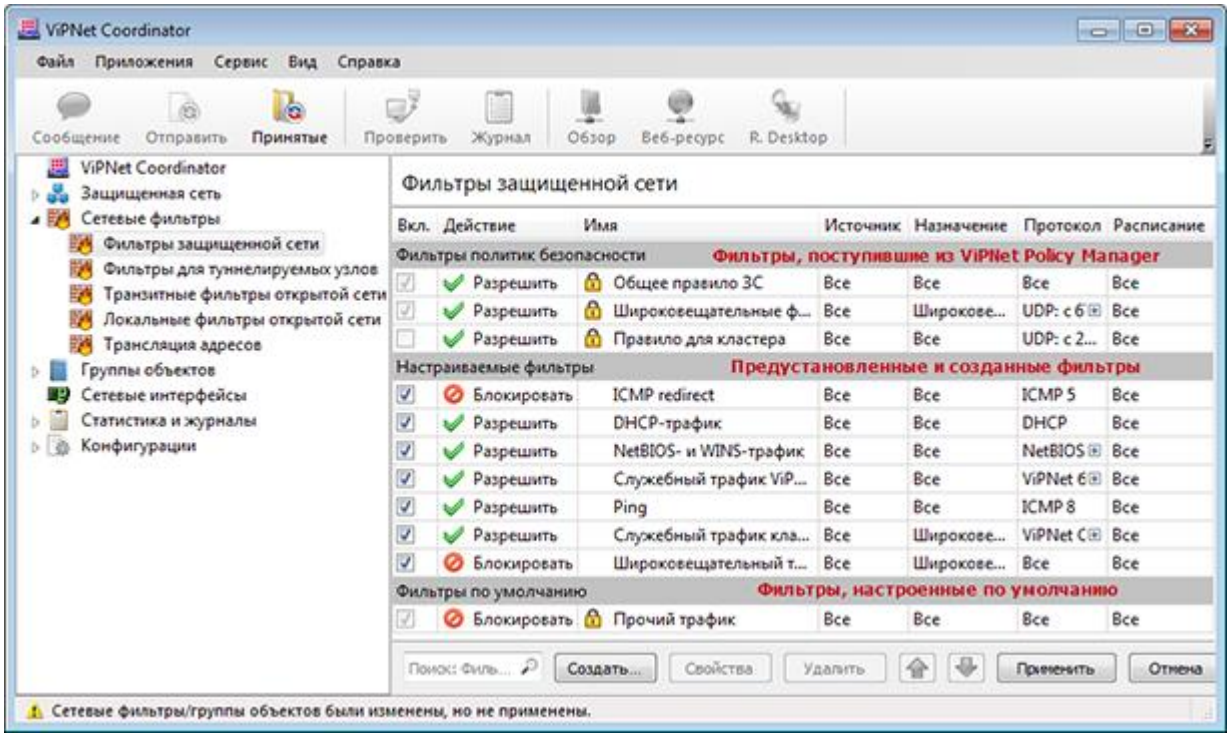


Рисунок 60: Пример отображения фильтров для защищенного трафика разных категорий

Сетевые фильтры имеют следующие особенности:

- Фильтры включают в себя следующие параметры:
  - Действие, применяемое к IP-пакетам. Фильтры могут пропускать (✔) или блокировать (⊘) IP-пакеты, соответствующие заданным параметрам.
  - Источник и назначение IP-пакетов, на которые распространяется действие фильтра.
  - Протоколы фильтрации IP-пакетов.
  - Расписание действия.

  Для задания параметров фильтра могут использоваться группы объектов (см. «Использование групп объектов» на стр. 163).

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

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

- В программе ViPNet Монитор фильтры различных категорий в списках фильтров отображаются в соответствующих группах и располагаются в порядке их приоритета согласно схеме выше.

  Порядок фильтров, поступивших из ViPNet Policy Manager, и фильтров по умолчанию изменить нельзя. Порядок предустановленных фильтров и фильтров, заданных в ViPNet Монитор, вы можете изменять с помощью кнопок  и  .

  Фильтры, которые нельзя отредактировать и удалить, отмечены значком  .

- Чтобы изменить действие фильтра, двойным щелчком откройте свойства фильтра и в разделе **Основные параметры** выберите требуемое значение. Чтобы включить или отключить фильтр, установите или снимите флажок рядом с именем фильтра.

- При изменении настроек сетевых фильтров или создании новых фильтров в строке состояния появляется сообщение о том, что фильтры были изменены, но не применены. Измененные или новые фильтры не вступят в действие до тех пор, пока вы не нажмете кнопку **Применить** и в течение 30 секунд не подтвердите сохранение изменений.

  Если вам не требуется сохранять новые настройки фильтров, нажмите кнопку **Отмена**. В этом случае произойдет возврат к тем настройкам фильтров, которые действовали на момент их изменения.

Использование групп объектов

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

Группы объектов делятся на несколько видов:

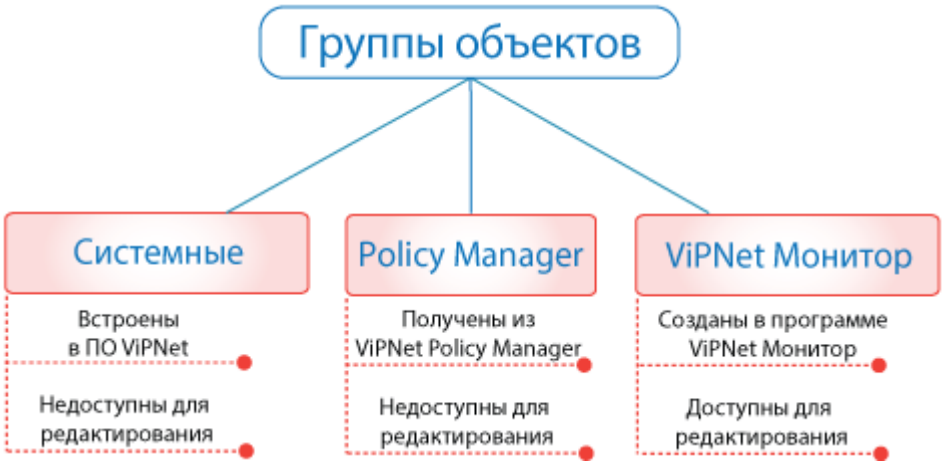


Рисунок 61: Виды групп объектов

Системные группы объектов — встроенные в ПО ViPNet Coordinator объекты с фиксированными именами, которые могут использоваться в создаваемых сетевых фильтрах для задания отправителей и получателей IP-пакетов, а также в других пользовательских группах объектов. Системные группы объектов не отображаются в списках групп и их нельзя изменить или удалить. Список системных групп объектов см. в разделе Системные группы объектов (на стр. 165).

Группы объектов, создаваемые в ПО ViPNet Policy Manager, — группы, которые рассылаются вместе с политиками безопасности. Они недоступны для редактирования и использования в создаваемых сетевых фильтрах, правилах трансляции, других пользовательских группах объектов. В программе ViPNet Монитор можно только просмотреть состав данных групп.

Пользовательские группы объектов — группы объектов, создаваемые пользователем непосредственно в программе ViPNet Монитор, а также некоторые группы, настроенные по умолчанию. Подробнее о группах по умолчанию см. в разделе Пользовательские группы объектов, настроенные по умолчанию (на стр. 166). У каждой группы объектов

есть свой состав, при этом из состава могут быть заданы некоторые исключения. В состав и исключения группы могут быть включены другие группы объектов той же категории или некоторые системные группы объектов. Работа с такими группами объектов осуществляется в окне программы ViPNet Coordinator Монитор в разделе **Группы объектов**.

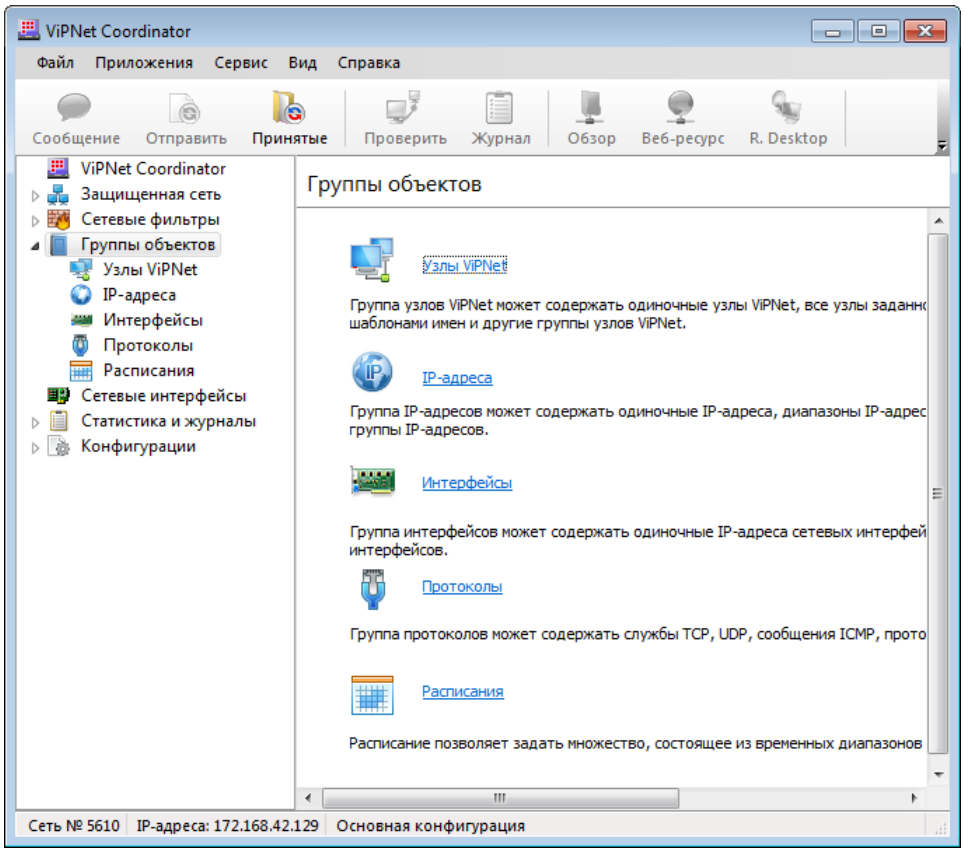


Рисунок 62: Работа с пользовательскими группами объектов

Пользовательские группы объектов делятся на следующие типы:

- **Узлы ViPNet** — группа узлов защищенной сети. Используется в фильтрах защищенной сети и туннелируемых узлов.
- **IP-адреса** — любая комбинация отдельных IP-адресов и диапазонов IP-адресов или DNS-имен. Используется в правилах трансляции IP-адресов и сетевых фильтрах (за исключением фильтров защищенной сети).
- **Интерфейсы** — любая комбинация сетевых интерфейсов или IP-адресов интерфейсов. Используется в сетевых фильтрах только на координаторе (за исключением фильтров защищенной сети).

- **Протоколы** — любая комбинация протоколов и портов. Используется во всех фильтрах и правилах трансляции IP-адресов.
- **Расписания** — любая комбинация условий применения сетевых фильтров по времени и дням недели. Используется во всех фильтрах.

Вы можете создать группу объектов любой категории. Имеет смысл создавать группы из часто используемых наборов объектов. Подробнее о создании групп см. в разделе Создание и изменение групп объектов (на стр. 166).

Системные группы объектов

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

Таблица 4. Системные группы объектов

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

Имя группы объектов	Значение
Групповые адреса	Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255) Можно указать только в качестве назначения для локальных открытых соединений

Пользовательские группы объектов, настроенные по умолчанию

В составе программы ViPNet Coordinator имеется ряд предварительно настроенных групп объектов:

- Две группы IP-адресов по умолчанию:
  - **Публичные IP-адреса** — группа, в составе которой указаны все IP-адреса, за исключением частных IP-адресов.
  - **Частные IP-адреса** — группа, в составе которой указаны IP-адреса локальных сетей: 10.0.0.0; 172.16.0.0; 192.168.0.0.
- Множество групп протоколов по умолчанию. В данном множестве представлены группы протоколов, которые чаще всего используются при создании сетевых фильтров. Одними из них являются группы: **DHCP**, **ViPNet базовые службы**, **ViPNet удаленный просмотр журнала** и другие.
- Две группы расписаний по умолчанию:
  - **Рабочие дни** — группа с расписанием, в котором заданы рабочие дни недели (понедельник — пятница).
  - **Выходные дни** — группа с расписанием, в котором заданы выходные дни (суббота и воскресенье).

Создание и изменение групп объектов

Чтобы создать новую группу объектов, выполните следующие действия:

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

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

Откроется окно свойств группы объектов, в котором вы можете задать параметры новой группы.

4 В разделе **Основные параметры** задайте имя группы объектов. Имя группы должно быть уникальным.

5 В разделе **Состав** определите состав создаваемой группы.

При формировании состава группы типа:

- **Узлы ViPNet —** укажите защищенные узлы, которые необходимо включить в создаваемую группу. Подробнее см. раздел Добавление сетевых узлов (на стр. 171).

  В состав группы узлов защищенной сети вы также можете включить системные группы объектов **Все координаторы** и **Все клиенты** (см. «Системные группы объектов» на стр. 165).

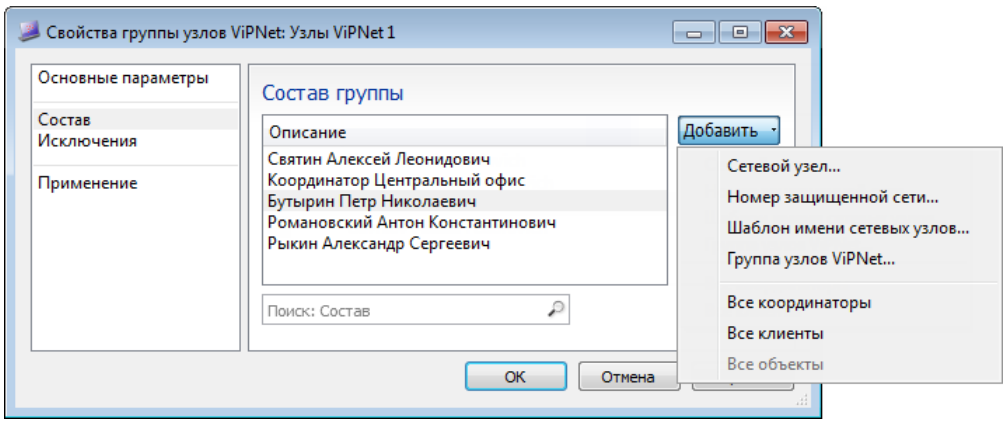


Рисунок 63: Формирование состава группы узлов

- **IP-адреса** — задайте отдельные IP-адреса, диапазон адресов или подсеть либо DNS-имена. Подробнее см. раздел Добавление IP-адресов и DNS-имен (на стр. 172).

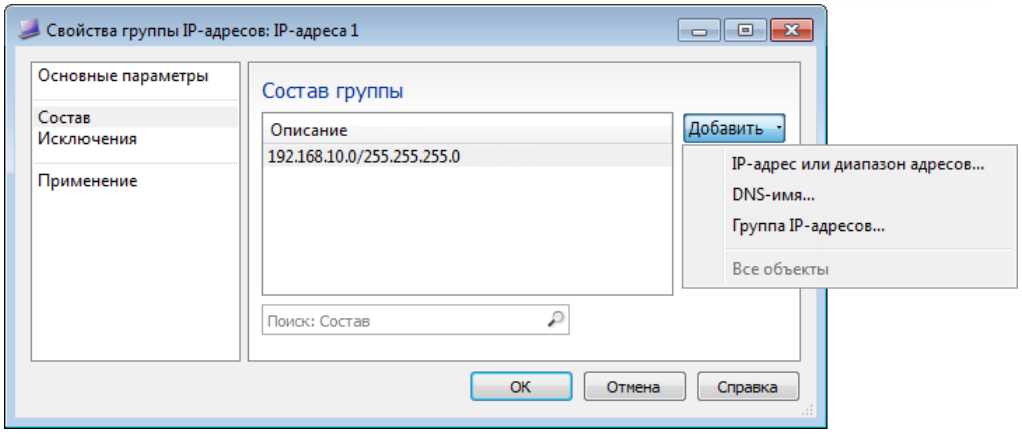


Рисунок 64: Формирование состава группы IP-адресов

- **Интерфейсы** — задайте IP-адрес интерфейса или группы интерфейсов. О добавлении IP-адресов сетевых интерфейсов см. раздел Добавление IP-адресов и DNS-имен (на стр. 172).

  В состав группы интерфейсов вы также можете включить доступные интерфейсы своего узла. Для этого не нужно задавать их IP-адреса, а достаточно выбрать интерфейсы в меню кнопки **Добавить**.

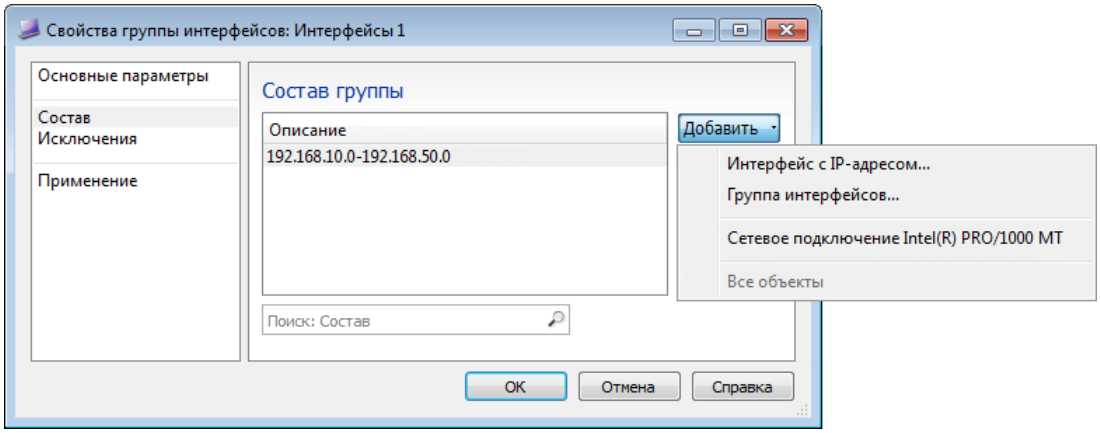


Рисунок 65: Формирование состава группы интерфейсов

- **Протоколы** — задайте протоколы и при необходимости номера портов. Подробнее см. раздел Добавление протоколов (на стр. 173).

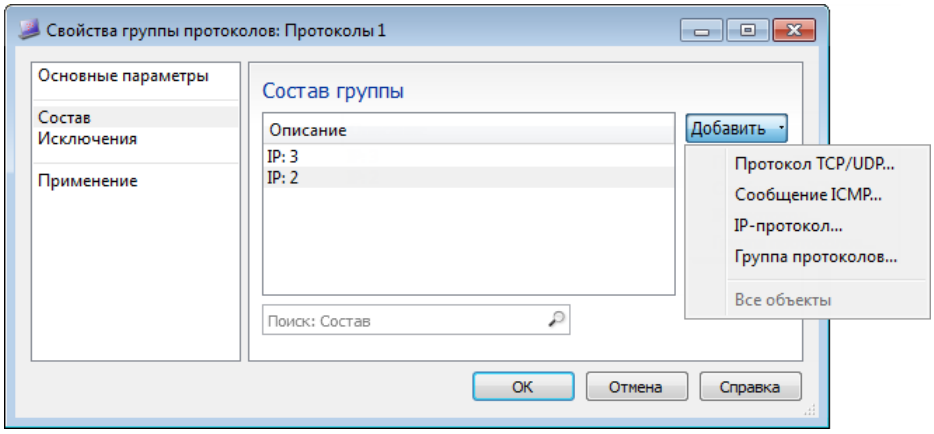


Рисунок 66: Формирование состава группы протоколов

- **Расписания** — задайте расписание, состоящее из дней недели или временных диапазонов. Впоследствии такие расписания можно использовать для ограничения времени действия сетевых фильтров. Подробнее см. раздел Добавление расписаний (на стр. 175).

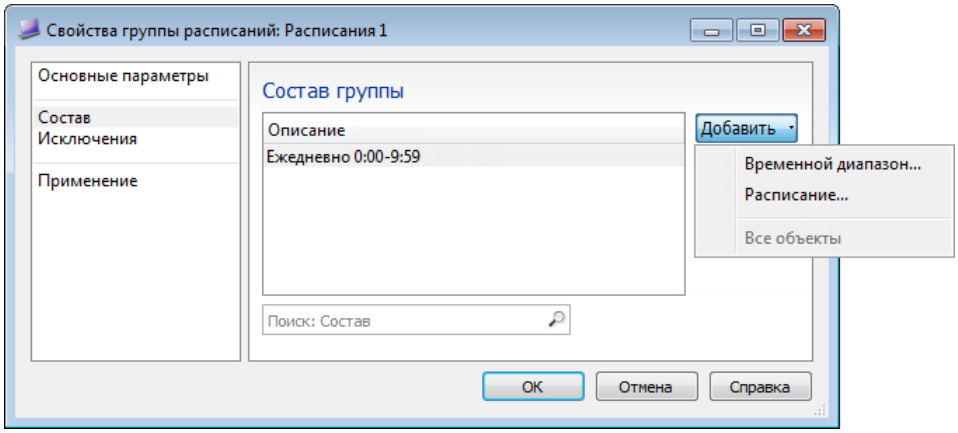


Рисунок 67: Формирование состава группы расписаний

Примечание. В состав каждой группы объектов могут входить группы объектов этого же типа, то есть можно организовать вложенность однотипных групп (см. «Вложенность групп объектов» на стр. 176).

Кроме этого, в составе любой группы объектов вы можете задать системную группу **Все объекты**, например при создании группы, состоящей из всех объектов, кроме некоторых исключений.

6 В разделе **Исключения** задайте исключения из состава группы объектов, то есть те элементы, которые в группу объектов не должны входить. Например, чтобы создать

группу защищенных узлов, состоящую из всех координаторов, кроме одного, добавьте в состав системную группу **Все координаторы**, а в качестве исключения задайте конкретный сетевой узел — координатор.

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

Формирование исключений осуществляется аналогично формированию состава групп объектов.

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

7 По завершении нажмите кнопку **ОК**.

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

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

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

Чтобы удалить группу объектов, выберите ее в соответствующем разделе групп объектов и нажмите кнопку **Удалить**. В появившемся окне подтвердите удаление группы. Если удаляемая группа объектов используется в каких-либо сетевых фильтрах или правилах трансляции адресов либо входит в другие группы объектов, то появится сообщение об этом и она не будет удалена. В данном случае с помощью кнопки **Показать подробности** в окне сообщения просмотрите, в каких элементах используется данная группа, и повторите удаление, предварительно исключив группу из состава данных элементов.

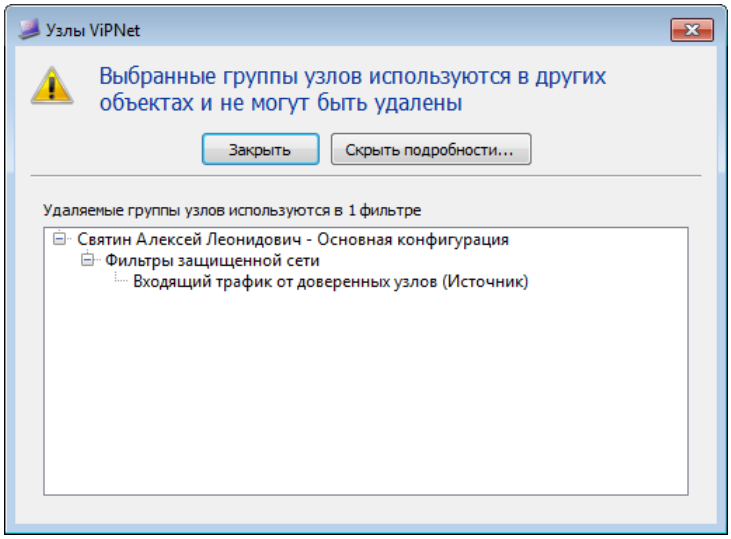


Рисунок 68: Невозможность удаления группы объектов

Чтобы новые или измененные группы объектов вступили в действие, в разделе групп объектов нажмите кнопку **Применить** и в течение 30 секунд подтвердите сохранение изменений. Если вы не хотите сохранять внесенные изменения в группы объектов, нажмите кнопку **Отмена**.

Добавление сетевых узлов

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

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

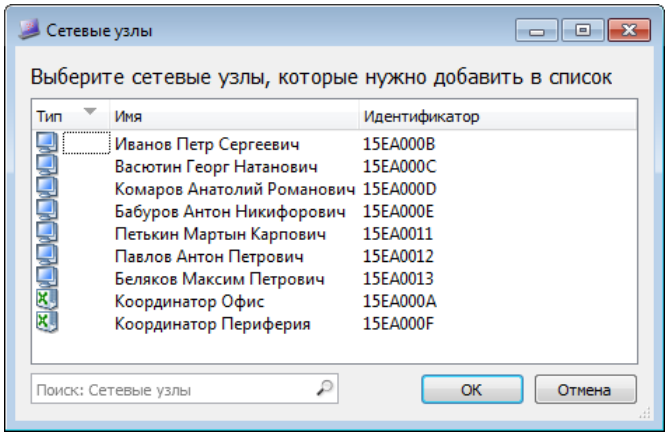


Рисунок 69: Выборочное добавление сетевых узлов

В результате будут добавлены выбранные узлы.

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

  В результате будут добавлены все узлы из заданной сети.

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

  В результате будут добавлены все узлы, имена которых соответствуют заданной маске.

Добавление IP-адресов и DNS-имен

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

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

Чтобы добавить IP-адреса в одном из указанных случаев:

1. В окне свойств группы IP-адресов, сетевого фильтра или правила трансляции в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **IP-адрес**

или диапазон адресов, в окне свойств группы интерфейсов, фильтра или правила при задании сетевых интерфейсов — **Интерфейс с IP-адресом**.

2 В появившемся окне выполните следующие действия:

- Если требуется добавить один конкретный IP-адрес (в том случае, если он известен), установите переключатель в положение **IP-адрес** и в поле напротив введите данный IP-адрес.
- Если требуется задать IP-адреса в рамках некоторой подсети, установите переключатель в положение **Подсеть**, после чего в соответствующих полях задайте адрес и маску данной подсети.
- Если требуется задать диапазон IP-адресов, установите переключатель в положение **Диапазон IP-адресов**, после чего в соответствующих полях задайте начальный и конечный адрес диапазона.

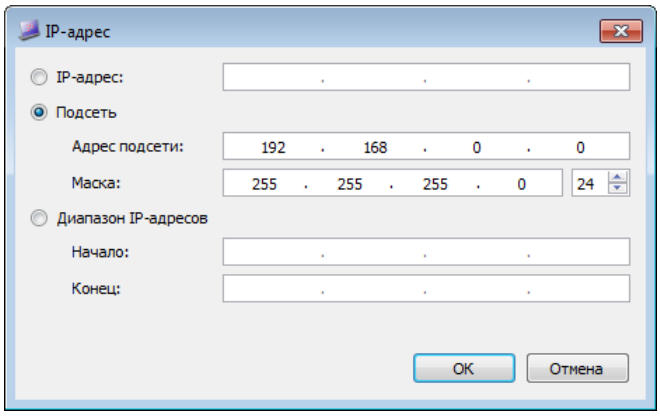


Рисунок 70: Добавление IP-адресов

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

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

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

В результате DNS-имя будет добавлено.

Добавление протоколов

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

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

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

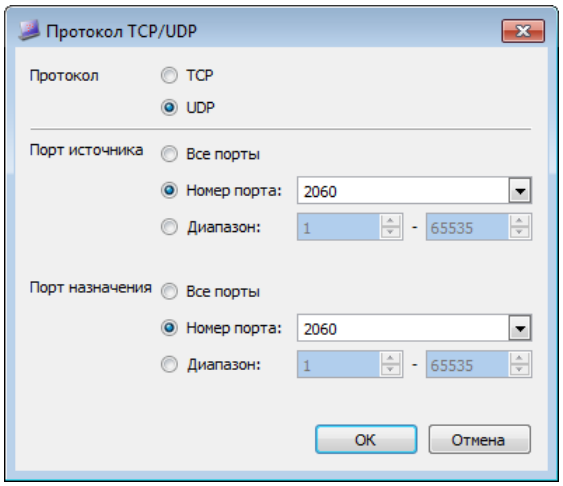


Рисунок 71: Добавление TCP- или UDP-протокола

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

- **Сообщение ICMP** — для добавления ICMP-протокола. В появившемся окне в соответствующих списках выберите тип и код ICMP-протокола (если требуется) и нажмите кнопку **OK**.

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

Добавление расписаний

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

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

1. В окне свойств группы расписаний или сетевого фильтра в соответствующем разделе нажмите кнопку **Добавить** и в меню выберите **Временной диапазон.**

2. В появившемся окне задайте параметры расписания:

   - В группе **Время выполнения фильтра** укажите временной интервал, в течение которого будет действовать сетевой фильтр.
   - Установите переключатель в положение:
     - **Ежедневно**, если сетевой фильтр должен действовать каждый день в указанное время. Если требуется, чтобы фильтр действовал в некоторый период времени (например, в течение двух недель), установите соответствующий флажок и задайте нужный период.
     - **Еженедельно**, если сетевой фильтр должен действовать в определенные дни недели. Установите флажки напротив нужных дней недели.

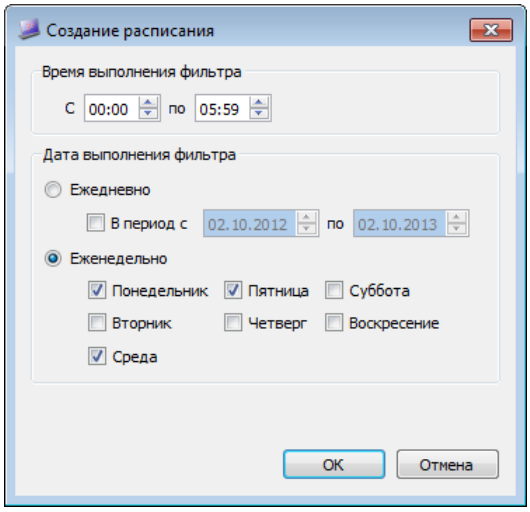


Рисунок 72: Добавление расписания

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

   В результате будет добавлено расписание с заданными параметрами.

Вложенность групп объектов

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

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

1. Разрешить любые соединения для сотрудников IT-отдела.
2. Организовать доступ всех сотрудников в Интернет.
3. Организовать доступ сотрудников департамента финансов к серверу 1С, который установлен в отдельном сегменте локальной сети.

Во всех трех случаях необходимо настроить сетевые фильтры для открытого трафика. При создании сетевых фильтров требуется указать IP-адреса источников и назначений IP-пакетов. Если требуется создать несколько сетевых фильтров для определенного множества IP-адресов, вы можете каждый раз добавлять IP-адреса по одному или диапазонами. Однако рекомендуется объединить часто используемые множества IP-адресов в группы, после чего вы сможете указать эти группы в качестве источников и назначений для нескольких сетевых фильтров. При этом целесообразно создать группы IP-адресов таким образом:

1. Для каждого подразделения создайте группу IP-адресов, включающую IP-адреса компьютеров этого подразделения.
2. Создайте общую группу, включающую вложенные группы IP-адресов всех подразделений.
3. С помощью групп IP-адресов, соответствующих IT-отделу и департаменту финансов, создайте сетевые фильтры для решения первой и третьей задач. С помощью общей группы IP-адресов создайте транзитный фильтр и правило трансляции адреса источника для решения второй задачи (см. «Организация DMZ» на стр. 239).

Рисунок 73: Вложенные группы IP-адресов

Аналогичным образом вы можете использовать вложенность при создании групп объектов других типов. Например, если сотрудники различных подразделений должны иметь доступ к различным типам интернет-ресурсов (веб-серверы, FTP-серверы, почтовые серверы, IP-телефония), вы можете использовать группы протоколов:

1. Создайте группы протоколов для каждого типа интернет-ресурсов.
2. Для каждого подразделения создайте группу протоколов и включите в ее состав вложенные группы, которые соответствуют типам интернет-ресурсов, доступных для этого подразделения.
3. Используйте созданные группы протоколов при создании фильтров открытой сети и правил трансляции адресов, обеспечивающих доступ сотрудников в Интернет.

Рисунок 74: Вложенные группы протоколов

Удобство использования вложенных групп объектов заключается в том, что при изменении структуры сети или политики безопасности вам требуется внести минимальные изменения в существующие сетевые фильтры и группы объектов. Например, если в каком-либо подразделении появятся новые сотрудники, то IP-адреса их компьютеров достаточно будет добавить только в группу IP-адресов этого подразделения. В результате новые сотрудники смогут осуществлять соединения в соответствии с имеющимися сетевыми фильтрами.

Создание сетевых фильтров

В программе ViPNet Coordinator предусмотрена возможность создания следующих фильтров:

- фильтров для защищенной сети,
- фильтров для туннелируемых узлов,
- транзитных фильтров для открытой сети,
- локальных фильтров для открытой сети.

Для создания любого из перечисленных фильтров выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел того типа фильтров, который вы хотите создать.
2. На панели просмотра нажмите кнопку **Создать**. Откроется окно свойств сетевого фильтра, в котором вы можете задать параметры нового фильтра.
3. В разделе **Основные параметры** выполните следующие действия:
   - Введите имя фильтра в соответствующем поле.
   - Укажите действие нового фильтра (блокировать или пропускать трафик), установив переключатель **Действие** в нужное положение. По умолчанию выбрано действие **Блокировать трафик**.

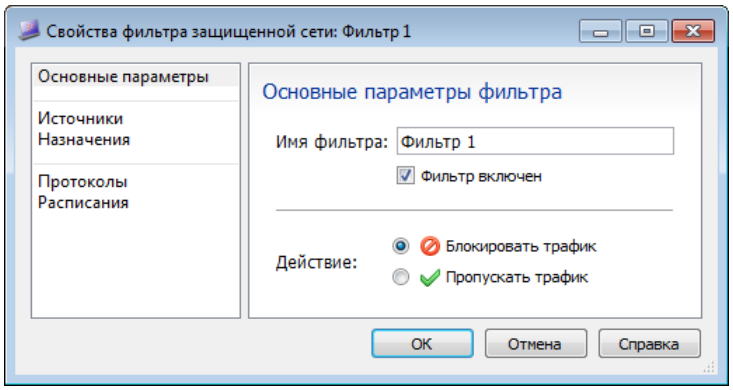


Рисунок 75: Задание основных параметров фильтра

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

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

6 В разделе **Протоколы** укажите протокол для фильтрации. Фильтром в данном случае будут обрабатываться только IP-пакеты, переданные с помощью указанного протокола. Вы можете добавить нужный протокол (см. «Добавление протоколов» на стр. 173) или сразу группу протоколов.

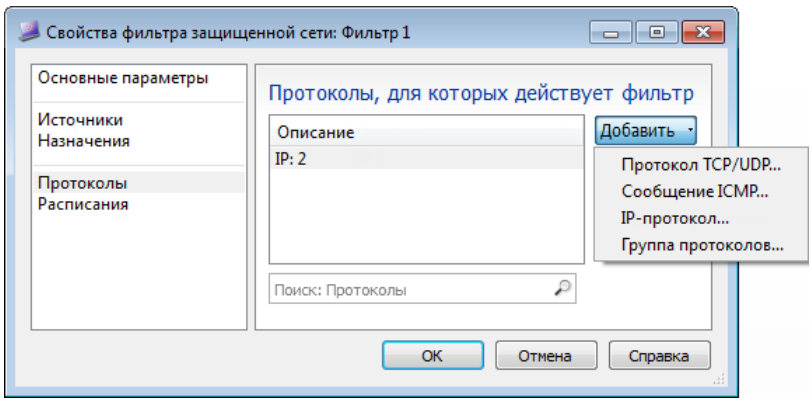


Рисунок 76: Добавление протоколов при создании фильтра

7 В разделе **Расписания** укажите расписание действия фильтра, если требуется. Вы можете добавить новое расписание (см. «Добавление расписаний» на стр. 175) или группу расписаний.

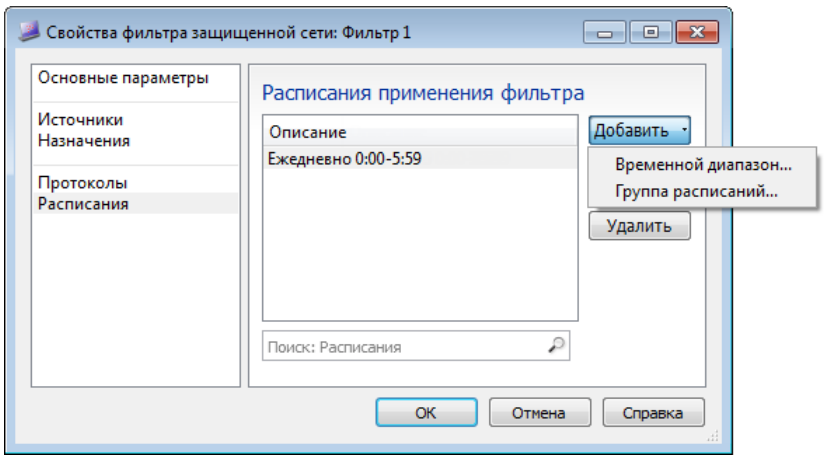


Рисунок 77: Добавление расписания при создании фильтра

8 Для сохранения параметров нового фильтра нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

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

9 Задайте приоритет созданного фильтра, установив его положение в списке с помощью кнопок  и  .

10 Чтобы созданный фильтр вступил в действие, по завершении всех операций с ним нажмите кнопку **Применить** и в появившемся окне в течение 30 секунд подтвердите сохранение изменений.

Подробнее о создании каждого типа фильтров см. соответствующие разделы ниже.

Создание фильтров для защищенной сети

Чтобы создать фильтр для защищенного трафика (см. «Общие сведения о сетевых фильтрах» на стр. 159), выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Фильтры защищенной сети.**

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

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик (см. Рисунок 75 на стр. 178).

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

- Один или несколько узлов защищенной сети (см. «Добавление сетевых узлов» на стр. 171).
- Одну или несколько групп узлов сети ViPNet, если такие созданы (см. «Создание и изменение групп объектов» на стр. 166).
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для исходящих соединений вашего сетевого узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для входящих соединений вашего сетевого узла.
- Системные группы объектов **Все координаторы** и **Все клиенты** (см. «Системные группы объектов» на стр. 165).

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

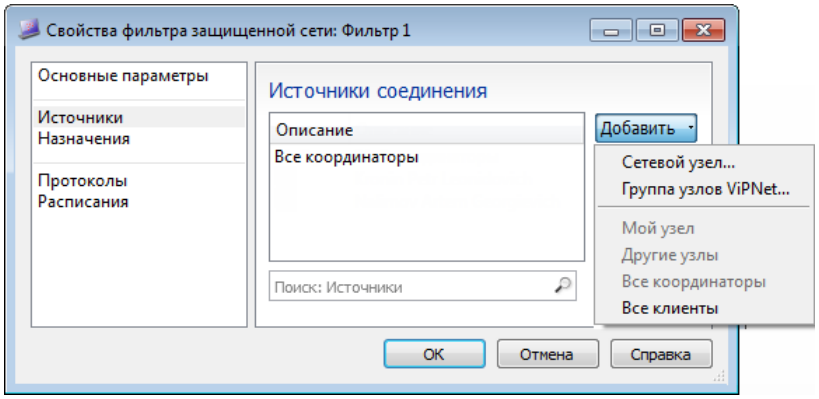


Рисунок 78: Задание отправителя защищенных IP-пакетов

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

- Один или несколько узлов защищенной сети (см. «Добавление сетевых узлов» на стр. 171).
- Одну или несколько групп узлов сети ViPNet, если такие созданы (см. «Создание и изменение групп объектов» на стр. 166).
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для входящих соединений вашего сетевого узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для исходящих соединений вашего сетевого узла.
- Системные группы объектов **Все координаторы** и **Все клиенты** (см. «Системные группы объектов» на стр. 165).
- Системную группу объектов **Широковещательные адреса**. В этом случае действие фильтра будет распространяться на широковещательные пакеты.

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

Если вы не укажете узел назначения, то действие фильтра будет распространяться на IP-пакеты, отправленные на любой узел сети, и ваш узел в том числе.

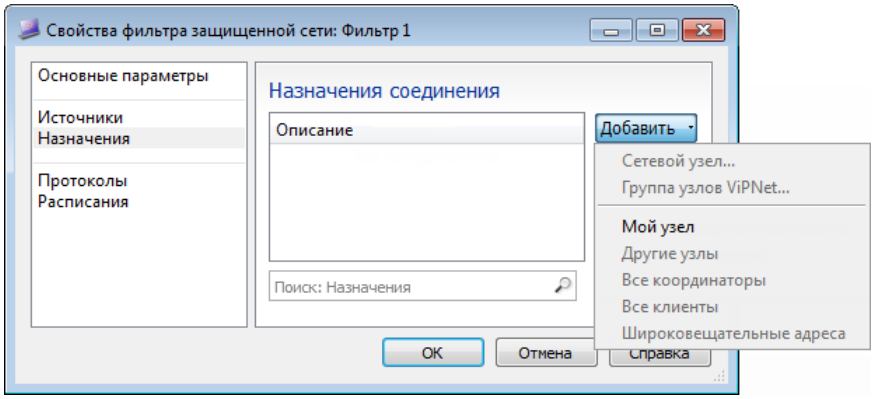


Рисунок 79: Задание получателя защищенных IP-пакетов

6 В разделе **Протоколы** укажите протокол для фильтрации.

7 В разделе **Расписания** укажите расписание действия фильтра.

8 Нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

Создание фильтров для туннелируемых узлов

Чтобы создать фильтр трафика между туннелируемыми узлами координатора и защищенными узлами (см. «Общие сведения о сетевых фильтрах» на стр. 159), выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Фильтры для туннелируемых узлов**.

2 На панели просмотра нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового фильтра трафика туннелируемых узлов.

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик (см. Рисунок 75 на стр. 178).

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

- Если отправителем выступает туннелируемый узел, то добавьте:
  - IP-адрес узла либо диапазон IP-адресов, если узлов несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 172).
  - Группу IP-адресов туннелируемых узлов, если такая имеется (см. «Создание и изменение групп объектов» на стр. 166).

- Системную группу объектов **Туннелируемые IP-адреса** (см. «Системные группы объектов» на стр. 165).

- Если отправителем выступает защищенный узел сети ViPNet, то добавьте:
  - Один или несколько узлов защищенной сети (см. «Добавление сетевых узлов» на стр. 171).
  - Одну или несколько групп узлов сети ViPNet, если такие созданы (см. «Создание и изменение групп объектов» на стр. 166).
  - Системные группы объектов **Все координаторы** и **Все клиенты**.

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

Если вы не укажете узел отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любым туннелируемым узлом либо любым защищенным узлом, в зависимости от того, какие заданы узлы назначения.

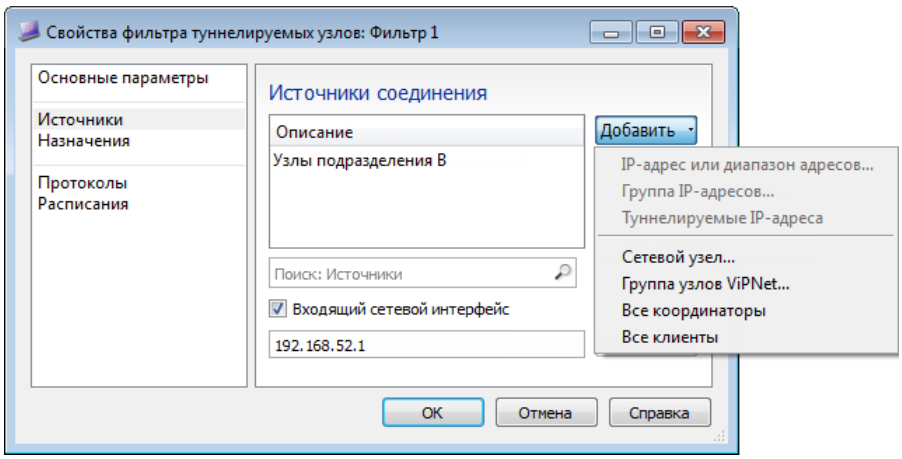


Рисунок 80: Указание отправителя IP-пакетов

5 При необходимости укажите сетевой интерфейс вашего узла, на котором должны быть приняты IP-пакеты от заданных источников при туннелируемом соединении. Для этого установите флажок **Входящий сетевой интерфейс** и добавьте:

- Отдельный IP-адрес интерфейса или диапазон IP-адресов интерфейсов (см. «Добавление IP-адресов и DNS-имен» на стр. 172).
- Один из доступных интерфейсов узла.
- Группу интерфейсов, если такая создана (см. «Создание и изменение групп объектов» на стр. 166).

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

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

7 При необходимости укажите сетевой интерфейс вашего узла, с которого должны быть отправлены IP-пакеты заданным получателям при туннелируемом соединении.

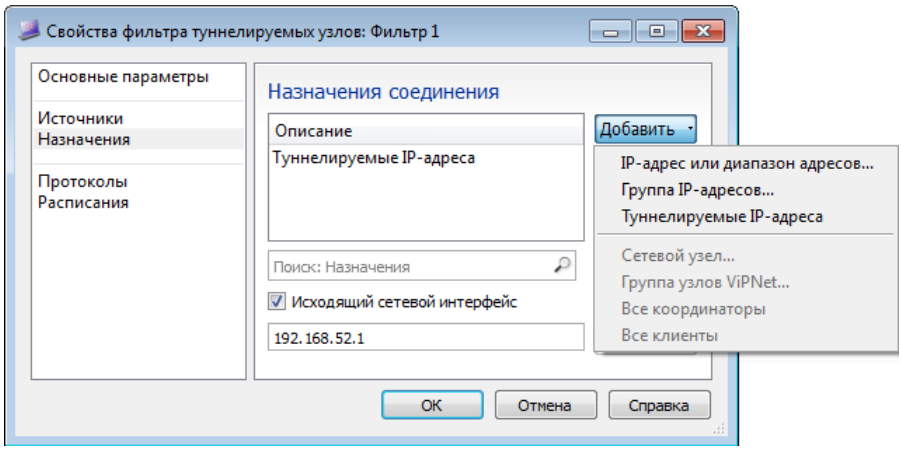


Рисунок 81: Указание назначения соединения при создании фильтра для туннелируемых узлов

8 В разделе **Протоколы** укажите протокол для фильтрации.

9 В разделе **Расписания** укажите расписание действия фильтра.

10 Нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

Создание транзитных фильтров для открытой сети

Транзитные фильтры определяют действия для открытых транзитных IP-пакетов, проходящих через координатор (то есть пакетов, адреса источника и назначения которых не совпадают ни с одним из адресов координатора).

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

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Транзитные фильтры открытой сети**.

2. На панели просмотра нажмите кнопку **Создать**, после чего в появившемся окне задайте параметры нового транзитного фильтра открытой сети.

3. В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик (см. Рисунок 75 на стр. 178).

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

   - IP-адрес или DNS-имя отправителя либо диапазон адресов, если их несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 172).
   - Группы IP-адресов отправителей, если такие созданы (см. «Создание и изменение групп объектов» на стр. 166).

   Если вы не укажете отправителя, то действие фильтра будет распространяться на транзитные IP-пакеты, отправленные любым открытым узлом через координатор.

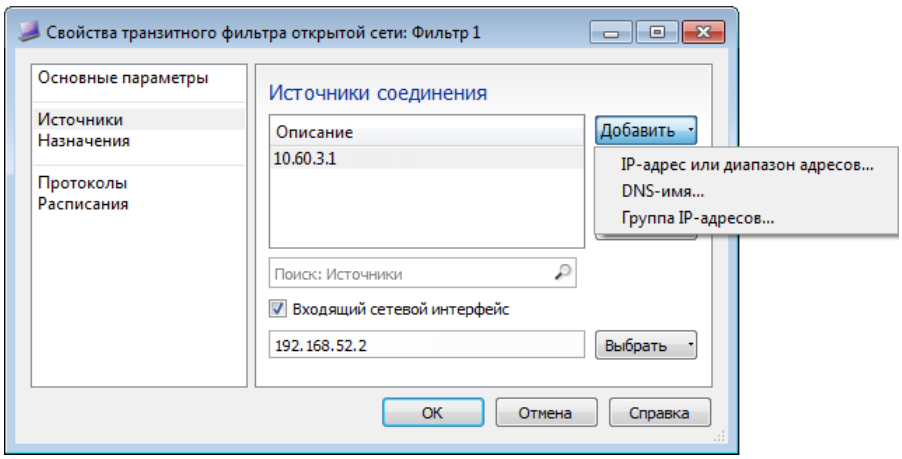


Рисунок 82: Указание отправителя транзитных IP-пакетов

5. При необходимости укажите сетевой интерфейс вашего узла, на котором должны быть приняты транзитные IP-пакеты от указанных источников. Для этого установите флажок **Входящий сетевой интерфейс** и добавьте:

   - Отдельный IP-адрес интерфейса или диапазон IP-адресов интерфейсов (см. «Добавление IP-адресов и DNS-имен» на стр. 172).
   - Один из доступных интерфейсов узла.
   - Группу интерфейсов, если такая создана (см. «Создание и изменение групп объектов» на стр. 166).

6 В разделе **Назначения** аналогичным образом задайте получателя транзитных IP-пакетов и при необходимости укажите сетевой интерфейс вашего узла, с которого должны отправляться транзитные IP-пакеты заданным получателям.

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

7 В разделе **Протоколы** укажите протокол для фильтрации.

8 В разделе **Расписания** укажите расписание действия фильтра.

9 Нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

Пример использования фильтров транзитного IP-трафика приведен в разделе Организация DMZ (на стр. 239).

Создание локальных фильтров для открытой сети

Чтобы создать фильтр для локального открытого трафика (см. «Общие сведения о сетевых фильтрах» на стр. 159), выполните следующие действия:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Локальные фильтры открытой сети.**

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

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик (см. Рисунок 75 на стр. 178).

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

   - IP-адрес или DNS-имя отправителя либо диапазон адресов, если их несколько (см. «Добавление IP-адресов и DNS-имен» на стр. 172).
   - Группы IP-адресов отправителей, если такие созданы (см. «Создание и изменение групп объектов» на стр. 166).
   - Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для исходящих открытых соединений вашего узла.
   - Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для входящих открытых соединений вашего узла.

   Если вы не укажете отправителя, то действие фильтра будет распространяться на IP-пакеты, отправленные любыми открытыми узлами, и вашим узлом в том числе.

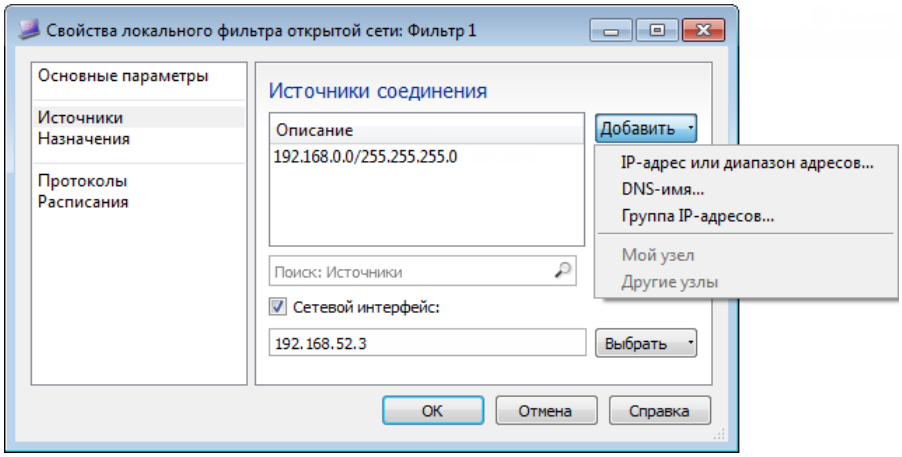


Рисунок 83: Задание отправителя открытых IP-пакетов

5 При необходимости укажите сетевой интерфейс вашего узла, на котором должны быть приняты открытые IP-пакеты от указанных источников либо с которого они должны быть отправлены (в случае, если в качестве отправителя был выбран **Мой узел**). Для этого установите флажок **Сетевой интерфейс** и добавьте:

- Отдельный IP-адрес интерфейса или диапазон IP-адресов интерфейсов (см. «Добавление IP-адресов и DNS-имен» на стр. 172).
- Один из доступных интерфейсов узла.
- Группу интерфейсов, если такая создана (см. «Создание и изменение групп объектов» на стр. 166).

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

- IP-адрес или DNS-имя получателя либо диапазон адресов, если их несколько.
- Группы IP-адресов получателей, если такие созданы.
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для входящих открытых соединений вашего узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для исходящих открытых соединений вашего узла.
- Широковещательные адреса, выбрав системную группу объектов **Широковещательные адреса**. В этом случае действие фильтра будет распространяться на широковещательные пакеты.
- Системную группу объектов **Групповые адреса**. В этом случае действие фильтра будет распространяться на пакеты, отправленные по групповой рассылке.

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

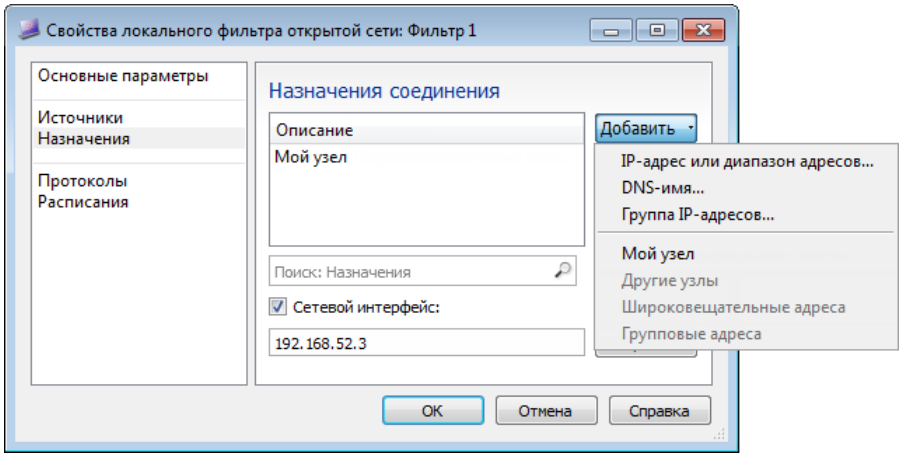


Рисунок 84: Указание получателя IP-пакетов в открытой сети

7 При необходимости укажите сетевой интерфейс вашего узла, с которого должны отправляться IP-пакеты заданным получателям.

8 В разделе **Протоколы** укажите протокол для фильтрации.

9 В разделе **Расписания** укажите расписание действия фильтра.

10 Нажмите кнопку **OK**. В результате в списке на панели просмотра появится новый фильтр.

Практический пример использования групп объектов и сетевых фильтров

Рассмотрим следующий пример использования групп объектов и сетевых фильтров. Допустим, в организации развернут почтовый сервер, на котором установлена программа ViPNet Монитор. Этот защищенный почтовый сервер выполняет следующие функции:

- Обмен сообщениями электронной почты с внешними почтовыми серверами;
- Передача сообщений электронной почты, отправленных удаленными сотрудниками или адресованных им.

Отправка сообщений на почтовый сервер внешними почтовыми серверами и пользователями осуществляется по протоколу SMTP. Передача сообщений электронной почты пользователям производится по протоколам POP3 и IMAP.

Чтобы организовать обмен сообщениями с внешними почтовыми серверами и пользователями и доступ пользователей к электронной почте из Интернета, на защищенном почтовом сервере необходимо создать сетевой фильтр, разрешающий прием и передачу IP-пакетов по 25-му порту протокола TCP (стандартный порт для протокола SMTP), а также по 110-му и 143-му порту (для протоколов POP3 и IMAP соответственно).

Вы можете создать группу протоколов, в которую будут входить все указанные выше протоколы. Данную группу вы сможете использовать при создании сетевого фильтра. Кроме этого, вы сможете использовать ее повторно в дополнительных фильтрах для почтового сервера, если такие в дальнейшем потребуется создать.

Чтобы создать группу протоколов, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Группы объектов** > **Протоколы.**
2. На панели просмотра нажмите кнопку **Создать** и в окне свойств создаваемой группы в разделе **Состав** добавьте все нужные протоколы.
3. Для добавления протокола SMTP в меню кнопки **Добавить** выберите пункт **Протокол TCP/UDP**, после чего в появившемся окне укажите:
   - в качестве протокола — **TCP**;
   - в качестве порта источника — **Все порты**;

- в качестве порта назначения — номер порта **25-smtp**.

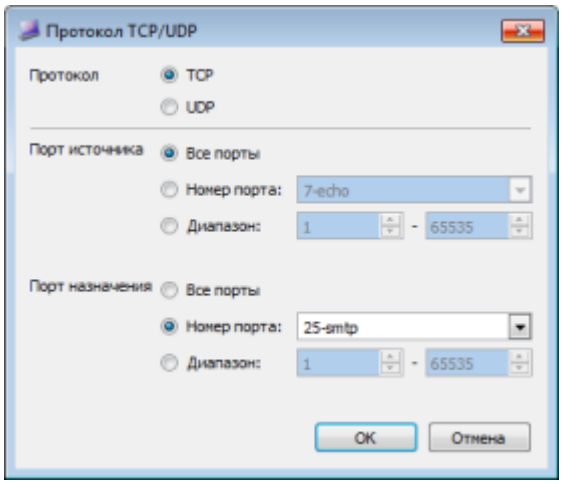


Рисунок 85: Пример добавления протокола SMTP в группу

4 Аналогичным образом добавьте протоколы POP3 и IMAP, указав вместо порта назначения номер порта 110 и 143 соответственно.

5 По завершении добавления протоколов в окне свойств группы нажмите кнопку **ОК**.

В результате будет создана группа протоколов. Используйте данную группу при создании фильтра.

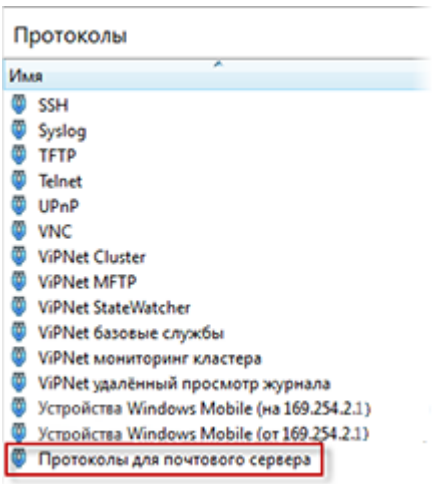


Рисунок 86: Результат создания группы протоколов для почтового сервера

Чтобы создать сетевой фильтр для обмена почтовыми сообщениями с внешними серверами и пользователями, на защищенном почтовом сервере выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Локальные фильтры открытой сети**.
2. В разделе **Локальные фильтры открытой сети** создайте сетевой фильтр для всех IP-адресов, так как IP-адреса внешних почтовых серверов заранее неизвестны и создаваемый фильтр должен распространяться на IP-адреса всех пользователей. Для этого на панели просмотра нажмите кнопку **Создать** и в появившемся окне свойств создаваемого фильтра задайте его параметры.
3. В разделе **Основные параметры** установите переключатель **Действие** в положение **Пропускать трафик**.
4. Чтобы действие фильтра распространялось на все IP-адреса, в разделах **Источники** и **Назначения** не задавайте отправителей и получателей соответственно.
5. В разделе **Протоколы** в меню кнопки **Добавить** выберите пункт **Группа протоколов**, после чего в появившемся окне выберите группу протоколов, которая была создана предварительно.
6. Расписание для данного фильтра формировать не следует.
7. Нажмите кнопку **OK**.

   В результате будет создан сетевой фильтр.

Таким образом, на защищенном почтовом сервере будет разрешен обмен сообщениями с внешними серверами и сотрудниками организации и доступ сотрудников к электронной почте.

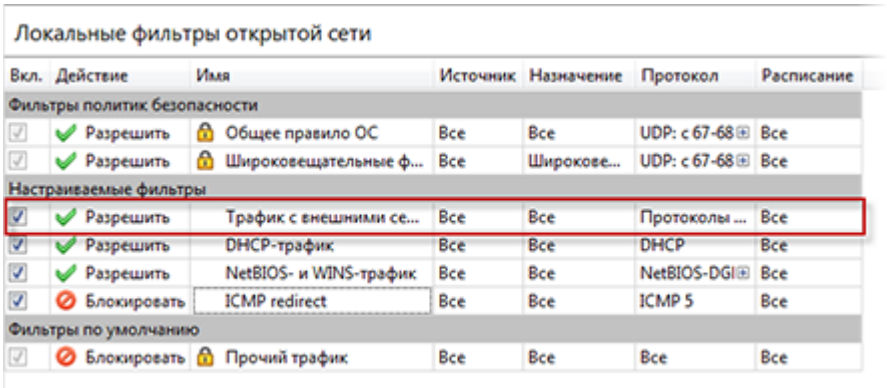


Рисунок 87: Результат создания разрешающего фильтра для протоколов SMTP, POP3, IMAP

Антиспуфинг

Программа ViPNet Coordinator обладает функцией антиспуфинга, то есть блокирования входящих IP-пакетов от отправителей, IP-адреса которых недопустимы на данном сетевом интерфейсе. Антиспуфинг работает только для открытого трафика, поскольку для защищенного трафика IP-адрес отправителя не имеет никакого значения. Открытые пакеты сначала проверяются системой антиспуфинга, а затем уже обрабатываются сетевыми фильтрами (см. «Основные принципы фильтрации трафика» на стр. 156).

Правила антиспуфинга задают для каждого сетевого интерфейса диапазоны IP-адресов, пакеты от которых недопустимы на данном интерфейсе. Пакеты, попадающие в такой диапазон, будут блокироваться.

Как видно из названия, основная задача антиспуфинга — это защита от так называемого спуфинга, одного из видов сетевых атак. При спуфинге злоумышленник посылает на атакуемый компьютер IP-пакет, в котором в качестве адреса отправителя указан не адрес злоумышленника, а адрес другого узла, которому разрешено соединение с этим компьютером. Например, таким образом можно отправить открытый пакет из Интернета через координатор, задав в качестве адреса отправителя адрес частной внутренней сети, которая также подключена к данному координатору. Правила антиспуфинга позволяют исключить такую возможность.

Таким образом, для обеспечения высокого уровня безопасности сети рекомендуется, чтобы на координаторе был включен антиспуфинг. По умолчанию антиспуфинг выключен.

Для включения антиспуфинга:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. В окне **Настройка** в разделе **Управление трафиком** установите флажок **Антиспуфинг**.
3. Нажмите кнопку **Применить**.

Правила антиспуфинга создаются автоматически на основе таблицы маршрутизации сетевого узла. В случае использования сложных схем маршрутизации (с метриками маршрутов или асимметричными маршрутами) функция антиспуфинга может работать некорректно, и ее следует отключить.

Правила антиспуфинга формируются только для открытого трафика следующим образом:

- Для всех интерфейсов, кроме интерфейса по умолчанию, блокируются IP-адреса источника, которые не совпадают с адресами, маршрутизируемыми через данный интерфейс.
- Для интерфейса по умолчанию блокируются IP-адреса источника, которые совпадают с зарегистрированными маршрутами других интерфейсов.

Допустим, на сетевом узле используется следующая таблица маршрутизации:

Таблица 5. Пример таблицы маршрутизации

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	10.0.8.1	10.0.8.54	20
10.0.8.0	255.255.255.0	On-link	10.0.8.54	276
10.0.8.54	255.255.255.255	On-link	10.0.8.54	276
10.0.8.255	255.255.255.255	On-link	10.0.8.54	276
127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
192.168.48.0	255.255.255.0	On-link	192.168.48.1	276
192.168.49.7	255.255.255.255	On-link	192.168.48.1	276
192.168.48.1	255.255.255.255	On-link	192.168.48.1	276
192.168.48.255	255.255.255.255	On-link	192.168.48.1	276
192.168.59.0	255.255.255.0	On-link	192.168.59.1	276
192.168.59.1	255.255.255.255	On-link	192.168.59.1	276
192.168.59.255	255.255.255.255	On-link	192.168.59.1	276
224.0.0.0	224.0.0.0	On-link	127.0.0.1	306
224.0.0.0	224.0.0.0	On-link	10.0.8.54	276
224.0.0.0	224.0.0.0	On-link	192.168.48.1	276
224.0.0.0	224.0.0.0	On-link	192.168.59.1	276
255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
255.255.255.255	255.255.255.255	On-link	10.0.8.54	276
255.255.255.255	255.255.255.255	On-link	192.168.48.1	276
255.255.255.255	255.255.255.255	On-link	192.168.59.1	276

Рассматриваемый узел имеет четыре сетевых интерфейса. Сетевой интерфейс с адресом 127.0.0.1 является интерфейсом «внутренней петли» (loopback), поэтому не будем его учитывать. Сетевой интерфейс с адресом 10.0.8.54 является интерфейсом в маршруте по умолчанию.

В результате на основе приведенной таблицы маршрутизации будет сформирован следующий набор правил антиспуфинга:

- На сетевом интерфейсе с адресом 192.168.48.1 разрешены входящие пакеты только от IP-адресов 192.168.48.0/24, 192.168.49.7.
- На сетевом интерфейсе с адресом 192.168.59.1 разрешены входящие пакеты только от IP-адреса 192.168.59.0/24.
- На сетевом интерфейсе с адресом 10.0.8.54 разрешены все входящие пакеты, кроме пакетов от IP-адресов 192.168.48.0/24, 192.168.49.7, 192.168.59.0/24.

Блокировка IP-трафика

С помощью программы ViPNet Монитор вы можете заблокировать весь IP-трафик компьютера. В этом случае любые соединения с защищенными и открытыми узлами будут запрещены.

Чтобы заблокировать IP-трафик, выполните следующие действия:

1. В программе ViPNet Монитор включите блокировку одним из следующих способов:
   - В меню **Файл** выберите пункт **Конфигурации** > **Блокировать IP-трафик.**
   - На панели задач щелкните правой кнопкой мыши значок программы  и в меню выберите пункт **Блокировать IP-трафик.**
2. Если вы хотите, чтобы после блокировки трафика при определенных условиях трафик был автоматически разблокирован, в окне **Блокирование IP-трафика**:
   - Установите флажок **Разрешить IP-трафик автоматически.**
   - Из списка под флажком выберите условие для автоматической разблокировки IP-трафика: после перезагрузки компьютера или по истечении определенного промежутка времени.

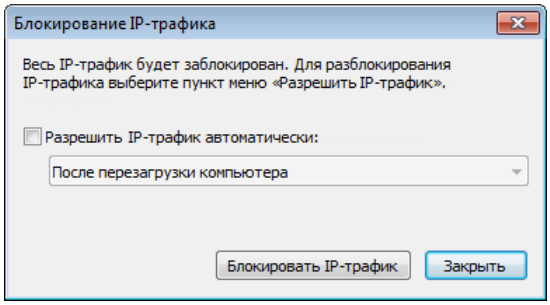


Рисунок 88: Включение блокировки IP-трафика

3. Нажмите кнопку **Блокировать IP-трафик**. Весь открытый и защищенный трафик компьютера будет заблокирован, значок программы ViPNet Монитор в области уведомлений примет следующий вид  .
4. Чтобы снять блокировку IP-трафика, в меню **Файл** выберите пункт **Конфигурации** > **Разрешить IP-трафик.**

Отключение защиты трафика

При необходимости вы можете отключить защиту трафика с помощью программного обеспечения ViPNet Coordinator. В этом случае будет прекращена любая обработка трафика и ведение журнала регистрации IP-пакетов. Соединение с защищенными узлами ViPNet будет невозможно. Также будет невозможно запустить программу ViPNet SafeDisk-V, если вы используете ее совместно с программой ViPNet Coordinator.

Внимание! Не следует работать на сетевом узле с отключенной защитой трафика, так как в этом случае компьютер не защищен от попыток несанкционированного доступа из сети. Рекомендуется отключать защиту трафика только на короткое время для тестирования.

Чтобы отключить защиту трафика, выполните следующие действия:

1. В программе ViPNet Монитор в меню **Файл** выберите пункт **Конфигурации** > **Отключить защиту**.
2. Если вы хотите, чтобы после отключения защиты трафика при определенных условиях защита была автоматически включена, в окне **Отключение защиты**:
   - Установите флажок **Включить защиту IP-трафика автоматически.**
   - Из списка под флажком выберите условие для автоматического включения защиты трафика: после перезагрузки компьютера или по истечении определенного промежутка времени.

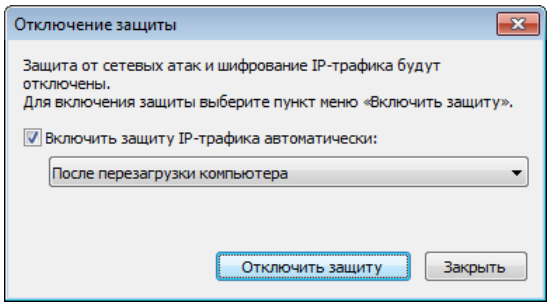


Рисунок 89: Отключение защиты трафика

3. Нажмите кнопку **Отключить защиту**. Защита трафика будет отключена, значок программы ViPNet Монитор в области уведомлений примет следующий вид .

4 Чтобы включить защиту трафика, в меню **Файл** выберите пункт **Конфигурации** > **Включить защиту**.

10

Обработка прикладных протоколов

Общие сведения о прикладных протоколах

Функционирование сетевых сервисов, например таких как, IP-телефония, DNS-служба, FTP-служба, обеспечивается прикладными протоколами. При использовании прикладных протоколов IP-адреса часто передаются в теле IP-пакета. Поведение подобного рода может привести к отсутствию сервиса на защищаемых ресурсах в случае использования технологии виртуальных IP-адресов или трансляции адресов. Кроме того, некоторые протоколы, помимо основного (управляющего) соединения, открывают для передачи данных дополнительные соединения на случайно выбранный порт. Для IP-пакетов, следующих на порт назначения, номер которого заранее не известен, невозможно создать разрешающий фильтр, следовательно, соединение будет заблокировано.

Решить перечисленные проблемы позволяет функция обработки прикладных протоколов, которая обеспечивает:

- Подмену виртуального IP-адреса в теле пакета на реальный IP-адрес в случае использования технологии виртуальных IP-адресов.

Подмену IP-адреса защищаемого узла в прикладном протоколе на транслируемый адрес в случае использования технологии трансляции адресов.

- Активацию разрешающего сетевого фильтра для дополнительного соединения на случайно выбранный порт, открываемый прикладным протоколом.

Примечание. В программе ViPNet Монитор обработка прикладных протоколов осуществляется для всех видов трафика: открытого, защищенного и туннелируемого.

Следует учитывать, что обработка прикладных протоколов не предполагает автоматического разрешения на установление управляющего соединения с открытыми узлами. Установление управляющего соединения с открытыми узлами осуществляется в соответствии с настроенными фильтрами трафика (см. «Общие сведения о сетевых фильтрах» на стр. 159).

Рассмотрим обработку прикладного протокола на примере протокола FTP.

При передаче файлов между FTP-клиентом и FTP-сервером протокол регламентирует установление двух TCP-соединений: управляющее соединение (для отправки команд

FTP-серверу и получения ответов от него) и дополнительное соединение (для передачи данных). Соединение клиента с сервером осуществляется в одном из двух режимов: активном и пассивном. В активном режиме клиент инициирует управляющее соединение с порта из диапазона 1024–65535 на порт с номером 21 на сервере. По номеру порта, с которого клиент инициировал соединение, сервер подключается к клиенту и устанавливает соединение для передачи данных. При этом со стороны сервера соединение происходит через порт с номером 20. В пассивном режиме после установления управляющего соединения сервер сообщает клиенту случайно выбранный номер порта из диапазона 1024–65535, к которому можно подключиться при установлении соединения для передачи данных. Таким образом, в активном режиме клиент должен принять соединение для передачи данных от сервера, в пассивном режиме соединение для передачи данных всегда инициирует клиент.

Для установления управляющего и дополнительного соединений в активном или пассивном режиме работы протокола FTP в программе ViPNet Монитор выполните следующие настройки:

- Создайте фильтр открытой сети (см. «Создание локальных фильтров для открытой сети» на стр. 186), разрешающий исходящее соединение по протоколу TCP на 21 порт FTP-сервера.
- Для разрешения дополнительного соединения в активном режиме работы должна быть включена обработка протокола FTP (см. «Настройка параметров обработки прикладных протоколов» на стр. 203), которая активирует необходимый фильтр трафика. Убедитесь, что она включена.
- Для разрешения дополнительного соединения в пассивном режиме работы специальные настройки не требуются.

Рассмотрим еще один пример — обработку прикладного протокола на примере протокола SIP.

Протокол SIP предназначен для организации, модификации и завершения сеансов связи — мультимедийных конференций, телефонных соединений — и распределения мультимедийной информации.

Вызывающий SIP-клиент отправляет запрос (например, приглашение к сеансу связи, подтверждение приема ответа на запрос, завершение сеанса связи) вызываемому SIP-клиенту с указанием его SIP-адреса. В зависимости от способа установления соединения запрос направляется вызываемому клиенту напрямую, либо с участием прокси-сервера SIP, либо с участием сервера переадресации. Вызываемый клиент в зависимости от типа полученного запроса передает вызывающему клиенту ответ на запрос (например, информацию об ошибке при обработке запроса, запрос успешно обработан, отклонение входящего вызова).

Для установления сеанса связи между SIP-клиентами протокол SIP регламентирует установление соединений TCP и UDP через порт 5060.

Чтобы установить сеанс связи между SIP-клиентами, убедитесь, что включена обработка протокола SIP (см. «Настройка параметров обработки прикладных протоколов» на стр. 203), и создайте фильтр открытой сети, разрешающий входящее и исходящее соединение по протоколам TCP и UDP на порт 5060.

Описание прикладных протоколов

Примечание. В программе ViPNet Монитор версии 3.2 и выше удалена веб-фильтрация и обработка прикладного протокола HTTP.

В программе ViPNet Монитор реализована возможность настройки параметров обработки следующих прикладных протоколов:

- Протокол FTP обеспечивает передачу файлов между FTP-клиентом и FTP-сервером.
- Протокол DNS (Domain Name System) обеспечивает разрешение DNS-имен сетевых узлов в IP-адреса.
- Протокол H.323 обеспечивает работу программ для проведения мультимедийных конференций через IP-сети, в том числе Интернет.
- Протокол SCCP (Skinny Client Control Protocol) обеспечивает передачу сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты Cisco Unity и Cisco CallManager.
- Протокол SIP (Session Initiation Protocol) обеспечивает установление сеансов связи при передаче голосовых звонков, видеоконференций, а также мультимедийной информации.

Примечание. Список поддерживаемых программой ViPNet Монитор прикладных протоколов задан по умолчанию, нельзя добавить протоколы или удалить протоколы из списка.

Настройка параметров обработки прикладных протоколов

Внимание! В сетях, где используется обработка прикладных протоколов средствами ViPNet, на сетевом оборудовании (маршрутизаторах, шлюзах) необходимо отключить функцию DPI (deep packet inspection — глубокий анализ пакетов). Применение DPI может привести к сбоям в работе приложений, использующих протоколы FTP, DNS, H.323, SCCP, SIP.

Чтобы настроить параметры обработки прикладных протоколов для открытого и защищенного трафика, выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. На панели навигации окна **Настройка** выберите раздел **Прикладные протоколы**.

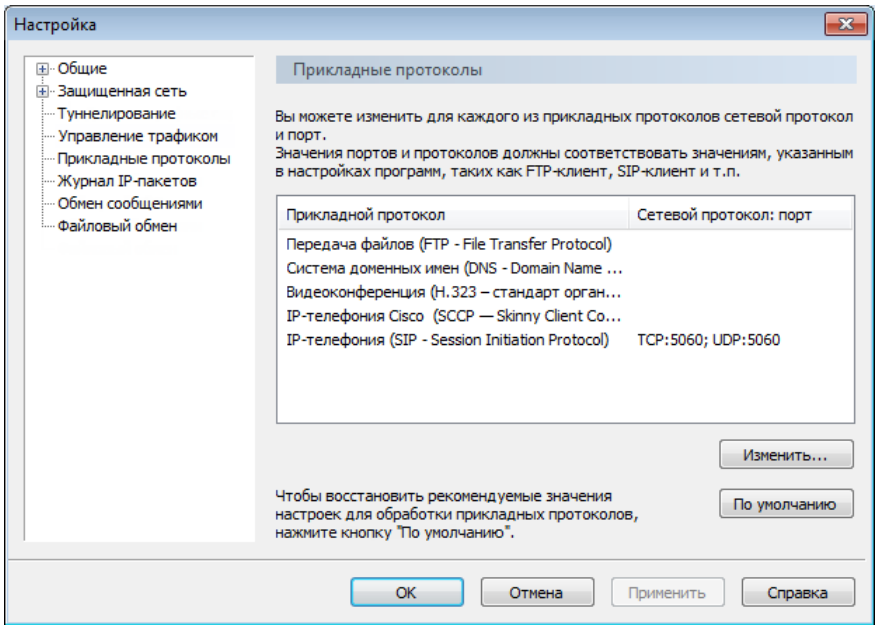


Рисунок 90: Раздел «Прикладные протоколы»

В разделе **Прикладные протоколы** приведен список поддерживаемых программой прикладных протоколов (см. «Описание прикладных протоколов» на стр. 202).

Примечание. По умолчанию для всех прикладных протоколов заданы наиболее часто используемые сетевые протоколы и порты.

Список поддерживаемых программой ViPNet Монитор прикладных протоколов задан по умолчанию, нельзя добавить протоколы или удалить протоколы из списка.

3 В разделе **Прикладные протоколы** выберите протокол, параметры обработки которого требуется отредактировать, затем нажмите кнопку **Изменить.**

4 Если требуется, в окне **Настройка прикладного протокола: <название прикладного протокола>** выполните следующие действия:

- Чтобы включить сетевой протокол, установите соответствующий флажок и задайте порты.

Примечание. Заданные параметры обработки прикладных протоколов должны соответствовать параметрам, указанным в настройках различных приложений, таких как FTP-клиент, DNS-клиент, SIP-клиент и других.

При вводе номеров портов, диапазонов номеров портов их необходимо разделять запятыми.

- Чтобы отключить сетевой протокол, снимите соответствующий флажок.
- Чтобы отключить обработку прикладного протокола:
  - Отключите все сетевые протоколы.
  - В окне предупреждения нажмите кнопку **OK.**

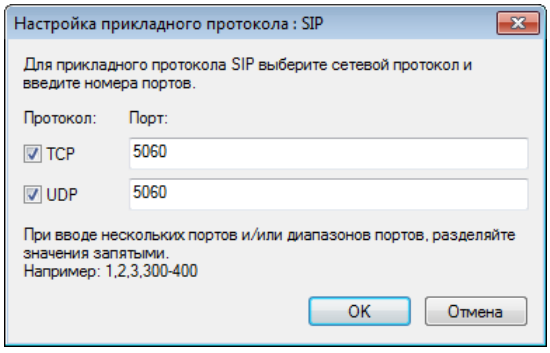


Рисунок 91: Настройка параметров обработки прикладного протокола

По окончании настройки нажмите кнопку **OK.**

Внимание! Не рекомендуется отключать обработку прикладных протоколов, в противном случае работа прикладных программ может быть затруднена.

5 Чтобы сохранить настройки, в окне **Настройка** нажмите кнопку **Применить**.

6 Чтобы восстановить настройки по умолчанию, в разделе **Прикладные протоколы** нажмите кнопку **По умолчанию**.

11

Трансляция сетевых адресов (NAT)

Зачем используется трансляция адресов

Трансляция сетевых адресов (NAT, Network Address Translation) — это механизм преобразования IP-адресов одной сети в IP-адреса другой сети. Положения технологии трансляции адресов регламентируются RFC 2663 http://tools.ietf.org/html/rfc2663.

Трансляция сетевых адресов обычно применяется для решения двух основных задач:

- При необходимости подключения локальной сети к Интернету, когда количество узлов локальной сети превышает выданное поставщиком услуг Интернета количество публичных IP-адресов (см. «Публичный адрес» на стр. 489). Таким образом, NAT позволяет локальным сетям, использующим частные адреса (см. «Частный адрес» на стр. 493), получать доступ к ресурсам Интернета.

  Для решения этой задачи используется трансляция адреса источника (на стр. 210).

- Для организации доступа к внутренним ресурсам из внешней сети. В результате применения технологии NAT локальные сети, имеющие частные адреса, могут быть доступны пользователям Интернета по публичным IP-адресам.

  Для решения этой задачи используется трансляция адреса назначения (на стр. 209).

Правила трансляции адресов могут быть настроены на межсетевом экране — компьютере, разграничивающем локальную (внутреннюю) сеть и глобальную (внешнюю) сеть, например Интернет. Межсетевой экран должен иметь как минимум два сетевых интерфейса:

- Внешний интерфейс — имеет публичный IP-адрес и обеспечивает доступ в Интернет.

- Внутренний интерфейс — имеет частный IP-адрес.

Трансляция сетевых адресов осуществляется для IP-пакетов, проходящих через межсетевой экран из внутренней сети во внешнюю или наоборот.

Трансляция адресов в технологии ViPNet

Внимание! Правила трансляции, описанные в данном разделе, относятся только к открытому трафику. Для защищенного трафика действуют автоматически заданные механизмы трансляции адресов, параметры которых не могут быть изменены.

Трансляция сетевых адресов (см. «Трансляция сетевых адресов (NAT)» на стр. 492) выполняется координатором в том случае, если настроены соответствующие правила (см. «Создание правила трансляции адресов» на стр. 213). На координаторе вы можете настроить правила трансляции адресов (NAT) следующих типов:

- Трансляция адреса назначения устанавливает соответствие между публичными IP-адресами или портами и частными IP-адресами или портами внутренней сети. Данная разновидность NAT применяется в тех случаях, когда один или несколько внутренних узлов должны быть доступны из внешней сети по постоянному IP-адресу (например, веб-серверы).

- Трансляция адреса источника (masquerading) устанавливает соответствие между несколькими частными адресами внутренней сети и одним публичным адресом межсетевого экрана. Данная разновидность NAT используется для предоставления компьютерам из локальной сети с частными адресами доступа к Интернету через межсетевой экран, имеющий всего один публичный адрес. Таким образом, несколько компьютеров локальной сети могут одновременно использовать один публичный IP-адрес.

- Одновременная трансляция адресов источника и назначения. Данная разновидность NAT позволяет организовать обмен данными между двумя сегментами сети таким образом, чтобы из одного сегмента узлы второго сегмента были доступны по IP-адресу координатора (как при трансляции адреса назначения), и при этом пакеты из первого сегмента приходили на узлы второго сегмента от имени соответствующего сетевого интерфейса координатора (как при трансляции адреса источника). Таким образом, для каждого сегмента адреса узлов в другом сегменте будут скрыты.

  Чтобы создать правило для одновременной трансляции адресов источника и назначения, в разделе **Трансляция адресов** одновременно установите флажки **Заменять адрес источника на** и **Заменять адрес назначения на**, затем задайте необходимые параметры (см. «Создание правила трансляции адресов» на стр. 213).

Чтобы обеспечить корректную работу некоторых прикладных протоколов (таких как FTP, SIP) в случае, когда соединение между клиентом и сервером устанавливается с использованием NAT, программное обеспечение ViPNet Coordinator выполняет дополнительную прикладную обработку трафика. Дополнительная обработка необходима для преобразования адресов, которые некоторые прикладные протоколы передают в теле IP-пакетов (см. «Обработка прикладных протоколов» на стр. 198).

Трансляция адреса назначения

Трансляция адреса узла назначения предназначена для организации доступа из Интернета к серверам локальной сети, не имеющим публичного IP-адреса. Правило трансляции адреса назначения ставит в соответствие частным IP-адресам локальных узлов публичный IP-адрес координатора. В соответствии с правилом, в заголовках IP-пакетов публичный IP-адрес (или IP-адрес и порт) назначения заменяется частным адресом локальной сети. Таким образом, по публичному IP-адресу внешние пользователи могут получить доступ к ресурсам локальной сети.

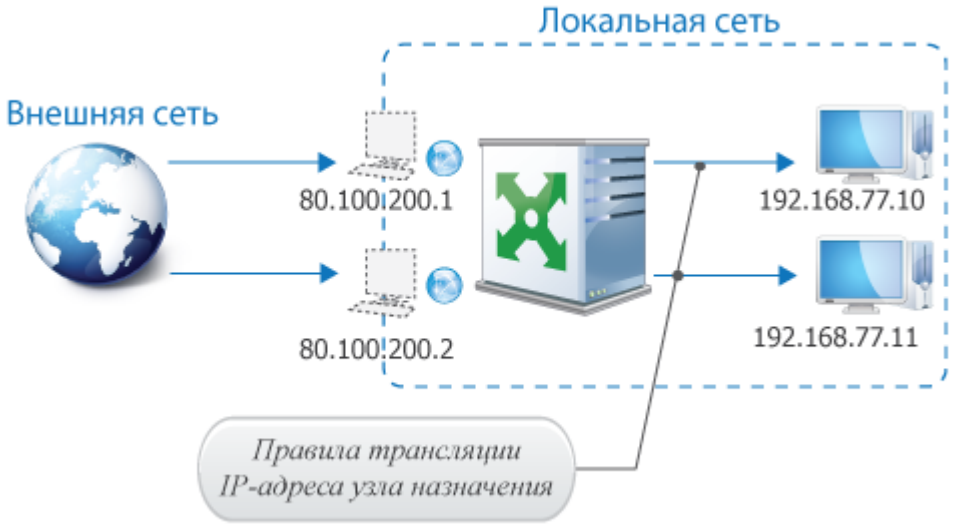


Рисунок 92: Доступ к внутренним ресурсам при помощи правил трансляции IP-адресов узлов назначения

Если для внешнего IP-адреса координатора задано правило трансляции адреса назначения, то при обращении к этому адресу из Интернета будут выполняться следующие преобразования:

- Во входящих IP-пакетах от внешнего узла координатор подменяет адрес получателя (публичный IP-адрес координатора) на локальный адрес в соответствии с

описанным правилом. Затем пакет передается через внутренний сетевой интерфейс на узел локальной сети, которому адресован пакет.

- При прохождении ответных пакетов (в рамках уже созданной сессии) координатор производит обратную замену IP-адресов. Адрес отправителя (IP-адрес локального узла) подменяется на публичный IP-адрес внешнего сетевого интерфейса координатора. Затем ответный пакет отправляется по назначению (узлу в Интернете).

  Таким образом, при передаче в Интернете пакет выглядит так, будто отправитель и получатель этого пакета имеют публичные IP-адреса.

Внимание! При трансляции адреса узла назначения инициировать соединение может только внешний узел. Чтобы локальный узел мог также иметь доступ в Интернет (двусторонний NAT), необходимо в дополнение к правилу трансляции адреса узла назначения задать также правило трансляции адреса источника.

Трансляция адреса источника

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

Рисунок 93: Организация доступа в Интернет при помощи правила трансляции IP-адреса источника

Если на координаторе настроено правило трансляции адреса источника, то транзитные IP-пакеты, проходящие через координатор из локальной сети в Интернет (или другие глобальные сети) будут преобразованы следующим образом:

- В момент передачи IP-пакета из локальной сети в Интернет ViPNet Coordinator преобразует адрес и (или) порт отправителя пакета для протоколов TCP и UDP. Для пакетов протокола ICMP преобразуется адрес отправителя, остальные параметры запоминаются. В процессе преобразования частный адрес отправителя пакета заменяется на публичный адрес внешнего сетевого интерфейса координатора, обеспечивающего доступ в глобальную сеть. При дальнейшей передаче в Интернете пакет имеет публичный IP-адрес отправителя. Номера портов отправителя (для протоколов TCP и UDP) и запоминаемые параметры (для протокола ICMP) пакетов имеют уникальные значения для всех исходящих IP-соединений внешнего сетевого интерфейса координатора. После преобразования пакет отправляется адресату в Интернете.

- При прохождении ответных пакетов ViPNet Coordinator производит обратное преобразование указанных параметров. То есть в момент передачи ответного IP-пакета ViPNet Coordinator заменяет в нем адрес получателя на частный адрес узла локальной сети, которому адресован ответный пакет. Преобразование происходит на основании уникальных номеров портов, присвоенных исходящим пакетам (для протоколов TCP и UDP), и запоминаемых параметров исходящих пакетов (для протокола ICMP). Номера портов (для протоколов TCP и UDP) также преобразуются в свои истинные значения. Затем ответные пакеты передаются через внутренний сетевой интерфейс узлу локальной сети, которому адресован пакет.

Примечание. Для всех протоколов, кроме TCP, UDP и ICMP, преобразуются только IP-адреса. Для протоколов с частичным преобразованием трансляция IP-адреса источника не будет работать, если несколько узлов локальной сети одновременно инициируют соединение с одним и тем же IP-адресом публичной сети.

Создание правила трансляции адресов

Чтобы создать правило трансляции адресов, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Трансляция адресов**.
2. На панели просмотра нажмите кнопку **Создать**. Откроется окно свойств правила трансляции адресов, в котором вы можете задать параметры нового правила.
3. В разделе **Основные параметры** задайте имя нового правила.

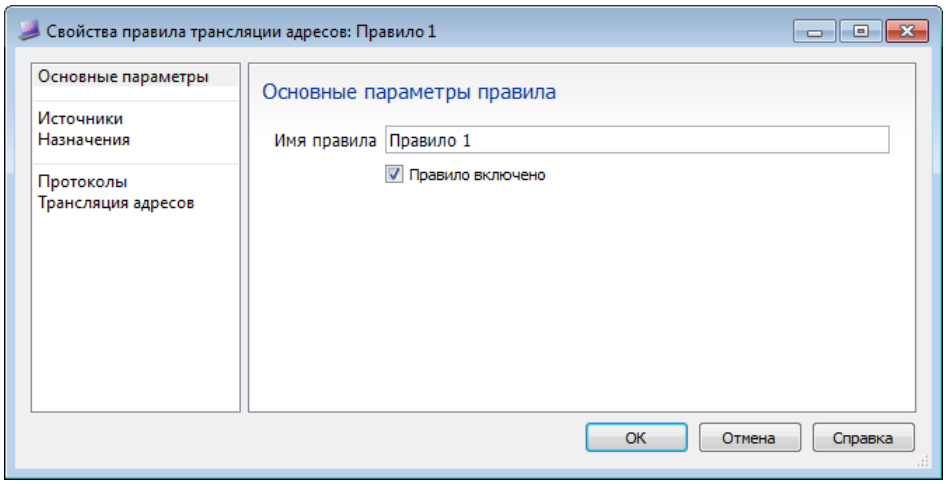


Рисунок 94: Задание имени правила трансляции IP-адресов

4. В разделе **Источники** определите отправителя IP-пакетов, для которых требуется выполнять трансляцию адресов. Для этого добавьте:
   - IP-адрес отправителя либо диапазон адресов, если их несколько. См. раздел Добавление IP-адресов и DNS-имен (на стр. 172).
   - Группу IP-адресов отправителей, если такие созданы (см. «Создание и изменение групп объектов» на стр. 166).

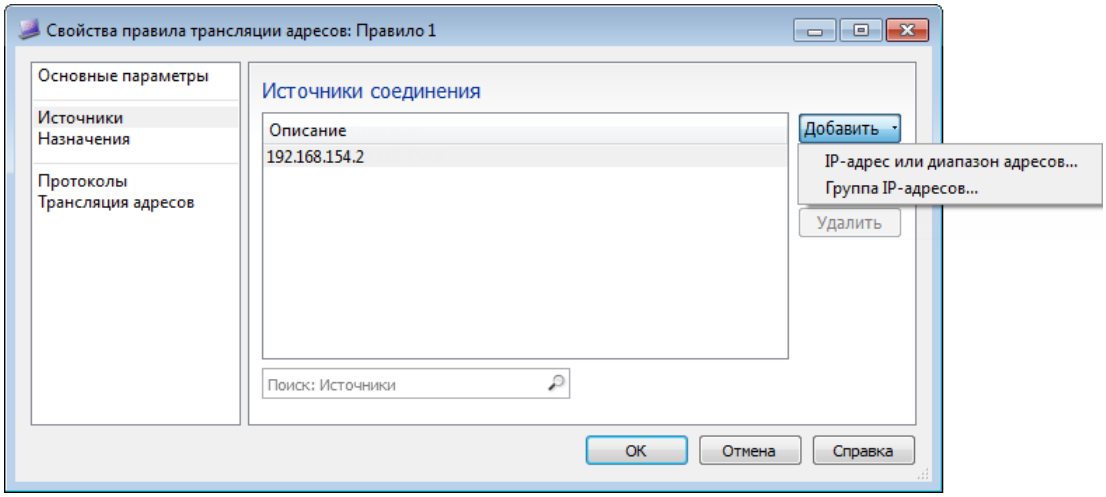


Рисунок 95: Указание отправителя IP-пакетов

5 В разделе **Назначения** определите получателя IP-пакетов, для которых требуется выполнять трансляцию адресов. Добавление получателя производится также как и добавление отправителя (см. предыдущий пункт).

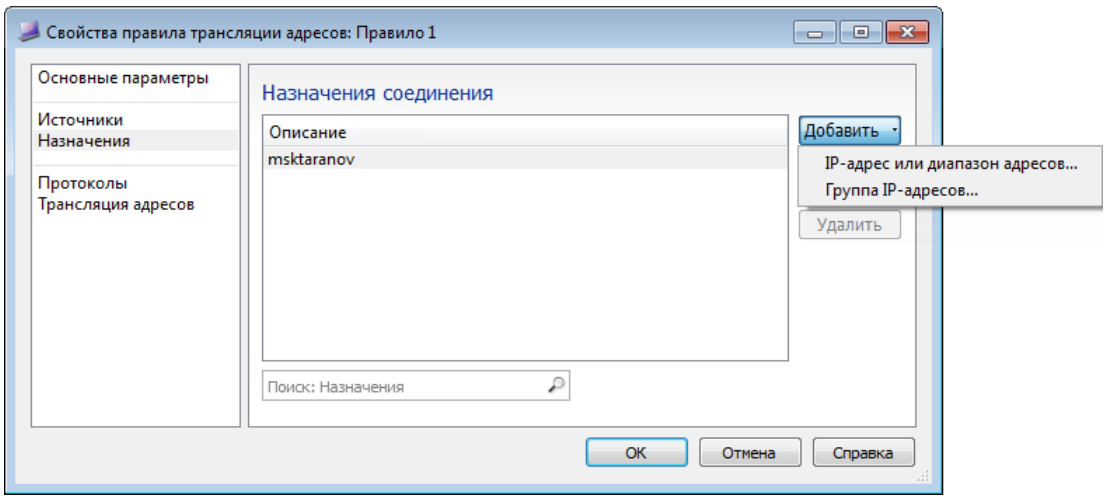


Рисунок 96: Указание получателя IP-пакетов

6 В разделе **Протоколы** укажите протокол для трансляции. Преобразованию будут подвергаться только IP-пакеты, переданные с помощью указанного протокола. Вы можете добавить нужные протоколы (см. «Добавление протоколов» на стр. 173) или группы протоколов, если такие созданы (см. «Создание и изменение групп объектов» на стр. 166).

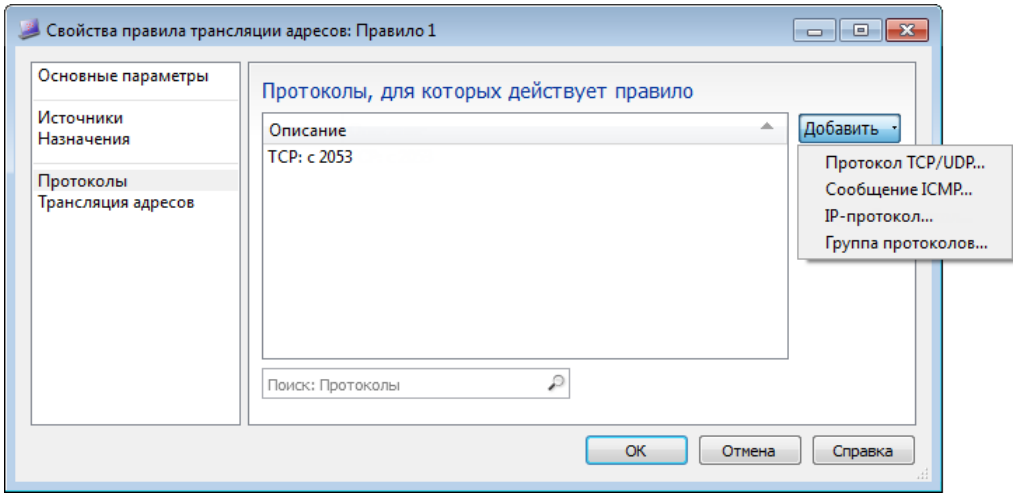


Рисунок 97: Добавление протокола при создании правила трансляции

7 В разделе **Трансляция адресов** задайте параметры трансляции IP-адресов источника и назначения.

При необходимости преобразования IP-адреса источника для исходящих IP-пакетов (см. «Трансляция адреса источника» на стр. 210):

- В группе **Трансляция источника** установите флажок **Заменять адрес источника на**.
- Выберите **Адрес исходящего интерфейса (определяется автоматически)**, чтобы IP-адрес отправителя заменялся на IP-адрес внешнего интерфейса координатора, который определяется автоматически.
- Если необходимо задать другой IP-адрес, на который будет заменяться IP-адрес источника отправляемых IP-пакетов, выберите **Другой адрес** и в поле справа от флажка введите IP-адрес.

При необходимости преобразования IP-адреса узла назначения для входящих IP-пакетов (см. «Трансляция адреса назначения» на стр. 209):

- В группе параметров **Трансляция назначения** установите флажок **Заменять адрес назначения на** и в поле справа от флажка введите локальный IP-адрес узла назначения, который будет присваиваться полученным на координаторе IP-пакетам.
- Если необходимо изменять порт, установите флажок **Заменять порт назначения на** и выберите из списка порт, который будет присваиваться полученным на координаторе IP-пакетам. Замена порта назначения будет происходить только для протоколов TCP и UDP.

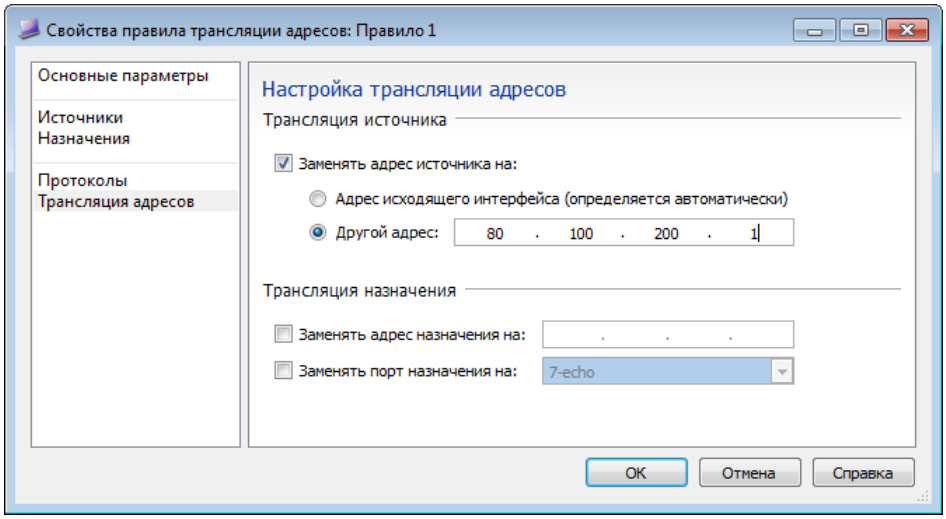


Рисунок 98: Настройка параметров трансляции

8 Для сохранения параметров нового правила нажмите кнопку **ОК**. В результате в списке на панели просмотра появится новое правило.

Созданное правило будет включено, если при задании его основных параметров не был снят соответствующий флажок. Если потребуется отключить правило, снимите флажок слева от его имени.

9 Задайте приоритет созданного правила, установив его положение в списке с помощью кнопок и .

10 Чтобы созданное правило вступило в действие, по завершении всех операций с ним нажмите кнопку **Применить** и в появившемся окне в течение 30 секунд подтвердите сохранение изменений.

Пример использования правил трансляции IP-адресов приведен в разделе Организация DMZ (на стр. 239).

12

Защита трафика открытых узлов (туннелирование)

Общие сведения

Нередко возникает задача защитить обмен данными между узлами на потенциально опасном участке сети или включить узел в сеть ViPNet, при этом ПО ViPNet на некоторые узлы не может быть установлено. Такая ситуация возможна, если узлы сети представляют собой специализированные устройства (например, IP-АТС или аппаратные IP-телефоны) или серверы (SQL, 1С, DHCP), установка дополнительного ПО на которые нежелательна.

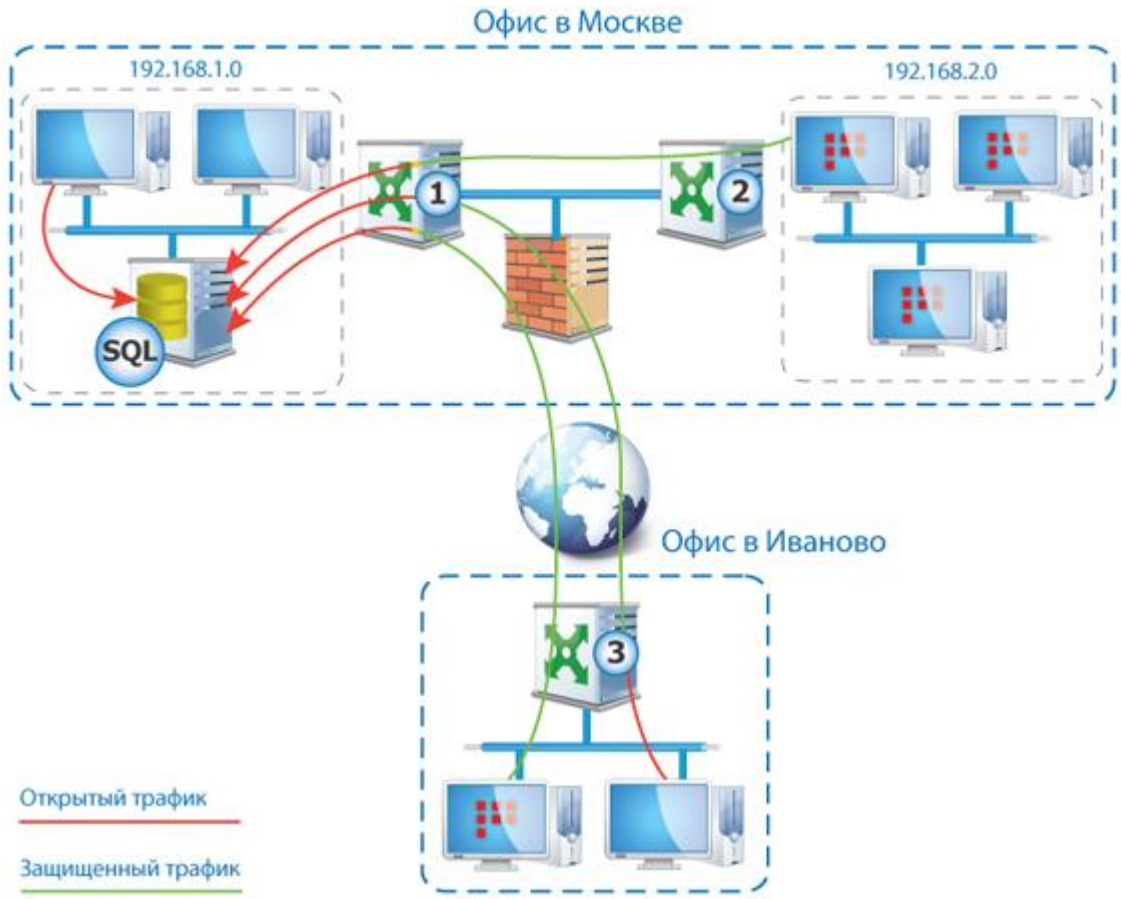


Рисунок 99: Схема защищенного доступа к серверу

В таких случаях используется технология туннелирования. Данная технология предполагает направление трафика узла не напрямую на другой узел, а через ViPNet Coordinator, где трафик фильтруется и защищается криптографическими методами.

В данном разделе рассматривается настройка туннелирования открытых узлов координатором. Для организации доступа к узлам, которые уже туннелируются другим координатором, см. раздел Настройка доступа к узлам, туннелируемым другим координатором (на стр. 129).

Защита трафика при туннелировании

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 по цепочке назначения в зашифрованном виде.
- На координаторе, туннелирующем узел получателя, трафик расшифровывается и передается на узел в открытом виде.

Рисунок 100: Виды туннелей в сети ViPNet

В терминологии ViPNet маршрут трафика от узла «1» до узла «2» называют полутуннелем, а маршрут трафика от узла «1» к узлу «3» — полным туннелем.

Настройка туннелирования

Для настройки туннелирования открытых узлов координатором выполните следующие действия:

1. В программе ViPNet Центр управления сетью или ViPNet Network Manager укажите для этого координатора максимальное допустимое число одновременно туннелируемых соединений.
2. Задайте IP-адреса открытых узлов, которые будут туннелироваться.
3. Создайте сетевые фильтры, если требуется ограничить доступ к туннелируемым узлам. Фильтры можно настроить непосредственно на координаторе (см. «Создание фильтров для туннелируемых узлов» на стр. 182) или отправить на координатор в соответствующей политике безопасности из программы ViPNet Policy Manager (см. «Обновление справочников, ключей и политик безопасности» на стр. 70).

Существует два способа задания узлов для туннелирования:

- В программе ViPNet Центр управления сетью или ViPNet Network Manager. В этом случае после рассылки новых справочников адреса туннелируемых узлов будут переданы и на туннелирующий координатор, и на все клиенты, связанные с этим координатором.

  Первый способ удобен тем, что позволяет задавать адреса для туннелирования централизованно. Мы рекомендуем пользоваться именно этим способом. Второй способ можно применить, когда доступ к туннелируемым адресам нужно организовать для небольшого числа клиентов.

- В программе ViPNet Монитор. В этом случае адреса туннелируемых узлов необходимо задать на туннелирующем координаторе (см. «Задание узлов для туннелирования» на стр. 221) и на каждом сетевом узле, который должен иметь доступ к туннелируемым узлам (см. «Настройка доступа к узлам, туннелируемым другим координатором» на стр. 129). Те узлы ViPNet, на которых не были указаны туннелируемые адреса, не будут иметь доступа к туннелируемым узлам.

Внимание! Необходимо выбрать один из способов задания туннелируемых узлов и придерживаться его при изменении конфигурации сети, так как задание адресов в программе ViPNet Центр управления сетью или ViPNet Network Manager перекрывает все настройки, сделанные ранее на координаторах и клиентах.

Задание узлов для туннелирования

Чтобы задать IP-адреса открытых узлов для туннелирования, на туннелирующем координаторе выполните следующие действия:

1 В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 В окне **Настройка** выберите раздел **Туннелирование**.

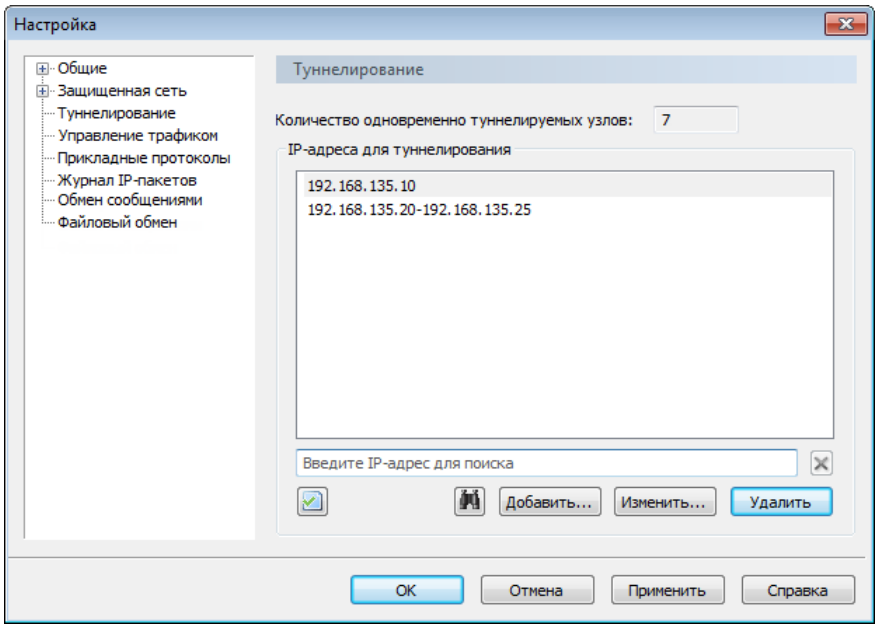


Рисунок 101: Добавление IP-адресов для туннелирования в ViPNet Coordinator

3 С помощью соответствующих кнопок сформируйте список IP-адресов туннелируемых узлов.

Примечание. Если в поле **Количество одновременно туннелируемых узлов** указано значение 0, изменение списка туннелируемых адресов будет невозможно. Задать количество одновременно туннелируемых адресов для координатора можно в программе ViPNet Центр управления сетью или ViPNet Network Manager.

Если вам не известен IP-адрес туннелируемого узла, то вы можете определить его по имени компьютера. Для этого нажмите кнопку  и в появившемся окне выполните поиск IP-адреса по указанному имени.

При добавлении IP-адреса будет автоматически выполнена его проверка на пересечение с IP-адресами, уже заданными в списке, и IP-адресами других сетевых узлов. Данная проверка позволит исключить возможность задания одинаковых IP-адресов. Если в ходе проверки будет обнаружено пересечение IP-адресов, появится соответствующее сообщение. Устраните пересечение IP-адресов (см. «Обнаружен конфликт IP-адресов» на стр. 375).

Вы также можете выполнить проверку на пересечение IP-адресов вручную. Для этого нажмите кнопку  .

4 По завершении всех действий нажмите кнопку **OK**.

После указания IP-адресов для туннелирования на координаторе вы можете создать сетевые фильтры, ограничивающие доступ к туннелируемым узлам координатора по определенным параметрам. Кроме того, чтобы пользователи других узлов сети ViPNet могли получить доступ к туннелируемым узлам данного координатора, необходимо указать IP-адреса этих узлов на каждом сетевом узле. Подробнее о настройке доступа на клиенте см. документ «ViPNet Client Монитор. Руководство пользователя», раздел «Настройка доступа к туннелируемым узлам».

Необходимые настройки на туннелируемых узлах

Примечание. При планировании сети необходимо учитывать, что туннелируемые узлы (без ПО ViPNet, но с защищенным доступом) рекомендуется размещать за отдельным интерфейсом координатора или за отдельным координатором. Это необходимо по соображениям безопасности, а также для удобства управления сетью ViPNet.

Чтобы обеспечить правильную маршрутизацию трафика между туннелируемыми узлами и защищенными узлами ViPNet, необходимо выполнение следующих условий:

- Туннелируемые узлы должны находиться в одной маршрутизируемой сети с туннелирующим координатором.
- IP-пакеты, отправляемые с туннелируемых узлов на защищенные узлы ViPNet, требуется направлять через туннелирующий координатор. Для этого выполните одно из действий:
  - На туннелируемых узлах в качестве шлюза по умолчанию укажите туннелирующий координатор.
  - На туннелируемых узлах задайте статические маршруты для защищенных узлов ViPNet через туннелирующий координатор.

Настройка доступа к туннелируемым узлам из внешней сети

С помощью технологий ViPNet можно легко решить распространенную задачу защищенного доступа к туннелируемым узлам для компьютеров из внешней сети.

Внимание! Описанная технология распространяется только на инициативные соединения от узлов внешней сети к туннелируемым серверам. Таким образом, для инициативного соединения от туннелируемого узла к узлам внешней сети данный способ организации связи не применим.

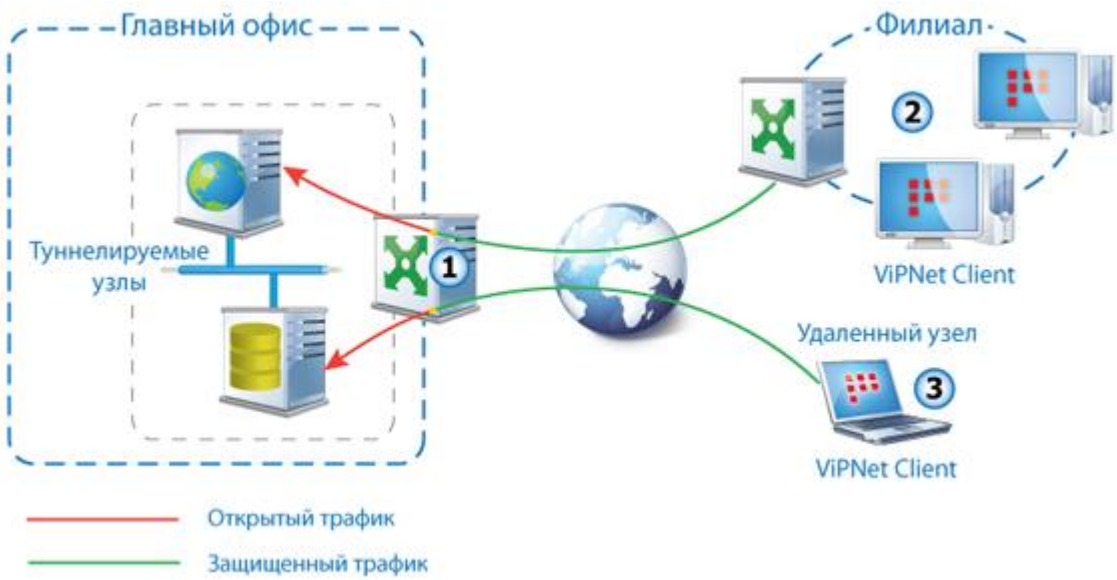


Рисунок 102: Доступ к туннелируемым узлам из внешней сети

Допустим, требуется обеспечить доступ сотрудников филиала и удаленных пользователей к туннелируемым серверам, находящимся в главном офисе компании. При организации доступа из внешней сети к туннелируемым узлам возникает проблема создания большого количества правил маршрутизации трафика для адресов видимости удаленных узлов на участке сети между координатором и туннелируемыми узлами. Для решения этой проблемы следует настроить правило трансляции IP-адреса источника из внешней сети на адрес туннелирующего координатора. Согласно приведенной схеме, для доступа к туннелируемым узлам необходимо создать правило трансляции IP-адреса

источника для узлов (см. «Трансляция адреса назначения» на стр. 209) 2 и 3 на адрес внутреннего интерфейса координатора 1.

Чтобы настроить правила трансляции IP-адреса источника, выполните следующие действия:

1. На координаторе **1** в программе ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Трансляция адресов**.
2. На панели просмотра нажмите кнопку **Создать.**
3. В окне свойств правила трансляции адресов в разделе **Источники** укажите адреса или диапазоны адресов видимости (см. «Адреса видимости» на стр. 482) узлов **2** и **3.**
4. В разделе **Трансляция адресов** установите флажок **Заменять адрес источника на**, затем установите переключатель в положение **Другой адрес** и укажите IP-адрес внутреннего сетевого интерфейса координатора, который находится со стороны туннелируемого узла.
5. Нажмите кнопку **OK**.

После настройки правила трансляции источника удостоверьтесь в том, что для удаленных узлов теперь обеспечен доступ к туннелируемым узлам.

13

Настройка сервера открытого Интернета

Технология доступа «Открытый Интернет»

Для организации доступа к Интернету с высоким уровнем защиты рекомендуется использовать технологию «Открытый Интернет». Данная технология позволяет произвести отключение компьютера сотрудника от корпоративной сети и предоставляет ему безопасный доступ к ресурсам сети Интернет.

Реализация технологии «Открытый Интернет» состоит в следующем: в сети выделяется виртуальный изолированный сегмент, который будет связан как с координатором с функцией «Открытый Интернет», так и с другими узлами локальной сети. Доступ в Интернет регулирует прокси-сервер, который может находиться как на сервере открытого Интернета, так и на выделенном компьютере.

Внимание! Для обеспечения безопасности вашей сети не рекомендуется размещать прокси-сервер на одном компьютере с координатором открытого Интернета. Более безопасной является конфигурация, в которой прокси-сервер расположен на открытом узле и туннелируется координатором открытого Интернета.

Рисунок 103: Технология «Открытый интернет» с выделенным прокси-сервером

Клиенты ViPNet, связанные с сервером открытого Интернета, могут работать только в одном из двух режимов:

- Работа в Интернете. Для подключения к Интернету в программе ViPNet Монитор на клиенте следует выбрать конфигурацию «Открытый Интернет». В этом режиме заблокированы соединения со всеми защищенными узлами, кроме координатора открытого Интернета.

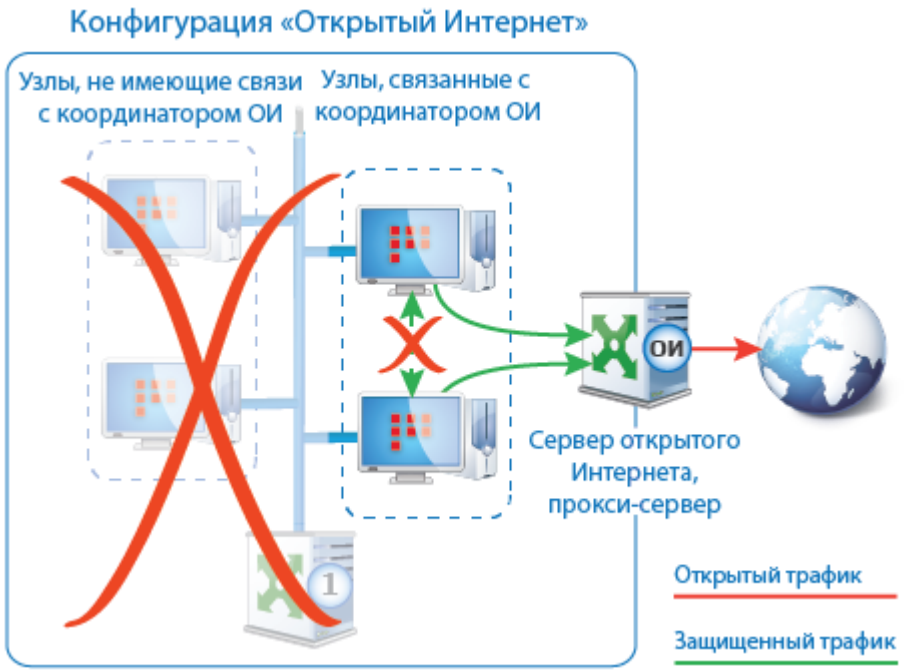


Рисунок 104: Схема работы в режиме «Открытый Интернет»

- Работа с узлами защищенной сети. Для подключения к защищенной сети в программе ViPNet Монитор на клиенте следует выбрать любую конфигурацию, кроме конфигурации «Открытый Интернет». В этом режиме соединения с координатором открытого Интернета заблокированы, доступ в Интернет невозможен.

Рисунок 105: Схема работы с ресурсами локальной сети

Использование технологии «Открытый Интернет» позволяет решить сразу несколько задач:

- предоставление сотрудникам безопасного и удобного доступа в сеть Интернет с рабочих мест без дополнительных трудозатрат;
- отсутствие затрат на создание и обслуживание специальной выделенной сети, посредством которой сотрудники учреждения получают доступ в сеть Интернет.

Порядок настройки схемы «Открытый Интернет»

Для организации защищенного доступа в Интернет по технологии «Открытый интернет» выполните следующие действия:

1. Установите на выделенный сервер программное обеспечение ViPNet Coordinator.
2. Установите на сервере дистрибутив ключей координатора, для которого включена функция сервера открытого Интернета.
3. На том же сервере, где установлено ПО ViPNet Coordinator, или на выделенном сервере установите ПО, выполняющее функции прокси-сервера прикладного уровня.

Внимание! ПО ViPNet может некорректно работать на одном компьютере с прокси-серверами прикладного уровня, которые также осуществляют преобразование сетевых адресов (NAT) и имеют функции межсетевого экрана. Это происходит из-за того, что ViPNet Coordinator может выполнять преобразование сетевых адресов (NAT) и быть межсетевым экраном.

Если на одном компьютере с координатором установлено программное обеспечение, выполняющее функции прокси-сервера, необходимо в этом программном обеспечении отключить службы NAT и межсетевого экрана.

Например, при установке программного обеспечения WinGate на один компьютер с ViPNet Coordinator не рекомендуется устанавливать ENS-драйвер (Extended Network Services driver), обеспечивающий в WinGate работу NAT, маршрутизации и межсетевого экрана.

4. Выполните на прокси-сервере необходимые настройки для доступа клиентов в Интернет.
5. Если прокси-сервер расположен на отдельном компьютере, добавьте его в список туннелируемых узлов координатора открытого Интернета (см. «Настройка туннелирования» на стр. 220).
6. Настройте на координаторе набор сетевых фильтров, обеспечивающих безопасный доступ клиентов в Интернет (см. «Настройка координатора открытого Интернета» на стр. 231).

7 Выполните настройку клиентов, которым разрешен доступ в Интернет (см. документ «ViPNet Client Монитор. Руководство пользователя»).

Внимание! Координатор открытого Интернета должен иметь связи только с теми узлами сети ViPNet, которым разрешен доступ в Интернет. Связи сетевых узлов задает администратор сети ViPNet в программе ViPNet Центр управления сетью.

Настройка координатора открытого Интернета

На координаторе, работающем в качестве сервера открытого Интернета, необходимо настроить сетевые фильтры, обеспечивающие безопасный доступ клиентов в Интернет. Для этого рекомендуется удалить все настроенные на координаторе сетевые фильтры и заново создать фильтры, перечисленные ниже (см. «Создание сетевых фильтров» на стр. 178). Кроме того, нужные фильтры могут быть отправлены на координатор в составе соответствующей политики из программы ViPNet Policy Manager (см. «Обновление справочников, ключей и политик безопасности» на стр. 70).

На сервере открытого Интернета настройте следующие сетевые фильтры:

- Если прокси-сервер установлен непосредственно на координаторе, создайте следующие сетевые фильтры, расположив их в порядке, который указан в таблице.

  Таблица 6. Сетевые фильтры для случая, когда прокси-сервер установлен на координаторе

Описание фильтра	Источник	Назначение	Протоколы	Действие
В разделе **Фильтры защищенной сети**				
Разрешить служебный трафик ViPNet	Все	Все	UDP: с 2046 на 2046 TCP: 5000-5002 TCP: с 2047 на 2047; ICMP 8	Пропускать
Разрешить входящие соединения с прокси-сервером	Другие узлы	Все	TCP: <порт подключения к прокси-серверу>	Пропускать
Блокировать другие защищенные соединения	Все	Все	Все	Блокировать
В разделе **Локальные фильтры открытой сети**				
Блокировать открытые соединения со стороны внутренней сети	<внутренний интерфейс>:Все	Все	Все	Блокировать

Описание фильтра	Источник	Назначение	Протоколы	Действие
Разрешить DHCP-трафик	Все	Все	DHCP	Пропускать
Разрешить NetBIOS- и WINS-трафик	Все	Все	NetBIOS-DGM и NetBIOS-NC	Пропускать
Разрешить исходящие соединения с узлами в Интернете	<внешний интерфейс>:Мой узел	Все	Все	Пропускать
В разделе **Транзитные фильтры открытой сети**				
Блокировать транзитные соединения	Все	Все	Все	Блокировать

- Если прокси-сервер установлен на отдельном компьютере и туннелируется координатором, создайте следующие сетевые фильтры, расположив их в порядке, который указан в таблице.

Таблица 7. Сетевые фильтры для случая, когда прокси-сервер установлен на отдельном компьютере

Описание фильтра	Источник	Назначение	Протоколы	Действие
В разделе **Фильтры защищенной сети**				
Разрешить служебный трафик ViPNet	Все	Все	UDP: с 2046 на 2046 TCP: 5000-5002 TCP: с 2047 на 2047; ICMP 8	Пропускать
Блокировать другие защищенные соединения	Все	Все	Все	Блокировать
В разделе **Локальные фильтры открытой сети**				
Блокировать открытые соединения со стороны внутренней сети	<внутренний интерфейс>:Все	Все	Все	Блокировать
Разрешить DHCP-трафик	Все	Все	DHCP	Пропускать

Описание фильтра	Источник	Назначение	Протоколы	Действие
Разрешить NetBIOS- и WINS-трафик	Все	Все	NetBIOS-DGM и NetBIOS-NC	Пропускать
В разделе **Фильтры для туннелируемых узлов**				
Разрешить соединения клиентов с прокси-сервером	<клиенты>	<прокси-сервер>	Все	Пропускать

Примечание. В данном разделе внутренним интерфейсом называется сетевой интерфейс координатора, со стороны которого находится локальная сеть с клиентами. Внешним интерфейсом называется сетевой интерфейс, со стороны которого находится Интернет.

14

Практические сценарии использования координатора

Использование DHCP-сервера в сети ViPNet

Варианты размещения DHCP-сервера

Протокол DHCP позволяет компьютерам автоматически получать от сервера IP-адреса и другие параметры, необходимые для работы в сети.

При использовании DHCP-сервера защищенными узлами в сети ViPNet возможны следующие варианты:

- DHCP-сервер и защищенные узлы могут находиться:
  - В одной подсети.
  - В разных подсетях, разделенных межсетевым экраном. Предположим, что в качестве межсетевого экрана используется координатор. В этом случае на координаторе требуется выполнить дополнительные настройки (см. «Размещение DHCP-сервера и клиентов в разных подсетях» на стр. 237).
- DHCP-сервер может быть:
  - Защищенным узлом (с программным обеспечением ViPNet Client или ViPNet Coordinator).
  - Туннелируемым узлом (см. «Защита трафика открытых узлов (туннелирование)» на стр. 217).
  - Открытым узлом.

При любом из перечисленных вариантов размещения DHCP-сервера защищенные узлы ViPNet могут использовать его для автоматического получения сетевых параметров.

Чтобы обеспечить соединение между защищенными узлами и DHCP-сервером, убедитесь в том, что на координаторе (в программе ViPNet Coordinator) и на клиентах (в программе ViPNet Client) выполнены необходимые настройки, а именно:

- В разделе **Фильтры защищенной сети** должен быть включен фильтр, разрешающий DHCP-трафик.

- В разделе **Локальные фильтры открытой сети** должен быть включен фильтр, разрешающий DHCP-трафик.
- Если защищенные узлы и DHCP-сервер находятся в разных подсетях, на координаторе, который играет роль межсетевого экрана, необходимо выполнить дополнительные настройки.

Рисунок 106: Транзитный DHCP-сервер

  - В разделе **Транзитные фильтры открытой сети** создайте фильтр со следующими параметрами:

Таблица 8. Транзитный фильтр для DHCP-сервера

Описание	Источник	Назначение	Протоколы	Действие
Разрешить DHCP-трафик	Все	Все	UDP: с 67 на 68 UDP: с 68 на 67	Пропускать

  - На координаторе требуется произвести системные настройки ОС Windows, обеспечивающие передачу сообщений DHCP между двумя сетями (см. «Размещение DHCP-сервера и клиентов в разных подсетях» на стр. 237). Данные настройки не затрагивают ПО ViPNet.
- Если DHCP-сервер туннелируется координатором, должны быть включены фильтры, разрешающие соединения между защищенными узлами и туннелируемыми узлами.

Рисунок 107: Туннелируемый DHCP-сервер

Размещение DHCP-сервера и клиентов в разных подсетях

Если DHCP-сервер и ViPNet-клиенты находятся в разных подсетях:

1 При необходимости туннелирования DHCP-сервера задайте для туннелирования IP-адрес DHCP-сервера.

Примечание. Туннелирование DHCP-сервера позволяет клиентам, получающим от этого сервера IP-адреса, взаимодействовать с ним по защищенному каналу.

2 Установите и настройте на координаторе агент DHCP-ретрансляции (DHCP Relay Agent).

Информацию о настройке агента DHCP-ретрансляции можно найти на сайте Microsoft http://technet.microsoft.com/ru-ru/library/cc781416(WS.10).aspx.

Внимание! Агент DHCP-ретрансляции используется в операционных системах Windows Server 2003 и Windows Server 2008.

Для того чтобы развернуть агент DHCP-ретрансляции, выполните на координаторе средствами ОС Windows следующее:

1 Запустите службу маршрутизации и удаленного доступа (RRAS, Routing and Remote Access Service).

2 Установите агент DHCP-ретрансляции.

3 Настройте агент DHCP-ретрансляции.

Организация DMZ

Назначение схемы DMZ

Простая схема DMZ (см. «DMZ (демилитаризованная зона)» на стр. 480) с одним межсетевым экраном подразумевает разделение сети на два сегмента:

- **Защищенный** — для узлов в данном сегменте разрешены исходящие соединения с узлами в Интернете и в сегменте DMZ, но запрещены входящие соединения из Интернета и из сегмента DMZ.
- **DMZ** — для узлов данного сегмента разрешены как исходящие, так и входящие соединения с узлами в Интернете. Со стороны защищенного сегмента разрешены только входящие соединения. Как правило, в этом сегменте располагаются серверы и сервисы, которые должны быть доступны внешним пользователям (из сети Интернет).

Разбиение сети на два сегмента позволяет ограничить доступ из внешней сети во внутреннюю к тем узлам, которые не являются публичными серверами, и таким образом повысить уровень защиты локальной сети.

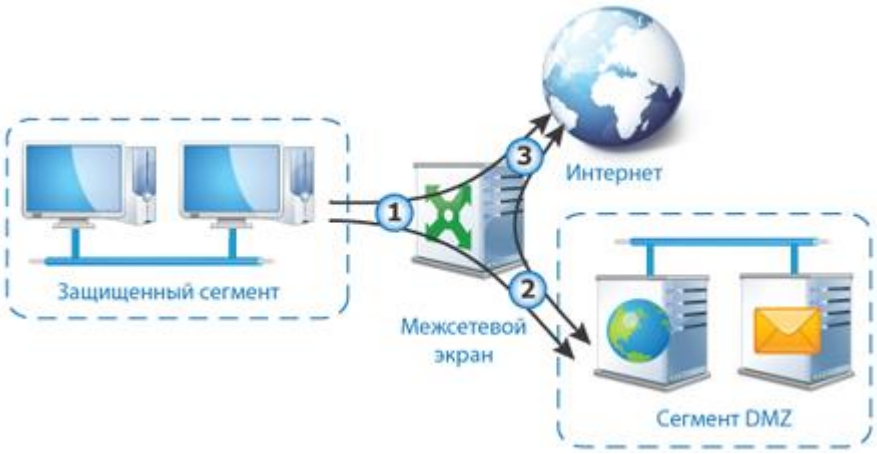


Рисунок 108: Движение трафика в схеме DMZ

На рисунке представлена схема организации DMZ. Координатор на схеме играет роль межсетевого экрана (дополнительно — NAT) и имеет как минимум три сетевых интерфейса:

1. Локальный, подключен к защищенному сегменту сети.
2. Локальный, подключен к сегменту DMZ.
3. Внешний (один или несколько), подключен к Интернету.

Исходящие соединения в данной схеме могут быть установлены в следующих направлениях:

-  от защищенного сегмента к сегменту DMZ.
-  от защищенного сегмента в Интернет.
-  из Интернета в сегмент DMZ и в обратную сторону.

Подобное разделение сети и ограничение движения трафика позволяют организовать внешний доступ к публичным серверам и сервисам, при этом обезопасив остальную локальную сеть от внешних вторжений. Даже если злоумышленник сможет получить контроль над сегментом DMZ, доступ из него в другой сегмент локальной сети для него будет невозможен.

Настройка ViPNet Coordinator

Настройка ПО ViPNet Coordinator в качестве межсетевого экрана, стоящего на границе DMZ, включает:

- Создание транзитных фильтров по всем разрешенным направлениям движения трафика.
- Создание правил трансляции IP-адресов для организации доступа узлов локальной сети в Интернет и доступа внешних узлов к публичному сегменту.

Настройка транзитных фильтров

Чтобы настроить сетевые фильтры, разрешающие передачу трафика между сегментами локальной сети и Интернетом в заданных направлениях, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Транзитные фильтры открытой сети**.
2. На панели просмотра создайте следующие сетевые фильтры (см. «Создание сетевых фильтров» на стр. 178):
   - Фильтр, разрешающий исходящие соединения из защищенного сегмента в сегмент DMZ.
   - Фильтр, разрешающий исходящие соединения из защищенного сегмента в Интернет.
   - Фильтр, разрешающий соединения из сегмента DMZ в Интернет, и фильтр, разрешающий соединения в обратном направлении.

   Параметры транзитных фильтров, которые требуется создать, приведены в следующей таблице. Номера сетевых интерфейсов в таблице указаны в соответствии с приведенной выше схемой (см. Рисунок 108 на стр. 239).

Таблица 9. Транзитные фильтры для организации DMZ

Описание фильтра	Источник	Назначение	Протоколы	Действие
Разрешить соединения из защищенного сегмента в DMZ	<внутренний интерфейс (1)>	<адреса сегмента DMZ>	<протоколы взаимодействия с серверами в DMZ>	Пропускать
Разрешить соединения из защищенного сегмента в Интернет	<внутренний интерфейс (1)>	<внешний интерфейс (3)>	TCP: 80, TCP: 443 и так далее	Пропускать
Разрешить соединения из DMZ в Интернет	<адреса сегмента DMZ>	<внешний интерфейс (3)>	TCP: 80, TCP: 443 и так далее	Пропускать
Разрешить соединения из Интернета в DMZ	<внешний интерфейс (3)>	<адреса сегмента DMZ>	<протоколы взаимодействия с серверами в DMZ>	Пропускать

Совет. В случае необходимости вы можете настроить расписание действия фильтров. Например, разрешить сотрудникам выход в Интернет с 9 до 18 часов по рабочим дням.

Настройка правил трансляции адресов

Чтобы организовать доступ в Интернет для узлов локальной сети и доступ к сегменту DMZ из Интернета, на координаторе требуется создать правила трансляции адресов (см. «Трансляция сетевых адресов (NAT)» на стр. 206). Для этого выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Сетевые фильтры** > **Трансляция адресов**.
2. В разделе **Трансляция адресов** создайте правило трансляции адреса источника (см. «Трансляция адреса источника» на стр. 210), обеспечивающее доступ локальных узлов в Интернет. В окне **Свойства правила трансляции адресов** задайте следующие параметры:
   - В разделе **Назначения** укажите множество публичных IP-адресов (см. «Публичный адрес» на стр. 489), выбрав группу IP-адресов **Публичные IP-адреса**. Данная группа в программе ViPNet Монитор настроена по умолчанию (см. «Пользовательские группы объектов, настроенные по умолчанию» на стр. 166).
   - В разделе **Трансляция адресов** установите флажок **Заменять адрес источника на** и установите переключатель в положение **Адрес исходящего интерфейса (определяется автоматически)**.
   - В разделах **Источники** и **Протоколы** настройка параметров не требуется.
3. Создайте правила трансляции адреса назначения (см. «Трансляция адреса назначения» на стр. 209), обеспечивающие доступ внешних узлов к серверам в сегменте DMZ. Для каждого сервера настройте отдельное правило, задав в окне **Свойства правила трансляции адресов** следующие параметры:
   - В разделе **Источники** укажите множество публичных IP-адресов, выбрав группу IP-адресов **Публичные IP-адреса**. Данная группа в программе ViPNet Монитор настроена по умолчанию.
   - В разделе **Назначения** укажите внешний IP-адрес координатора, который будет принимать запросы к серверам, расположенным в сегменте DMZ.
   - В разделе **Протоколы** укажите протоколы и порты доступа к серверу.

- В разделе **Трансляция адресов** установите флажок **Заменять адрес назначения на** и укажите частный адрес сервера в сегменте DMZ, на который требуется перенаправлять запросы.

Протоколы и порты для доступа к различным видам серверов

- Для связи с веб-сервером должны быть разрешены следующие протоколы и порты:
  - TCP 80 (HTTP);
  - TCP 443 (HTTPS).
- Для связи с почтовым сервером должны быть разрешены следующие протоколы и порты:
  - TCP 25 (SMTP) — отправка сообщений;
  - TCP 110 (POP3) — прием сообщений.
- Для связи с FTP-сервером должен быть разрешен протокол TCP 21.

15

Интеграция с программой ViPNet SafeDisk-V

Общие сведения о программе ViPNet SafeDisk-V

Программа ViPNet SafeDisk-V предназначена для защиты конфиденциальной информации, которая хранится на диске или съемном носителе.

Информация, которую требуется защитить, помещается в контейнер SafeDisk-V. Контейнер представляет собой зашифрованный файл. При подключении контейнера в программе ViPNet SafeDisk-V он отображается как логический диск в операционной системе.

Данные, которые записываются в подключенный контейнер, автоматически зашифровываются и также автоматически расшифровываются в процессе чтения. Шифрование осуществляется незаметно для пользователя, не требуя от него никаких дополнительных действий.

При отключении контейнер перестает отображаться в системе, и установить сам факт наличия конфиденциальной информации и получить к ней доступ невозможно.

Доступ к защищенной информации, хранящейся в контейнерах SafeDisk-V, имеет только пользователь программы ViPNet Coordinator. При работе с контейнерами обеспечивается дополнительная защита средствами ViPNet Coordinator.

Программа ViPNet SafeDisk-V, интегрированная с ViPNet Coordinator, имеет по сравнению с обычной программой ViPNet SafeDisk следующие преимущества:

- Доступ к контейнерам имеет только пользователь узла.
- Ключи не надо обновлять самостоятельно.

  При совместной работе ViPNet SafeDisk-V с ViPNet Coordinator обновление ключей контейнера ViPNet SafeDisk-V выполняется при обновлении ключей сетевого узла и ключей пользователя ViPNet. Такая возможность появилась благодаря тому, что при работе ViPNet SafeDisk-V совместно с ViPNet Coordinator ключи контейнера защищены ключами сетевого узла и ключами пользователя сети ViPNet (см. рисунок ниже).

Совет. При работе с контейнерами SafeDisk-V рекомендуется отключать автоматическую установку обновлений (см. «Автоматическая установка обновлений» на стр. 97). Все поступающие обновления в этом случае можно

устанавливать только вручную.

Рисунок 109: Схема иерархии защиты ключа контейнера в ПО ViPNet SafeDisk-V, интегрированного с ViPNet Client

Подробная информация о программе ViPNet SafeDisk-V содержится в документе «ViPNet SafeDisk-V. Руководство пользователя».

Обеспечение интеграции ViPNet Coordinator с ViPNet SafeDisk-V: порядок действий

Внимание! ПО ViPNet Coordinator версий 4.0 и выше может быть интегрировано только с версией ViPNet SafeDisk-V 4.2.

Для того чтобы использовать программу ViPNet SafeDisk-V совместно с программой ViPNet Coordinator, необходимо выполнить действия из приведенного ниже списка.

Таблица 10. Порядок действий при интеграции ПО ViPNet Coordinator с ViPNet SafeDisk-V

	Действие	Ссылка
☐	Администратору сети ViPNet следует: • В сети ViPNet CUSTOM — в программе ViPNet Центр управления сетью добавить на сетевой узел роль «SafeDisk». • В сети ViPNet VPN — в программе ViPNet Network Manager выбрать сетевой узел и на вкладке **Ключи** установить флажок **Использовать SafeDisk-V**.	«ViPNet Administrator Центр управления сетью. Руководство администратора» «ViPNet VPN. Руководство пользователя»
☐	Администратору сети ViPNet следует: • В сети ViPNet CUSTOM — при создании нового сетевого узла в программе ViPNet Удостоверяющий и ключевой центр сформировать дистрибутив ключей и установить его на узле. Для созданного ранее сетевого узла в программе ViPNet Центр управления сетью сформировать справочники и отправить их на узел. • В сети ViPNet VPN — в программе ViPNet Network Manager отправить на сетевой узел ключи или сохранить ключи в файл и установить их на узле вручную.	«ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора» «ViPNet Administrator Центр управления сетью. Руководство администратора» «ViPNet VPN. Руководство пользователя»

	Действие	Ссылка
☐	Пользователю, обладающему правами администратора в ОС Windows, следует установить на сетевой узел программу ViPNet SafeDisk-V.	«ViPNet SafeDisk-V. Руководство пользователя»
☐	Ознакомиться с принципом взаимодействия программ ViPNet Coordinator и ViPNet SafeDisk-V.	Работа с интегрированной программой ViPNet SafeDisk-V
☐	Удостовериться, что в программе ViPNet Coordinator включена защита IP-трафика. При отключенной защите IP-трафика программа ViPNet SafeDisk-V не может быть запущена.	Отключение защиты трафика (на стр. 196)

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

Работа с интегрированной программой ViPNet SafeDisk-V

Если выполнены все условия совместной работы программы ViPNet Coordinator и ViPNet SafeDisk-V:

- Запустите программу ViPNet Монитор, после чего запустите программу ViPNet SafeDisk-V.

  Если программа ViPNet Монитор не будет запущена либо в программе будет отключена защита IP-трафика, то появится соответствующее сообщение и запустить программу ViPNet SafeDisk-V вы не сможете.

- При запуске SafeDisk-V появится окно **ViPNet SafeDisk-V**, в котором вы сможете задать параметры защиты трафика в программе ViPNet Coordinator. В результате в программе ViPNet Coordinator будут добавлены соответствующие сетевые фильтры, которые будут действовать только во время работы программы ViPNet SafeDisk-V.

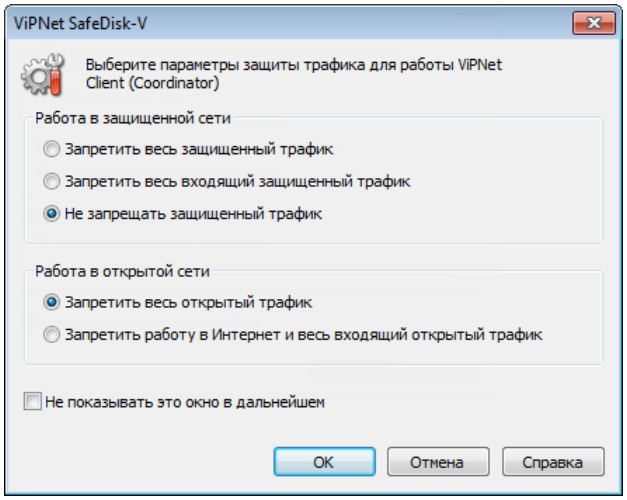


Рисунок 110: Настройка параметров защиты трафика для работы ViPNet Coordinator

Данные параметры невозможно изменить в программе ViPNet Монитор, что обеспечивает дополнительную защиту от несанкционированного доступа к защищенным контейнерам пользователей как открытой, так и защищенной сети (например, системный администратор или администратор сети ViPNet не смогут получить доступ к контейнеру).

По умолчанию при работе с защищенными контейнерами независимо от настроек ViPNet Coordinator всегда запрещаются любые открытые соединения (в группе **Работа в открытой сети** установлен режим **Запретить весь открытый трафик**). Крайне не рекомендуется изменять настройки работы в открытой сети, установленные по умолчанию, так как даже разрешение только исходящих открытых соединений (установка режима **Запретить работу в Интернет и весь входящий открытый трафик** в группе **Работа в открытой сети**) является потенциально опасным при работе с информацией в защищенных контейнерах.

- После того как в программе ViPNet SafeDisk-V будут заданы параметры защиты трафика, интерфейс ПО ViPNet Монитор будет ограничен (например, работа с сетевыми фильтрами будет невозможна и так далее) и будут заблокированы следующие возможности:
  - возможность входа в программу в режиме администратора;
  - возможность отключения защиты IP-трафика;
  - выход и смена пользователя.

  Также перед фильтрами, заданными в ViPNet Coordinator, автоматически будут установлены запрещающие фильтры в соответствии с настройками в окне SafeDisk-V. Данные фильтры не отображаются в интерфейсе ViPNet Coordinator.

- После завершения программы SafeDisk-V (в том числе при запуске команд **Срочное отключение контейнеров** в режиме **«Опасность»** и **Ликвидировать все контейнеры** в режиме **«Большая опасность»**) в программе ViPNet Coordinator будут выполнены следующие действия:
  - будут выгружены все фильтры, автоматически созданные при запуске SafeDisk-V;
  - программа ViPNet Coordinator продолжит работу с фильтрами конфигурации, в которой находилась до запуска программы ViPNet SafeDisk-V;
  - ограничение на интерфейс будет снято и станут доступными следующие возможности:
    - возможность входа в программу в режиме администратора;
    - возможность отключения защиты IP-трафика;
    - выход и смена пользователя.

16

Встроенные средства коммуникации

Общие сведения

В состав программы ViPNet Монитор входит несколько дополнительных инструментов, предоставляющих возможность быстрого и защищенного обмена информацией:

- Обмен защищенными сообщениями / Защищенная конференция.
- Файловый обмен.
- Вызов внешних приложений.
- Функция «Открыть веб-ресурс сетевого узла».
- Функция «Обзор общих ресурсов сетевого узла».
- Проверка соединения с другим сетевым узлом ViPNet.

Обмен защищенными сообщениями

Пользователи сети ViPNet могут в режиме реального времени обмениваться мгновенными сообщениями с другими пользователями ViPNet или участвовать в конференции с несколькими пользователями:

- Вы можете начать сеанс обмена сообщениями, чтобы отправлять сообщения одному или нескольким пользователям одновременно и получать от них ответы. При этом все участники сеанса будут получать ваши сообщения, но не будут получать ответные сообщения от других пользователей.

  Чтобы начать сеанс обмена сообщениями, в окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть,** затем на панели просмотра выберите один или несколько сетевых узлов. В контекстном меню узлов выберите пункт **Послать сообщение** или на панели инструментов нажмите кнопку **Сообщение**  .

- Вы можете начать конференцию с несколькими пользователями, чтобы все участники сеанса могли получать сообщения от других пользователей и отвечать на них. В этом заключается отличие конференции от сеанса обмена сообщениями.

  Чтобы начать конференцию, в окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**, затем на панели просмотра выберите несколько сетевых узлов. В контекстном меню узлов выберите пункт **Конференция** или на панели инструментов нажмите кнопку **Конференция**  (по умолчанию эта кнопка скрыта).

Пользователь ViPNet может участвовать в нескольких сеансах обмена сообщениями одновременно. Если получено сообщение, которое не относится ни к одному из текущих сеансов, будет открыт новый сеанс обмена сообщениями.

Все сообщения, полученные и отправленные в течение сеанса, записываются в протокол сеанса. Если в рамках сеанса отправить сообщение какому-либо пользователю, его ответ придет в том же сеансе и будет сохранен в том же протоколе. При необходимости вы можете сохранить протокол сеанса как текстовый файл.

Во время сеанса обмена сообщениями вы можете отправлять пользователям файлы и письма.

Примечание. Если на вашем сетевом узле обмен сообщениями недоступен, обратитесь к администратору сети ViPNet с просьбой разрешить обмен сообщениями.

Интерфейс программы обмена защищенными сообщениями

Прием и отправка сообщений выполняются в окне **Оперативный обмен защищенными сообщениями**, которое представлено на следующем рисунке:

Цифрами на рисунке обозначены:

1. Главное меню программы обмена защищенными сообщениями.
2. Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Настроить панель.**
3. Панель **Получатели сообщений**. Содержит список пользователей, участвующих в данном сеансе. После отправки сообщения его статус отображается с помощью следующих символов:
   - О — сообщение отправлено, но еще не доставлено.
   - Д — сообщение доставлено, на экране получателя появилось уведомление о сообщении.
   - Ч — сообщение прочитано получателем.
   - П — сообщение было прочитано, получатель собирается ответить.

   Сообщения пронумерованы в порядке их отправки. Колонки со статусами отправленных сообщений расположены в обратном порядке (начиная с последнего отправленного сообщения). Сообщения отправляются пользователям, рядом с именами которых установлены флажки.
4. Строка поиска, предназначенная для фильтрации списка получателей на панели **Сеансы** и для поиска слов в сообщениях на панели **Протокол сеанса.** В протоколе сеанса все вхождения заданной строки поиска отмечаются желтым фоном.
5. Контекстное меню, вызываемое щелчком правой кнопки мыши по имени получателя. Позволяет проверить соединение с получателем (см. «Проверка соединения с сетевым узлом» на стр. 269).
6. Панель **Сообщение**. Предназначена для ввода новых сообщений.
7. Панель **Протокол сеанса**. На этой панели отображается история сообщений (протокол) текущего сеанса.

8 Панель **Сеансы**. Содержит список открытых сеансов и кнопки перехода между сеансами. Описание колонок на панели **Сеансы** приведено в следующей таблице:

Колонка	Описание
	Статус сеанса: Значки отсутствуют. Сеанс открыт, все сообщения были обработаны. Сеанс открыт, получены новые сообщения. Сеанс закрыт инициатором, однако в сеансе есть непрочитанные сообщения (этот значок отображается, только если сеанс инициирован другим пользователем). Сеанс закрыт инициатором (этот значок отображается, только если сеанс инициирован другим пользователем).
№	Номер сеанса.
Получатели	Список участников сеанса.
Новых	Число новых (необработанных) сообщений. Если новых сообщений нет, это поле пусто.
Не прочитано	Число непрочитанных сообщений. Если непрочитанных сообщений нет, это поле пусто. Если в сеансе есть непрочитанные сообщения, атрибуты этого сеанса выделены полужирным шрифтом.
Время последнего обмена	Дата и время последнего сообщения сеанса.

Под списком открытых сеансов расположены кнопки и , с помощью которых можно перейти к предыдущему или к следующему просмотренному сеансу. В истории переходов между сеансами запоминается 10 последних сеансов, просмотр которых продолжался более 5 секунд.

Отправка сообщений

Для обмена мгновенными сообщениями выполните следующие действия:

1 Если окно **Оперативный обмен защищенными сообщениями** закрыто, чтобы открыть его, в меню программы ViPNet Монитор выберите пункт **Приложения > Обмен сообщениями**. В окне **Оперативный обмен защищенными сообщениями** будут открыты все начатые ранее сеансы обмена сообщениями.

2 Чтобы начать новый сеанс обмена сообщениями или конференцию, в окне **Оперативный обмен защищенными сообщениями** выполните следующие действия:

- В меню **Сеанс** выберите пункт **Новый**, а затем щелкните **Обмен сообщениями** или **Конференция**.
- В окне **Выбор сетевого узла** укажите узлы, с пользователями которых вы хотите начать обмен сообщениями или конференцию. Затем нажмите кнопку **Выбрать**.

Откроется новый сеанс обмена сообщениями. Если вы указали единственный сетевой узел, с которым сеанс обмена сообщениями уже был начат, то вместо нового сеанса откроется существующий сеанс.

Примечание. Чтобы начать новый сеанс обмена сообщениями или конференцию, вы также можете выбрать сетевые узлы в разделе **Защищенная сеть** и выбрать в контекстном меню узлов соответствующий пункт (см. «Обмен защищенными сообщениями» на стр. 253).

---

3 В окне **Оперативный обмен защищенными сообщениями** выберите сеанс, в который вы хотите отправить новые сообщения.

4 На панели **Сообщение** введите текст сообщения.

5 Нажмите кнопку **Отправить** или клавишу **F5**.

Совет. В настройках программы обмена сообщениями можно выбрать, какое действие выполняется по нажатию клавиши **Enter** на панели **Сообщение**: отправка сообщения или переход на новую строку. Для этого в программе ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**, откроется окно **Настройка**. В разделе **Обмен сообщениями** в группе **Назначить горячие клавиши** выберите **Ctrl+Enter: отправка сообщения, Enter: перевод строки** или наоборот.

Прием сообщений

По умолчанию при поступлении новых сообщений в области уведомлений появляется значок, текст сообщения отображается во всплывающем окне над областью уведомлений. Чтобы прочитать новые сообщения, выполните одно из действий:

- Щелкните значок в области уведомлений.

- В окне **Оперативный обмен защищенными сообщениями** на панели инструментов нажмите кнопку **Прочитать** .

Вы можете изменить способ уведомления о новом сообщении. Для этого выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. В окне **Настройка** в разделе **Обмен сообщениями** установите или снимите следующие флажки:
   - **Уведомлять о приходе сообщения полупрозрачным окном**.
   - **Уведомлять о приходе сообщения миганием кнопки на панели задач**.
   - **Уведомлять о приходе сообщения окном поверх всех окон**.
   - **Показывать новые сообщения в отдельном окне**.

     Если флажок **Показывать новые сообщения в отдельном окне** установлен, при получении сообщений откроется окно **Новые сообщения**.

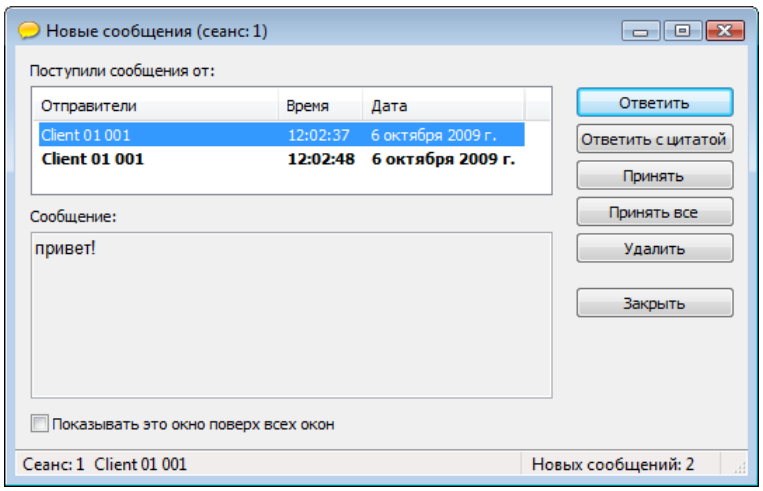


Рисунок 111: Новые сообщения в отдельном окне

В окне **Новые сообщения** отображается список новых сообщений в порядке поступления. С помощью кнопок в правой части окна вы можете принять сообщение (тогда оно будет сохранено в протоколе сеанса), ответить на сообщение или удалить его.

Прекращение обмена сообщениями

Чтобы закрыть сеанс обмена сообщениями:

1. В окне **Оперативный обмен защищенными сообщениями** на панели **Сеансы** выберите сеанс, который требуется закрыть.
2. Если вы хотите сохранить протокол сеанса в виде текстового файла, щелкните сеанс правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить как**, затем укажите файл для сохранения протокола.
3. Выполните одно из действий:
   - В меню **Сеанс** выберите пункт **Закрыть**.
   - Нажмите клавишу **F8**.
   - На панели инструментов нажмите кнопку **Закрыть**  .
4. После закрытия сеанс будет удален с панели **Сеансы**.

Чтобы закрыть программу обмена защищенными сообщениями, выполните одно из действий:

- В меню **Сеанс** выберите пункт **Выход**.
- Нажмите кнопку **Закрыть**  .

Примечание. При повторном открытии окна **Оперативный обмен защищенными сообщениями** все текущие сеансы будут восстановлены.

Файловый обмен

С помощью приложения «Файловый обмен» пользователи сети ViPNet могут пересылать друг другу файлы по защищенному каналу VPN. Ограничения на размер и тип передаваемых файлов отсутствуют. Кроме этого обеспечивается контроль их целостности. Если целостность файла при передаче была нарушена, то данный файл автоматически удаляется.

Примечание. Для файлов, полученных от пользователей, у которых установлено ПО ViPNet более ранних версий, проверка целостности не выполняется. В окне **Файловый обмен** (см. Рисунок 112 на стр. 260) для таких файлов указан статус **Целостность не подтверждена**. Решение об использовании такого файла принимается на усмотрение пользователя.

Приложение «Файловый обмен» вы можете вызвать из программы ViPNet Монитор, из контекстного меню Windows или из программы обмена защищенными сообщениями.

Примечание. Если на вашем сетевом узле файловый обмен недоступен, обратитесь к администратору сети ViPNet с просьбой разрешить файловый обмен.

Интерфейс программы «Файловый обмен»

Для просмотра файлов, отправленных и принятых по файловому обмену, откройте окно «Файловый обмен». Для этого в программе ViPNet Монитор выберите пункт меню **Приложения** > **Файловый обмен.**

Окно «Файловый обмен» также появляется каждый раз при отправке или приеме файлов.

Внешний вид окна программы «Файловый обмен» представлен на следующем рисунке.

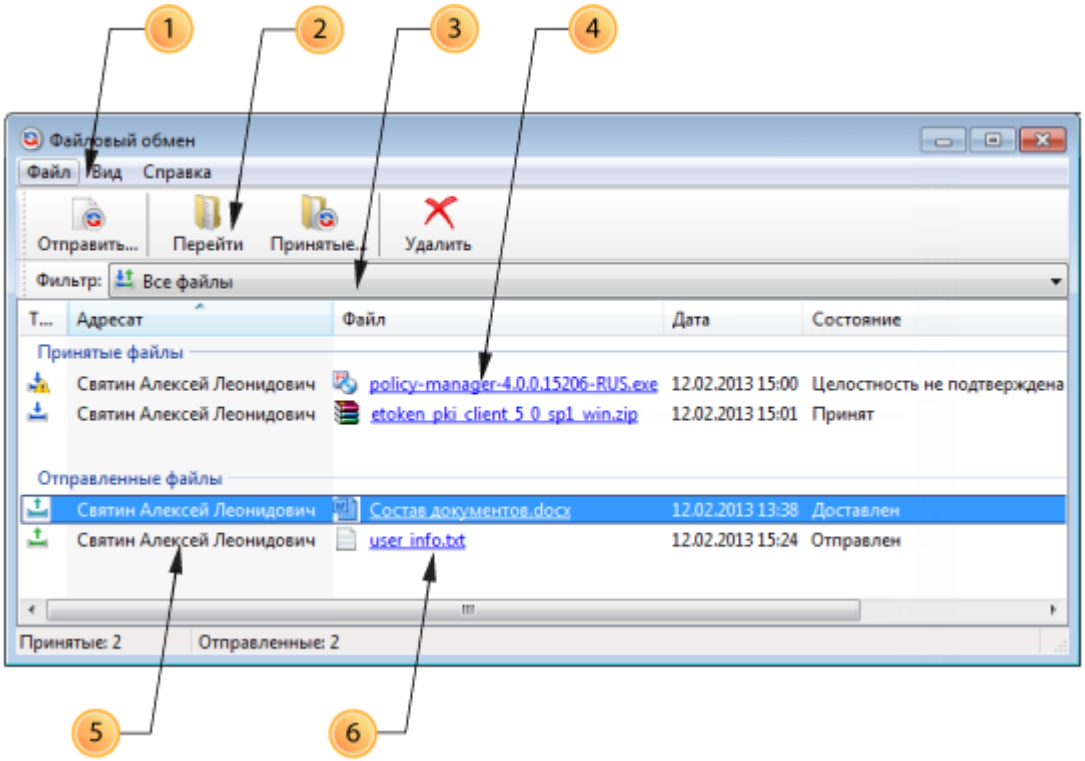


Рисунок 112: Окно файлового обмена

Цифрами на рисунке обозначены:

1. Главное меню программы.
2. Панель инструментов. С помощью кнопок на панели инструментов можно отправить новый файл, перейти к принятым файлам или удалить файл из списка.

   Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Настроить панель.**
3. Фильтр списка файлов. Предусмотрено три режима отображения списка:
   - Все файлы.
   - Принятые файлы.
   - Отправленные файлы.
4. Группа **Принятые файлы**. В этой группе отображаются файлы, полученные от пользователей других сетевых узлов ViPNet.
5. Группа **Отправленные файлы**. В этой группе отображаются файлы, переданные пользователям других сетевых узлов ViPNet.
6. Ссылка для перехода в папку, в которой находится файл.

Отправка файлов из программы ViPNet Монитор

Чтобы отправить файл с помощью программы ViPNet Монитор:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** выберите сетевой узел, на который требуется отправить файл. Чтобы выбрать несколько сетевых узлов, зажмите клавишу **Ctrl** и по очереди щелкните нужные узлы. Чтобы отфильтровать список сетевых узлов, воспользуйтесь строкой поиска в нижней части раздела **Защищенная сеть**.
3. Выполните одно из действий:
   - Нажмите кнопку **Отправить**  на панели инструментов.
   - Щелкните сетевой узел правой кнопкой мыши и в контекстном меню выберите пункт **Отправить файл**.
4. В появившемся окне укажите файлы или папки, которые требуется отправить, и нажмите кнопку **Открыть**.

   Выбранные файлы будут отправлены адресату.

Внимание! При отправке файла длина его имени (включая путь) не должна превышать 130 символов. При отправке папки:

- Имя папки (включая путь) должно иметь длину не более 31 символа и не должно содержать восклицательный знак.
- Имена вложенных папок и файлов должны иметь длину не более 31 символа.

Если указанные ограничения нарушены, программа выдаст сообщение об ошибке, файлы и папки не будут отправлены.

---

5. Откроется окно **Файловый обмен** (см. Рисунок 112 на стр. 260), в котором отображается информация об отправленных файлах и их состоянии.
6. Когда отправленные файлы будут доставлены получателю, программа выдаст уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

Примечание. Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу

Файловый обмен.

Отправка файлов с помощью контекстного меню Windows

Чтобы отправить файл пользователю ViPNet:

1. В Проводнике Windows выберите файл для отправки. Если нужно выбрать несколько файлов, удерживайте клавишу **Ctrl** и по очереди щелкните нужные файлы.
2. Щелкните один из выбранных файлов правой кнопкой мыши и в контекстном меню выберите пункт **Отправить файл адресату ViPNet.**

Внимание! При отправке файла длина его имени (включая путь) не должна превышать 130 символов. При отправке папки:

- Имя папки (включая путь) должно иметь длину не более 31 символа и не должно содержать восклицательный знак.
- Имена вложенных папок и файлов должны иметь длину не более 31 символа.

Если указанные ограничения нарушены, программа выдаст сообщение об ошибке, файлы и папки не будут отправлены.

3. В окне **Файловый обмен: Выбор сетевого узла** выберите из списка одного или нескольких получателей. Чтобы отфильтровать список пользователей, воспользуйтесь строкой поиска в нижней части окна.

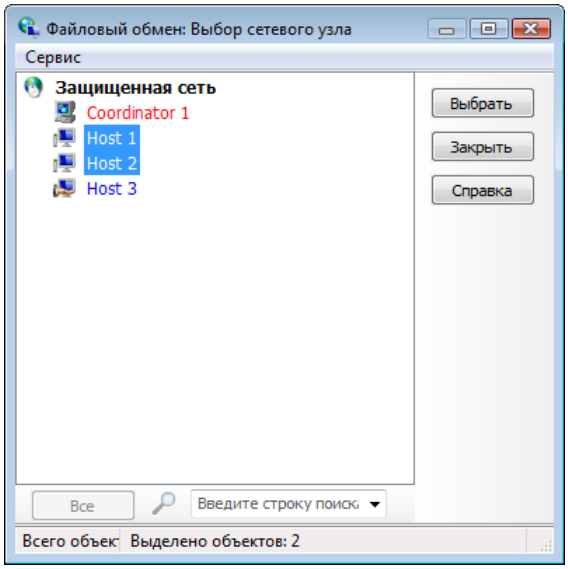


Рисунок 113: Выбор получателя для отправляемых файлов

4 Выбрав получателей, нажмите кнопку **Выбрать**. Файлы будут отправлены выбранным получателям.

5 Откроется окно **Файловый обмен** (см. Рисунок 112 на стр. 260), в котором отображается информация об отправленных файлах и их состоянии.

6 Когда отправленные файлы будут доставлены получателю, программа выдаст уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

Примечание. Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу **Файловый обмен**.

Отправка файлов из программы обмена защищенными сообщениями

Чтобы отправить файл во время обмена мгновенными сообщениями с пользователями ViPNet, выполните следующие действия:

1 В окне **Оперативный обмен защищенными сообщениями** (см. рисунок на стр. **Ошибка! Закладка не определена.**) на панели **Сеансы** выберите сеанс, участникам которого вы хотите отправить файл.

2 На панели **Получатели сообщений** выберите участников и на панели инструментов нажмите кнопку **Файл** .

3 В появившемся окне укажите файлы, которые требуется отправить, и нажмите кнопку **Открыть**.

Выбранные файлы будут отправлены участникам сеанса.

Внимание! При отправке файла длина его имени (включая путь) не должна превышать 130 символов. Если указанное ограничение нарушено, программа выдаст сообщение об ошибке, файлы не будут отправлены.

4 Откроется окно **Файловый обмен** (см. Рисунок 112 на стр. 260), в котором отображается информация об отправленных файлах и их состоянии.

5 Когда отправленные файлы будут доставлены получателям, программа выдаст уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

Примечание. Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу **Файловый обмен**.

Прием файлов

При поступлении файлов от другого пользователя ViPNet:

1 Программа выдаст сообщение о принятом файле, в области уведомлений появится значок программы файлового обмена .

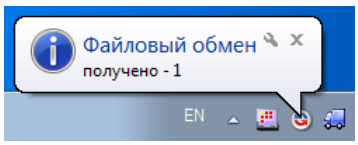


Рисунок 114: Уведомление о принятом файле

Примечание. Для настройки уведомлений в окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения** и перейдите к разделу **Файловый обмен**.

2 Чтобы просмотреть полученные файлы, щелкните значок файлового обмена в области уведомлений. Откроется окно **Файловый обмен** (см. Рисунок 112 на стр. 260).

3 В окне **Файловый обмен** в группе **Принятые файлы** выберите нужный файл и выполните одно из действий:

- Щелкните имя файла в столбце **Файл**.
- Нажмите кнопку **Принятые** на панели инструментов.

В новом окне будет открыта папка, содержащая выбранный файл.

Чтобы просмотреть файлы, полученные от определенного пользователя сети ViPNet:

1 В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.

2 В разделе **Защищенная сеть** выберите сетевой узел, от пользователя которого были приняты файлы, и нажмите кнопку **Принятые** на панели инструментов.

В новом окне будет открыта папка, содержащая файлы, поступившие с выбранного сетевого узла.

Примечание. Если в разделе **Защищенная сеть** выбрать несколько сетевых узлов и нажать кнопку **Принятые**, откроется папка, содержащая подпапки с файлами, которые были получены от разных пользователей ViPNet.

Вызов внешних приложений

Программы ViPNet Client и ViPNet Coordinator поддерживают вызов внешних приложений, таких как:

- VNC Viewer.
- Remote Desktop Connection.
- Radmin Viewer.

Подробнее о работе с программами Radmin Viewer, VNC Viewer и Remote Desktop Connection можно прочесть в разделе Запуск программы удаленного доступа (на стр. 295).

С помощью внешних программ пользователи ViPNet могут пользоваться различными сервисами, предоставляемыми через Интернет, например, доступом к удаленному рабочему столу. Преимущество работы с внешними программами в сети ViPNet состоит в том, что весь трафик этих программ надежно шифруется.

Для взаимодействия с другим пользователем ViPNet с помощью внешнего приложения:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** щелкните нужный сетевой узел правой кнопкой мыши и в контекстном меню выберите пункт **Внешние программы**, затем щелкните команду вызова требуемой программы.

   Внешняя программа будет автоматически запущена в защищенном режиме, а пользователю выбранного сетевого узла ViPNet будет предложено подтвердить запуск той же программы на его компьютере.

Просмотр веб-ресурсов сетевого узла

Если на компьютере, где установлено ПО ViPNet Client или ViPNet Coordinator, также установлен какой-либо веб-сервер или веб-приложение, то другие пользователи сети ViPNet могут осуществлять защищенное (шифрованное) соединение с этим веб-сервером.

При этом данный веб-сервер будет доступен только пользователям сети ViPNet, которым разрешено соединение с сетевым узлом, на котором установлен сервер. Это позволяет реализовать идею защищенного интернет-портала, в который могут быть интегрированы различные приложения — CRM, CMS, приложения на основе баз данных и многое другое.

Чтобы установить такое соединение:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** выберите сетевой узел, на котором организован защищенный Интернет-портал, и выполните одно из действий:
   - Нажмите кнопку **Веб-ресурс**  на панели инструментов.
   - Щелкните выбранный узел правой кнопкой мыши и в контекстном меню выберите пункт **Web-ссылка**.

Обзор общих ресурсов сетевого узла

Функция «Обзор общих ресурсов сетевого узла» позволяет открыть сетевые ресурсы с общим доступом на сетевом узле ViPNet. Соединение устанавливается в защищенном режиме.

Чтобы открыть общий ресурс сетевого узла ViPNet:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть.**
2. В разделе **Защищенная сеть** выберите нужный сетевой узел и выполните одно из действий:
   - Нажмите кнопку **Обзор**  на панели инструментов.
   - Щелкните выбранный узел правой кнопкой мыши и в контекстном меню выберите пункт **Открыть сетевой ресурс**.

В результате Проводник Windows в новом окне отобразит доступные сетевые ресурсы на выбранном сетевом узле. Пункт контекстного меню и кнопка на панели инструментов доступны, только если выбран один сетевой узел.

Проверка соединения с сетевым узлом

С помощью программы ViPNet Монитор можно проверить текущий статус других сетевых узлов ViPNet из раздела **Защищенная сеть** — доступны они или нет, активны или нет и так далее. Для проверки соединения с сетевым узлом необходимо, чтобы этот узел имел версию ПО ViPNet не ниже 2.8.9.

Чтобы проверить соединение с одним или несколькими сетевыми узлами ViPNet и узнать статус их пользователей:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть.**
2. В разделе **Защищенная сеть** выберите сетевой узел, соединение с которым требуется проверить. Чтобы выбрать несколько сетевых узлов, зажмите клавишу **Ctrl** и по очереди щелкните нужные узлы.
3. Выполните одно из действий:
   - Нажмите кнопку **Проверить** на панели инструментов.
   - Нажмите клавишу **F5.**
   - Щелкните один из выбранных сетевых узлов правой кнопкой мыши и в контекстном меню выберите пункт **Проверить соединение.**

   Откроется окно **Проверка соединения**, содержащее информацию о выбранных сетевых узлах.

Внешний вид окна **Проверка соединения** представлен на следующем рисунке:

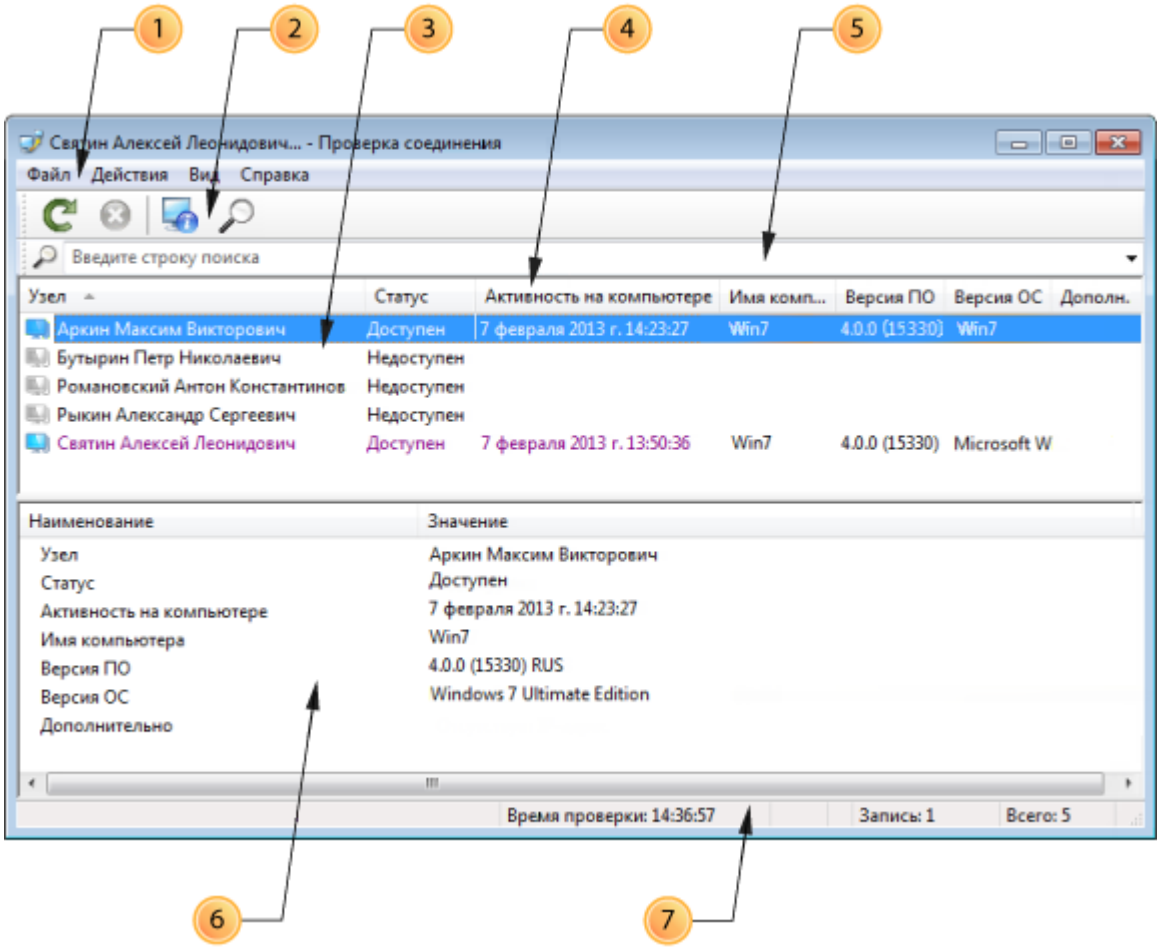


Рисунок 115: Окно проверки соединения

Цифрами на рисунке обозначены:

1 Главное меню программы проверки соединения.

2 Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Настроить панель.**

3 Основная панель. Содержит список сетевых узлов, с которыми осуществляется проверка соединения.

Цвет и цветовое выделение (фон) имени сетевого узла обозначают его текущее состояние:

Цвет имени	Состояние сетевого узла
Фиолетовый	Сетевой узел доступен, но последние 15 минут не проявлял активности на компьютере.
Черный на зеленом фоне	Сетевой узел доступен и проявлял активность за последние 15 минут.
Черный	Сетевой узел в данный момент не подключен к сети.

- Чтобы посмотреть подробную информацию о сетевом узле в отдельном окне, выполните одно из действий:
  - Дважды щелкните нужный сетевой узел.
  - Выберите сетевой узел из списка и нажмите кнопку **Свойства** на панели инструментов.
  - Выберите сетевой узел из списка и нажмите клавишу **F3**.

  Откроется окно **Свойства узла**.

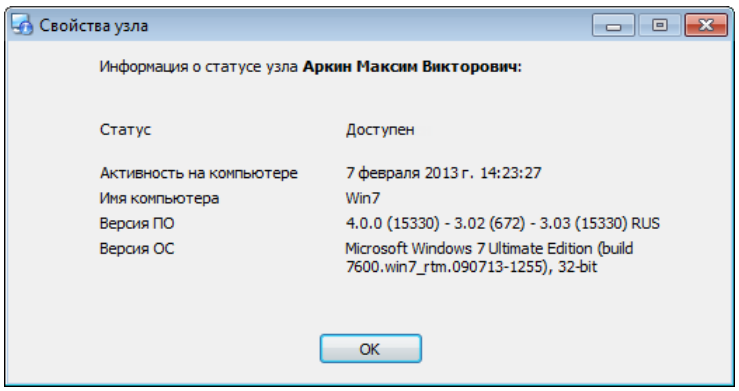


Рисунок 116: Подробная информация о статусе сетевого узла

- Чтобы отправить на один из сетевых узлов в окне **Проверка соединения** письмо программы ViPNet Деловая почта, начать сеанс обмена защищенными сообщениями или выполнить другое действие, доступное в разделе **Защищенная сеть**, щелкните выбранный узел правой кнопкой мыши и в контекстном меню выберите соответствующий пункт.

4 Столбцы основной панели. Статус сетевых узлов указан в столбце **Статус.** Описание возможных статусов приведено в таблице ниже.

Статус	Описание
Доступен	Есть полноценная связь с сетевым узлом.
Связь по VPN есть, но программа Монитор не доступна	На сетевом узле не активна программа ViPNet Монитор, но сам узел доступен по защищенному каналу. В этом случае при взаимодействии с сетевым узлом недоступны встроенные средства коммуникации (такие как обмен защищенными сообщениями, файловый обмен и другие), но возможен просмотр общих ресурсов и веб-ресурсов сетевого узла, подключение через удаленный рабочий стол.
Недоступен	Связь с сетевым узлом отсутствует.

В столбце **Активность на компьютере** указано время последней активности.

Чтобы отсортировать список по одному из столбцов, щелкните заголовок столбца. С помощью контекстного меню можно удалить или добавить столбцы.

5 Строка поиска. Предназначена для фильтрации списка сетевых узлов на основной панели (**3**).

6 Панель свойств узла. Содержит подробную информацию о сетевом узле, выбранном на основной панели (**3**).

7 Строка состояния.

Примечание. По умолчанию в окне **Проверка соединения** не отображаются панель инструментов (**2**), строка поиска (**5**), панель свойств узла (**6**) и строка состояния (**7**). Для отображения этих элементов интерфейса в меню **Вид** установите флажки в соответствующих пунктах.

17

Административные функции

Работа с журналом IP-пакетов

В разделе **Журнал IP-пакетов** на основе различных параметров поиска можно сформировать отчет о зарегистрированных программой IP-пакетах. Такие отчеты позволяют контролировать все входящие и исходящие соединения компьютера.

Настройка параметров поиска IP-пакетов

Для просмотра журнала IP-пакетов:

1 В окне программы ViPNet Монитор выберите раздел **Статистика и журналы** > **Журнал IP-пакетов**.

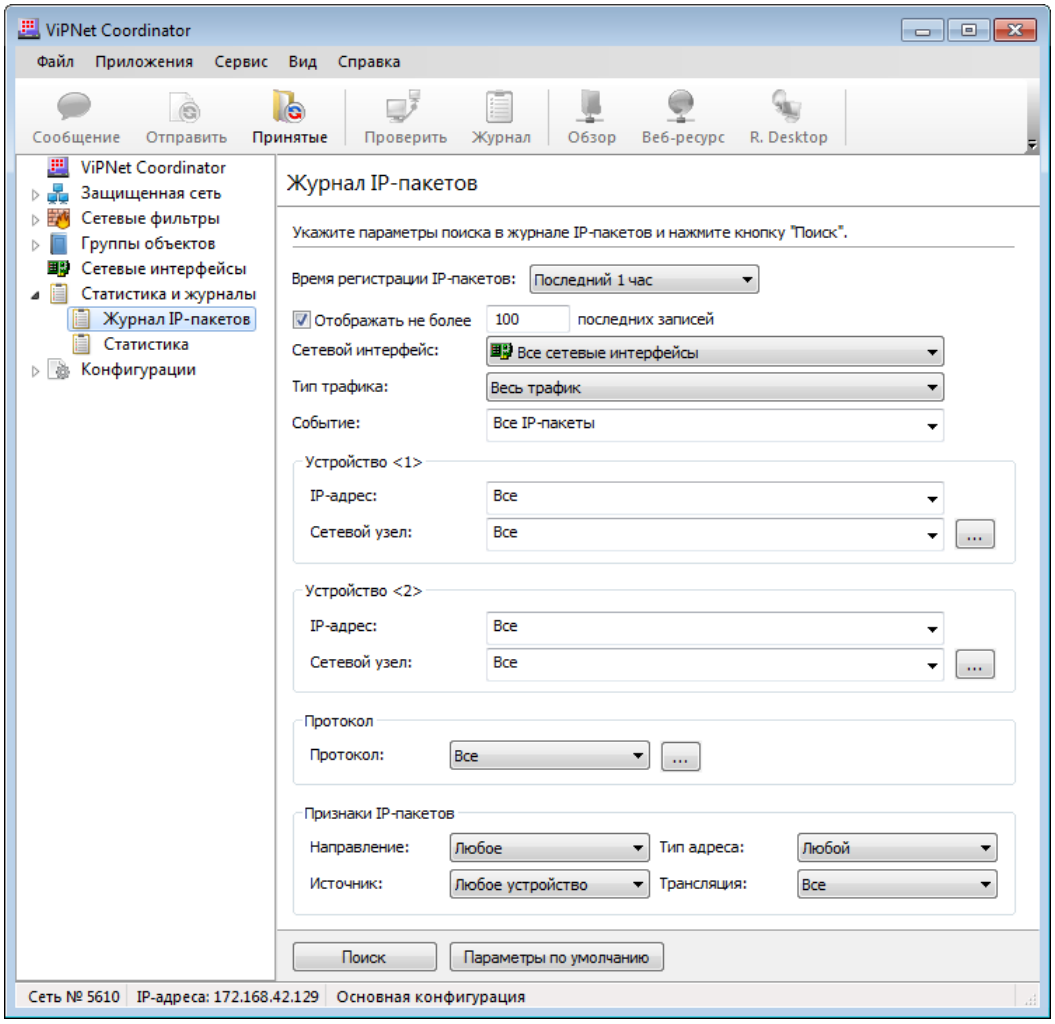


Рисунок 117: Настройка параметров поиска по журналу IP-пакетов

2 В разделе **Журнал IP-пакетов** задайте следующие параметры поиска:

- **Время регистрации IP-пакетов** (последние 24 часа, последний час, заданный интервал времени).
- **Число отображаемых записей журнала**. По умолчанию установлен флажок **Отображать не более** и заданное количество записей равно 100. Если снять этот флажок, будут показаны все записи, соответствующие параметрам поиска.
- В списке **Сетевой интерфейс** выберите интерфейс координатора, через который проходили искомые IP-пакеты.
- В списке **Тип трафика** выберите один из пунктов:
  - **Весь трафик** — будут отображены записи обо всех IP-пакетах.

- **Туннелируемый** — будут отображены записи об IP-пакетах, которые зарегистрированы в рамках туннельных соединений.
- **Транзитный защищенный** — будут отображены записи о зашифрованных IP-пакетах, проходящих через данный координатор, который выступает в роли маршрутизатора. Отправителями и получателями пакетов выступают защищенные узлы. Сам координатор ни отправителем, ни получателем пакетов не является.
- **Транзитный открытый** — аналогично параметру **Транзитный защищенный**, но участниками соединения в данном случае являются открытые узлы (узлы, на которых не установлено ПО ViPNet и которые при этом не туннелируется координатором).
- **Локальный защищенный** — будут отображены записи о зашифрованных IP-пакетах, отправителем или получателем которых является выбранный интерфейс данного координатора.
- **Локальный открытый** — будут отображены записи об открытых IP-пакетах, отправителем или получателем которых является выбранный интерфейс данного координатора.

- В списке **Событие** укажите для поиска определенный тип или группу типов событий, которые ViPNet Монитор сопоставляет каждому IP-пакету (см. «События, отслеживаемые ПО ViPNet» на стр. 418).
- В группе **Устройство <1>** укажите IP-адрес (диапазон адресов) компьютера или имя сетевого узла ViPNet, являющегося одним из участников соединения (отправителем или получателем IP-пакетов).
- В группе **Устройство <2>** укажите IP-адрес (диапазон адресов) компьютера или имя сетевого узла ViPNet, являющегося вторым участником соединения.

Примечание. Задавать значения для обоих полей (**IP-адрес** и **Сетевой узел**) имеет смысл в случае, если участник соединения имеет несколько IP-адресов и необходимо получить статистику соединений с каким-либо конкретным IP-адресом, зарегистрированным на выбранном участнике.

- В списке **Протокол** выберите протокол передачи IP-пакетов, которые требуется найти. Если в списке нет нужного протокола, нажмите кнопку  и в окне **Список протоколов** добавьте требуемый протокол.
- В группе **Признаки IP-пакетов**:
  - В списке **Направление** выберите направление передачи IP-пакетов, которые требуется найти (**Любое**, **Входящие**, **Исходящие**).

- В списке **Тип адреса** укажите, на какие адреса отправлялись IP-пакеты (**Любой**, **Одноадресный**, **Широковещательный**, **Групповой**).
- В списке **Источник** укажите, какой из участников соединения является отправителем IP-пакетов.
- В списке **Трансляция** укажите, следует ли отображать IP-пакеты, которые в процессе следования подверглись трансляции (подмене IP-адресов) по правилам трансляции, заданным на координаторе.

o Чтобы восстановить начальные параметры поиска, нажмите кнопку **Параметры по умолчанию**.

3 Задав параметры поиска, нажмите кнопку **Поиск**.

Примечание. Если выполнить поиск с параметрами по умолчанию, в отчете будет показано не более 100 записей об IP-пакетах, зарегистрированных за последний час.

Просмотр результатов поиска

После нажатия кнопки **Поиск** в разделе **Журнал IP-пакетов** будет выполнен поиск по журналу в соответствии с указанными параметрами. Результаты поиска отобразятся в окне **Журнал регистрации IP-пакетов**.

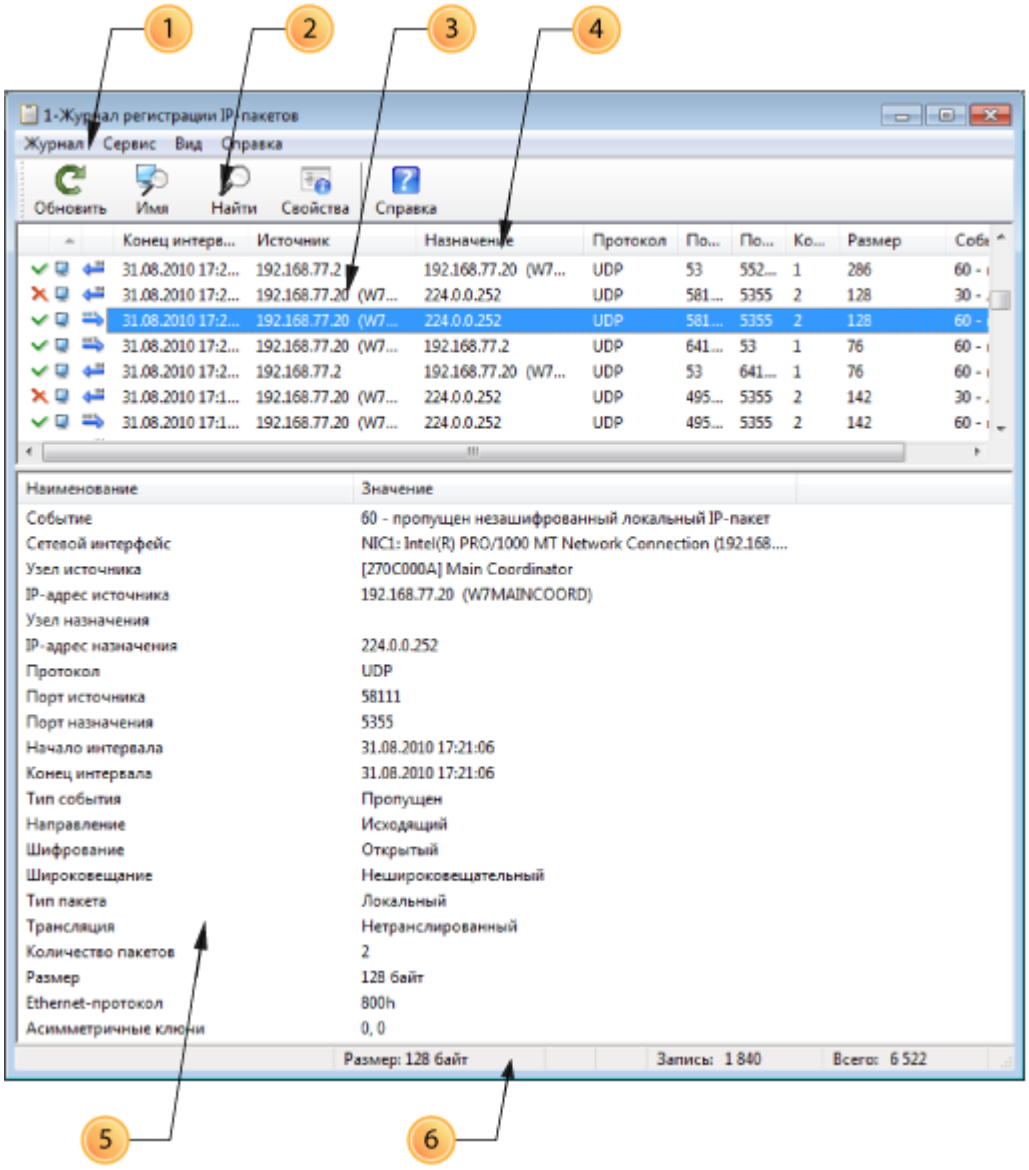


Рисунок 118: Просмотр журнала IP-пакетов

Цифрами на рисунке обозначены:

1 Главное меню.

2 Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Настроить панель**.

3 Основная панель. Содержит список записей журнала, соответствующих заданным параметрам поиска.

- Чтобы просмотреть подробную информацию о выбранном IP-пакете в отдельном окне, нажмите кнопку **Свойства IP-пакетов** на панели инструментов окна **Журнал регистрации IP-пакетов**.
- Чтобы найти имя компьютера-отправителя или получателя выбранного пакета, нажмите кнопку **Определить имя компьютера** на панели инструментов или щелкните запись о пакете правой кнопкой мыши и в контекстном меню выберите пункт **Определить имя компьютера**.

4 Столбцы основной панели.

Чтобы отсортировать список по одному из столбцов, щелкните заголовок столбца. С помощью контекстного меню можно удалить или добавить столбцы.

Описание столбцов приведено в таблице ниже.

Таблица 11. Описание столбцов основной панели

Название столбца	Описание
Тип события	Типы событий обозначаются следующими значками: — IP-пакеты заблокированы. — IP-пакеты пропущены. — IP-пакеты относятся к служебным событиям.
Тип пакета	Типы пакетов обозначаются следующими значками: — транзитный IP-пакет. — локальный IP-пакет. — туннелируемый IP-пакет.
Свойства пакета	Свойства IP-пакетов обозначаются следующими значками: — открытые входящие IP-пакеты. — открытые исходящие IP-пакеты. — зашифрованные входящие IP-пакеты. — зашифрованные исходящие IP-пакеты.
Начало интервала	Дата и время создания записи для группы однотипных IP-пакетов (регистрация первого пакета). Подробнее о регистрации однотипных пакетов в течение определенного интервала времени можно узнать в разделе Настройка параметров регистрации IP-пакетов в журнале.

Конец интервала	Конец интервала регистрации группы однотипных IP-пакетов. Если на данный момент интервал еще не закончился, то в этом столбце указано время регистрации последнего IP-пакета данного типа. Если будут зарегистрированы новые пакеты данного типа, значение данного параметра изменится.
Источник	Имя сетевого узла (для защищенных узлов ViPNet) или IP-адрес и имя компьютера (для открытых узлов) отправителя пакета.
Узел источника	Имя сетевого узла отправителя пакета (только для защищенных узлов). Если пакет отправлен открытым узлом, этот столбец будет пустым.
IP-адрес источника	IP-адрес и имя компьютера (если определилось) отправителя пакета.
Порт источника	Номер порта отправителя пакета.
Назначение	Имя сетевого узла (для защищенных узлов ViPNet) или IP-адрес и имя компьютера (для открытых узлов) получателя пакета.
Узел назначения	Имя сетевого узла получателя (только для защищенных узлов). Если пакет предназначен для открытого узла, этот столбец будет пустым.
IP-адрес назначения	IP-адрес и имя компьютера (если определилось) получателя пакета.
Порт назначения (Тип / код ICMP)	Номер порта получателя пакета.
Протокол	Протокол, по которому было установлено соединение.
Событие	Событие, соответствующее данной записи. Описание событий содержится в приложении События, отслеживаемые ПО ViPNet (на стр. 418).
Количество пакетов	Количество однотипных IP-пакетов, сгруппированных в одну запись в течение заданного интервала времени.
Размер	Размер (в байтах) всех IP-пакетов, сгруппированных в одну запись.

5 Панель свойств IP-пакетов. Содержит подробную информацию о записи, выбранной на основной панели (**3**).

6 Строка состояния. Содержит размер выбранного пакета (или группы пакетов) в байтах, порядковый номер записи в списке и общее число найденных записей. Если на основной панели (**3**) выбрано несколько записей, в строке состояния отображается суммарный размер соответствующих IP-пакетов.

Совет. Чтобы определить суммарный объем IP-трафика, зарегистрированного на сетевом узле ViPNet, выполните поиск всех IP-пакетов в журнале. Затем в окне **Журнал регистрации IP-пакетов** с помощью сочетания клавиш **Ctrl+A** выберите все записи. В строке состояния будет показан суммарный размер найденных IP-пакетов.

Просмотр журнала IP-пакетов в интернет-браузере или в Microsoft Excel

Чтобы экспортировать результаты поиска, в окне **Журнал регистрации IP-пакетов** щелкните меню **Журнал**, а затем выберите один из пунктов:

- **Просмотр в веб-браузере.** Таблица с результатами поиска будет открыта в вашем веб-браузере. В строке адреса будет указан путь к файлу отчета.
- **Просмотр в Excel.** Таблица с результатами поиска будет открыта в приложении Microsoft Excel (для этого приложение должно быть установлено на компьютере). Чтобы сохранить эту таблицу, в Microsoft Excel воспользуйтесь функцией **Сохранить как**.

Выбор IP-пакетов

В журнале регистрации IP-пакетов можно выделить IP-пакеты:

- широковещательные;
- относящиеся к служебным событиям;
- принадлежащие одной сессии, установленной в начале взаимодействия между двумя узлами;
- принадлежащие одним и тем же IP-адресам вне зависимости от направления пакета и порта соединения.

Примечание. Под сессией подразумеваются все IP-пакеты, передаваемые между узлом 1 и узлом 2. Если при этом соединение осуществляется по протоколу TCP или UDP, то учитываются также и порты. Например, соединение между узлом 1 и узлом 2 по протоколу HTTP будет считаться одной сессией (узел 1 открывает веб-страницу с сервера IIS, установленного на узле 2). Однако если узел 1 подключится к узлу 2 по протоколу FTP (скачает файл с FTP-сервера, установленного на узле 2), то это уже будет считаться другой сессией.

Чтобы выделить IP-пакеты:

1. В окне **Журнал регистрации IP-пакетов** щелкните запись журнала правой кнопкой мыши.
2. В появившемся контекстном меню выберите:
   - **Выделить по IP-адресам**, чтобы выделить все записи IP-пакетов, имеющих те же IP-адреса, что выбранный пакет.
   - **Выделить сессию**, чтобы выделить все записи IP-пакетов, относящихся к сессии выбранного пакета.
   - **Выделить широковещательные**, чтобы выделить записи широковещательных пакетов.
   - **Выделить служебные**, чтобы выделить записи служебных событий.
3. Чтобы снять выделение, в контекстном меню выберите пункт **Отменить выделение**.

Подсчет объема трафика

С помощью журнала IP-пакетов можно подсчитать общий размер IP-пакетов, удовлетворяющих критериям поиска. Для этого:

1. В окне **Журнал регистрации IP-пакетов** в основной панели выделите интересующие вас записи журнала.

   Чтобы выделить все IP-пакеты, показанные в журнале воспользуйтесь комбинацией клавиш **Ctrl+A.**
2. В строке состояния отобразится суммарный размер выделенных IP-пакетов.

Рекомендации по анализу открытых (нешифрованных) и зашифрованных соединений

Для удобства анализа открытых соединений в журнале регистрации IP-пакетов рекомендуется произвести следующие настройки:

1. В окне **Журнал регистрации IP-пакетов** щелкните правой кнопкой мыши по любому из заголовков столбцов.
2. В появившемся контекстном меню выберите **Свойства.**
3. Для анализа:
   - открытых (нешифрованных) соединений:

- в окне **Поля** настройте отображение следующих столбцов: **IP-адрес источника**, **IP-адрес назначения**.
- в окне **Поля** скройте следующие столбцы: **Источник**, **Узел источника**, **Назначение**, **Узел назначения**.

o закрытых (зашифрованных) соединений:

- в окне **Поля** настройте отображение следующих столбцов: **Узел источника**, **Узел назначения**.
- в окне **Поля** скройте следующие столбцы: **IP-адрес источника**, **IP-адрес назначения**.

4 По окончании настройки нажмите кнопку **OK** для закрытия окна и сохранения изменений или кнопку **Отмена** для выхода без сохранения изменений.

Создание сетевого фильтра при просмотре журнала IP-пакетов

Если требуется пропускать IP-пакеты в рамках запрещенных соединений либо блокировать IP-пакеты в рамках разрешенных соединений, вы можете создать сетевой фильтр для таких IP-пакетов при просмотре соединений в журнале IP-пакетов. Для этого выполните следующие действия:

1 В окне **Журнал регистрации IP-пакетов** (см. «Просмотр результатов поиска» на стр. 277) выберите запись о заблокированном соединении, которое должно быть разрешено, либо разрешенное соединение, которое должно быть заблокировано.

2 Щелкните выбранную запись правой кнопкой мыши и в контекстном меню выберите пункт **Создать фильтр**.

В зависимости от типа выбранного соединения появится окно создания:

- Фильтра открытой сети — если в рамках соединения передавались незашифрованные IP-пакеты.
- Фильтра защищенной сети — если в рамках соединения передавались зашифрованные IP-пакеты.
- Транзитного фильтра открытой сети — если в рамках соединения передавались транзитные IP-пакеты.
- Фильтра для туннелируемых узлов — если в рамках соединения передавались IP-пакеты между туннелируемыми узлами координатора и защищенными узлами.

3 В разделах окна свойств сетевого фильтра будут автоматически заданы параметры, сформированные из записи выбранного соединения. При необходимости внесите соответствующие изменения (см. «Создание сетевых фильтров» на стр. 178).

4 В окне свойства сетевого фильтра нажмите кнопку **OK**. В результате созданный фильтр появится в списке сетевых фильтров.

Просмотр архива журналов IP-пакетов

Архивация журналов IP-пакетов применяется для оптимизации поиска по IP-пакетам и для рационального использования дискового пространства.

Новый архив создается, когда текущий журнал IP-пакетов достиг размера, определенного параметром **Максимальный размер журнала**. Если данный параметр установлен в значение «0», архивирование журнала не происходит.

Для просмотра архива журнала IP-пакетов:

1 В окне программы ViPNet Монитор в разделе **Журнал IP-пакетов** выберите подраздел **Архив журналов** и далее архив с нужным интервалом дат.

Примечание. Если подраздел **Архив журналов** не отображается, значит, системой не было создано ни одного архива.

2 Укажите параметры поиска по архиву журнала (см. «Настройка параметров поиска IP-пакетов» на стр. 274).

3 Результаты поиска будут отображены в окне **Журнал регистрации IP-пакетов**.

Совет. Чтобы удалить неактуальные архивы журналов IP-пакетов, в подразделе **Архив журналов** выберите один или несколько архивов и воспользуйтесь клавишей **Delete** на клавиатуре или командой **Удалить** из контекстного меню.

Просмотр журнала IP-пакетов другого сетевого узла

При работе в режиме администратора сетевого узла можно запросить журнал IP-пакетов другого сетевого узла ViPNet, с которым у данного узла есть связь. Для этого выполните следующие действия:

1. Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304).
2. В окне программы ViPNet Монитор на панели навигации выберите раздел **Журнал IP-пакетов**.
3. В списке **Журнал сетевого узла** выберите сетевой узел, журнал которого требуется просмотреть. Если нужного сетевого узла нет в списке, нажмите кнопку  и в окне **Выбор сетевого узла** укажите нужный узел.
4. После выбора сетевого узла, журнал которого требуется просмотреть, с этим узлом будет установлено соединение. В случае успешного соединения имя выбранного узла появится в списке **Журнал сетевого узла**. Чтобы прервать процесс подключения, нажмите кнопку **Отмена**.

Примечание. Если сетевой узел, с которого запрашивается журнал IP-пакетов, имеет версию ПО ViPNet ниже 3.0, то параметры поиска будут существенно ограничены. Это связано с тем, что в версии 3.0 формат журнала IP-пакетов изменился. При ограничении параметров поиска появится соответствующее предупреждение.

Следует иметь в виду, что при просмотре журнала IP-пакетов другого сетевого узла параметры поиска соответствуют типу этого узла. То есть если в программе ViPNet Coordinator запросить журнал IP-пакетов клиента, можно указать только параметры, доступные на клиентах.

---

5. Задайте параметры поиска (см. «Настройка параметров поиска IP-пакетов» на стр. 274) и нажмите кнопку **Поиск**.

Настройка параметров регистрации IP-пакетов в журнале

Чтобы настроить параметры журнала IP-пакетов:

1. В главном окне ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2 На панели навигации окна **Настройка** выберите раздел **Журнал IP-пакетов**.

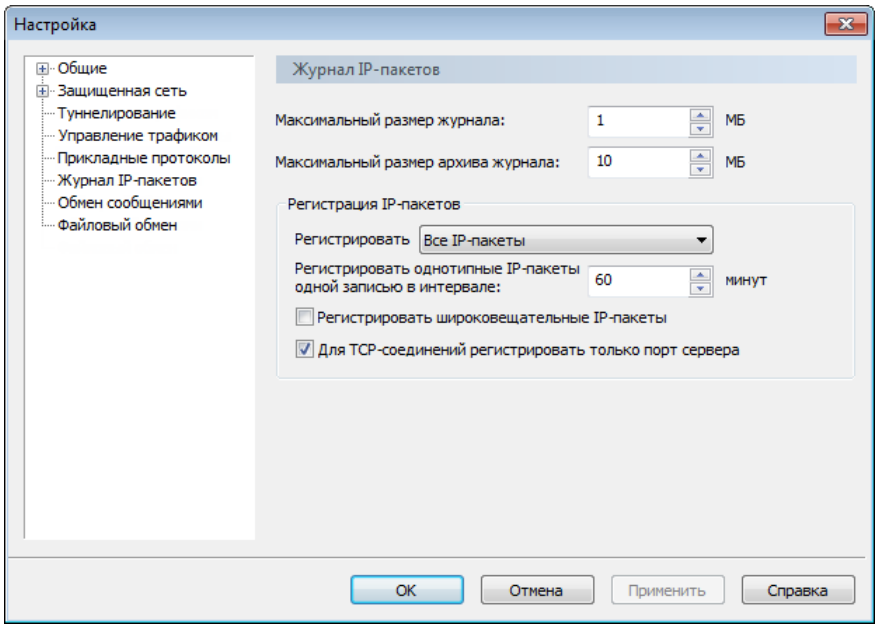


Рисунок 119: Настройка параметров журнала IP-пакетов

3 Задайте значения следующих параметров:

- В поле **Максимальный размер журнала** укажите размер журнала в мегабайтах (по умолчанию — 1 Мбайт). Если размер журнала превысит указанное значение, записи в хронологическом порядке будут переноситься в архив.

  Чтобы отключить ведение журнала, задайте значение 0. Записи о новых зарегистрированных IP-пакетах не будут добавляться в журнал. Однако записи, созданные до присвоения значения 0, будут сохранены.

  При первой архивации журнала IP-пакетов на панели навигации главного окна ViPNet Монитор создается раздел **Архив журналов**.

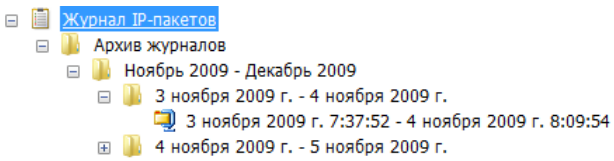


  Рисунок 120: Архив журнала IP-пакетов

- В поле **Максимальный размер архива журнала** укажите размер архива в мегабайтах (по умолчанию — 10 Мбайт). Если размер архива журнала превысит указанное значение, старые записи будут удаляться из архива в хронологическом порядке.

  Чтобы отключить перенос записей в архив, задайте значение 0. Однако данные, помещенные в архив до присвоения значения 0, будут сохранены.

- С помощью списка **Регистрировать** укажите, какие IP-пакеты следует регистрировать в журнале: **Все IP-пакеты** или **Только блокируемые IP-пакеты.**
- В поле **Регистрировать однотипные IP-пакеты одной записью в интервале** укажите интервал времени в минутах. По истечении указанного интервала для IP-пакетов определенного типа будет создаваться новая запись в журнале.

  Смысл данного параметра состоит в том, что при регистрации пакета с определенными параметрами (IP-адрес, протокол, порт и так далее) для него создается запись в журнале. В течение указанного интервала времени IP-пакеты, которые имеют те же IP-адрес, протокол, порт и другие параметры, регистрируются, но записи в журнале для них не создаются. Число таких пакетов, зарегистрированных в течение интервала, указано в столбце **Количество пакетов** в окне **Журнал регистрации IP-пакетов.**

  Когда заданный интервал времени истекает, для следующего IP-пакета создается новая запись в журнале, даже если этот пакет имеет параметры, которые уже зафиксированы в другой записи. Если поступает пакет другого типа, для него также создается новая запись в журнале. После создания новой записи снова начинается отсчет интервала времени для пакетов с одинаковыми параметрами. Данный механизм распространяется на все регистрируемые IP-пакеты.

  Начало и конец интервала времени, в течение которого были зарегистрированы IP-пакеты, объединенные одной записью, указаны в столбцах **Начало интервала** и **Конец интервала.**

  Данный механизм позволяет значительно сократить размер журнала IP-пакетов, сохранив его информативность. Чем больше заданный интервал времени, тем меньше размер журнала. Однако с увеличением интервала регистрации уменьшается точность данных в журнале (невозможно определить время регистрации пакетов).

  Если задать нулевое значение интервала регистрации пакетов, для каждого зарегистрированного IP-пакета будет создаваться запись в журнале. Однако размер журнала при этом может сильно увеличиться. Нулевое значение интервала рекомендуется задавать только для тестирования и на короткое время. ViPNet-драйвер может хранить не более 10000 записей журнала. По достижении этого ограничения более старые записи заменяются новыми. Если обмен трафиком достаточно интенсивен, часть информации может быть потеряна. Кроме того, обработка трафика может замедлиться, так как увеличится нагрузка на процессор компьютера.
- Установите флажок **Регистрировать широковещательные IP-пакеты**, чтобы такие пакеты фиксировались в журнале.

- Убедитесь, что установлен флажок **Для TCP-соединений регистрировать только порт сервера**. В этом случае IP-пакеты протокола TCP будут группироваться по порту сервера вне зависимости от порта клиента.

4 Чтобы сохранить настройки, нажмите кнопку **Применить**.

Просмотр статистики фильтрации IP-пакетов

Чтобы просмотреть статистику фильтрации IP-пакетов, в окне программы ViPNet Монитор на панели навигации выберите раздел **Статистика и журналы** > **Статистика**.

В разделе **Статистика** представлены данные о количестве входящих и исходящих IP-пакетов, которые были пропущены или заблокированы в соответствии с заданными фильтрами трафика. Эта информация может быть полезна при первоначальной настройке программы ViPNet Монитор.

Чтобы обнулить статистику IP-пакетов, нажмите кнопку **Очистить**.

Чтобы просмотреть статистику IP-пакетов только по одному сетевому интерфейсу координатора, в списке **Сетевой адаптер** выберите нужный интерфейс.

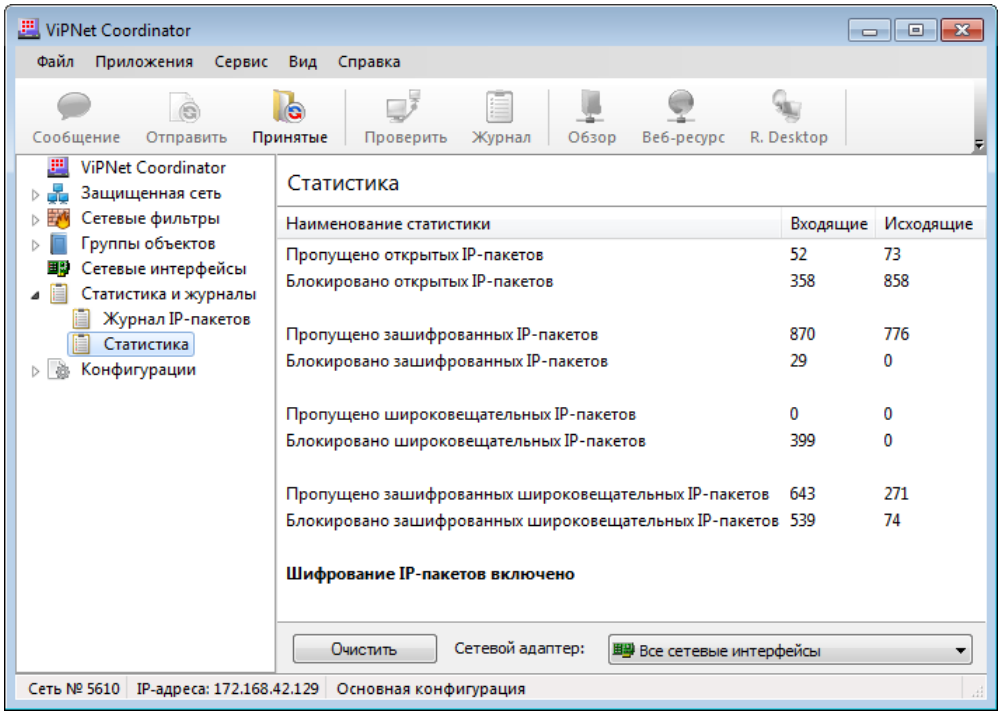


Рисунок 121: Просмотр статистики IP-пакетов

Просмотр информации о координаторе, времени работы программы и числе соединений

Чтобы получить информацию о сети ViPNet, в которой находится координатор, о пользователе, который произвел вход в программу, сведения о соединениях координатора и другую дополнительную информацию, в окне программы ViPNet Монитор выберите раздел **ViPNet Coordinator**.

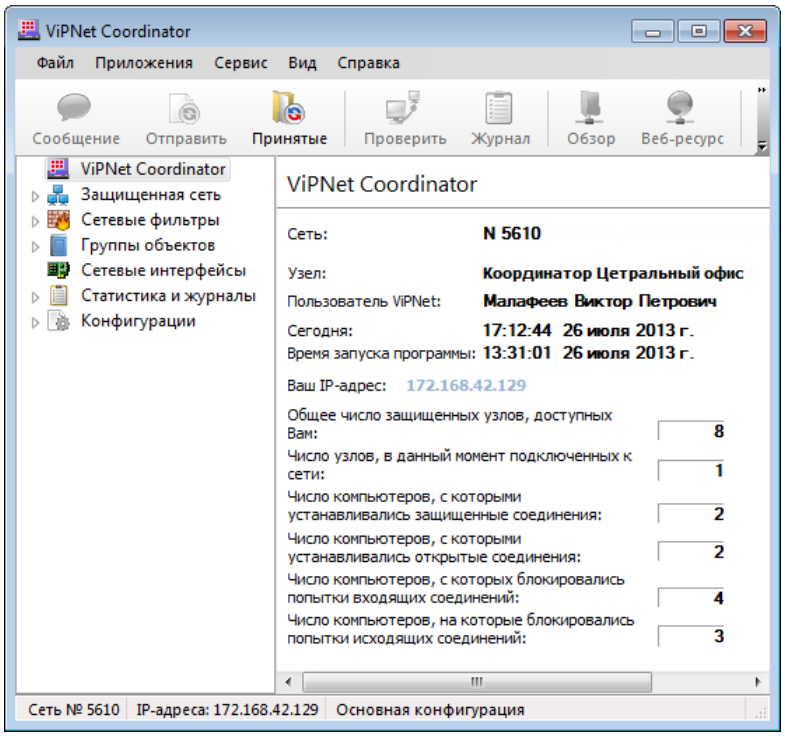


Рисунок 122: Просмотр дополнительной информации о координаторе

Управление конфигурациями программы

Конфигурация — это совокупность всех настроек ViPNet Монитор. В разделе **Конфигурации** можно создать несколько дополнительных конфигураций и установить требуемую конфигурацию в любой момент.

Использование нескольких конфигураций может быть полезно в следующем случае. Предположим, что политика безопасности компании запрещает одновременно работать с локальными ресурсами и ресурсами Интернета. Тогда следует создать две конфигурации: в одной конфигурации должна быть разрешена работа в Интернете и запрещен доступ в локальную сеть, во второй конфигурации должна быть разрешена работа в локальной сети и запрещен доступ в Интернет.

При первом запуске программы создается **Основная конфигурация**, которая содержит настройки по умолчанию. Эту конфигурацию нельзя переименовать или удалить.

В программе ViPNet Монитор вы можете выполнить следующие действия по управлению конфигурациями:

1 Чтобы создать новую конфигурацию, в окне программы ViPNet Монитор на панели навигации щелкните правой кнопкой мыши раздел **Конфигурации** и в контекстном меню выберите **Создать конфигурацию**.

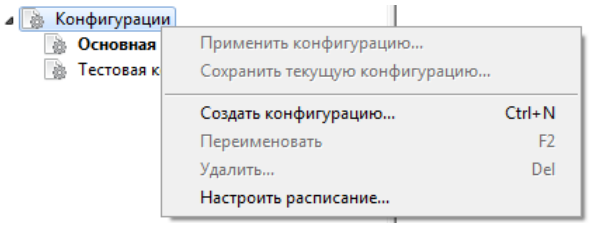


Рисунок 123: Создание новой конфигурации

В списке конфигураций появится элемент **Новая конфигурация**.

Примечание. В режиме администратора можно создать конфигурацию программы для любого пользователя, зарегистрированного на узле. В данном режиме отображаются все конфигурации, созданные в процессе работы с программой, причем они сгруппированы по пользователям, от имени которых были созданы.

2 Чтобы переименовать конфигурацию, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Переименовать**.

3 Чтобы загрузить (сделать активной) одну из конфигураций, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Применить конфигурацию**.

Примечание. Загрузить нужную конфигурацию вы также можете из главного меню программы **Файл** > **Конфигурации** либо из контекстного меню значка программы ViPNet Монитор в области уведомлений на панели задач.

---

4 Если в текущей конфигурации были изменены параметры программы (например, созданы новые сетевые фильтры, изменены настройки), то вы можете сохранить изменения в любой другой существующей конфигурации, кроме основной. Для этого щелкните нужную конфигурацию правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить текущую конфигурацию**. В окне подтверждения нажмите кнопку **Да**.

В текущей конфигурации все изменения сохраняются автоматически.

Если в программе создано несколько конфигураций и при этом в настройках установлен флажок **Вызывать окно выбора конфигурации** (см. «Настройка параметров запуска и аварийного завершения программы ViPNet Монитор» на стр. 316), то при запуске ViPNet Монитор откроется окно выбора конфигурации.

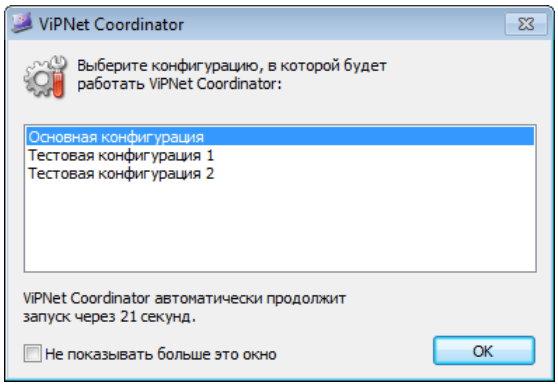


Рисунок 124: Выбор конфигурации при запуске программы

Для того чтобы загрузить одну из этих конфигураций, выберите ее в списке и нажмите кнопку **ОК**.

Если в течение 30 секунд с момента появления окна не будет выбрана ни одна конфигурация, программа ViPNet Монитор продолжит работу в основной конфигурации.

Если в программе создано несколько конфигураций, которые используется в конкретные периоды времени, то для удобства вы можете настроить расписание автоматической смены данных конфигураций (см. «Настройка расписания смены конфигураций программы» на стр. 293).

Настройка расписания смены конфигураций программы

Если в процессе работы в программе ViPNet Монитор используется несколько конфигураций, каждая из которых должна устанавливаться в конкретное время, настройте расписание автоматической смены конфигураций.

Примечание. Настроить расписание смены конфигураций можно только в том случае, если в программе создано более двух конфигураций. Основная конфигурация при этом не учитывается, расписание ее установки настроить нельзя. Основная конфигурация автоматически устанавливается и вступает в действие в те промежутки времени, в которые не действуют по расписанию остальные конфигурации.

Чтобы настроить расписание смены конфигураций, выполните следующие действия:

1. В окне программы ViPNet Монитор на панели навигации щелкните правой кнопкой мыши раздел **Конфигурации** или любую созданную конфигурацию и в контекстном меню выберите пункт **Настроить расписание**.

2. В окне **Настройка расписания смены конфигурации** установите флажок **Устанавливать конфигурации в соответствии с расписанием**, после чего добавьте в список конфигураций, которые требуется устанавливать автоматически.

   При добавлении конфигурации в окне **Параметры расписания** задайте следующие данные:

   - в поле **Начало действия** — время установки конфигурации (в часах);
   - в поле **Длительность** — время, в течение которого должна действовать конфигурация после установки (количество часов);
   - в группе **Повторение** — дни недели, в которые должна устанавливаться конфигурация.

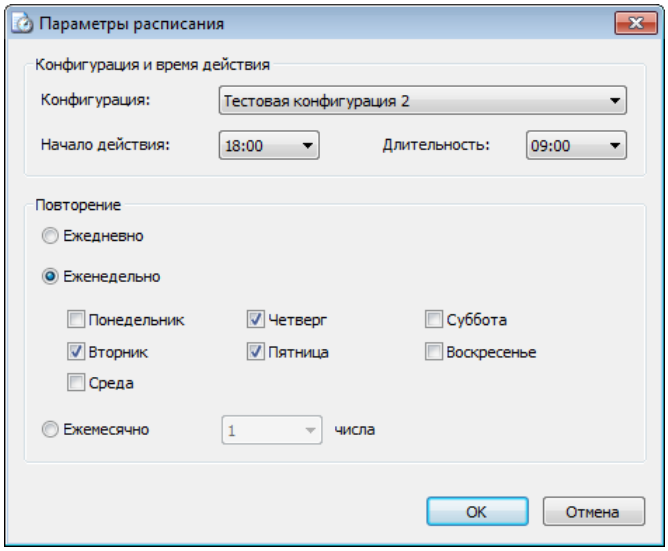


Рисунок 125: Настройка расписания смены конфигураций

3 Нажмите кнопку **OK**.

В результате расписание смены конфигураций будет настроено.

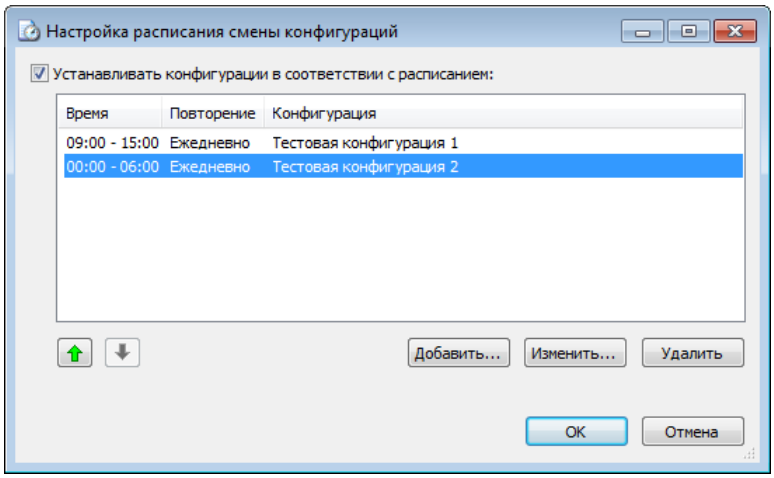


Рисунок 126: Сформированное расписание смены конфигураций

Чтобы установка конфигураций перестала производиться автоматически в соответствии с расписанием, в окне **Настройка расписания смены конфигурации** снимите соответствующий флажок.

Чтобы перед каждой сменой конфигурации по расписанию производилось оповещение, в настройках программы в разделе **Предупреждения** установите флажок **Выдавать предупреждение перед сменой конфигурации по расписанию**.

Запуск программы удаленного доступа

Программа ViPNet Монитор позволяет получить удаленный доступ к сетевому узлу ViPNet с помощью внешних программ, таких как Remote Administrator (Radmin), VNC или Remote Desktop Connection. Удаленный доступ к сетевому узлу может потребоваться администратору этого узла, если физический доступ к компьютеру затруднен, или пользователю, например, для работы на компьютере, находящемся в офисе, из дома.

Чтобы запустить программу удаленного доступа:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. Щелкните правой кнопкой мыши сетевой узел, к которому требуется получить удаленный доступ, в контекстном меню выберите пункт **Внешние программы**, затем выберите команду запуска нужной программы удаленного доступа.

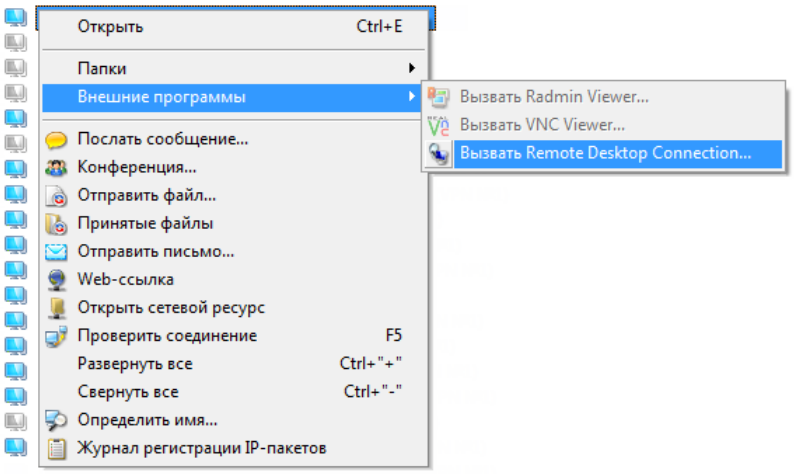


Рисунок 127: Вызов внешней программы

Команды подменю **Внешние программы** активны, только если на компьютере установлены соответствующие программы (см. «Установка программного обеспечения для удаленного управления» на стр. 296). Кроме того, выбранный сетевой узел должен иметь ненулевой IP-адрес доступа, и на этом узле должно быть установлено, запущено и настроено соответствующее серверное программное обеспечение (например, Radmin Server, VNC Server).

Примечание. При использовании программы Remote Desktop установка серверного программного обеспечения не требуется. С помощью Remote Desktop можно получить удаленный доступ к любому сетевому узлу ViPNet, работающему под управлением ОС Windows.

При соблюдении указанных условий откроется окно соединения. Если соединение установлено, появится окно ввода пароля доступа к выбранному узлу. После успешного ввода пароля откроется окно с отображением рабочего стола удаленного сетевого узла.

Примечание. Следует иметь в виду, что для успешного подключения к сетевому узлу ViPNet требуется правильно настроить используемое для удаленного доступа программное обеспечение.

Например, при использовании программы Remote Desktop на сетевом узле, к которому осуществляется подключение, должны быть выполнены следующие настройки:

- В свойствах системы должно быть разрешено удаленное подключение к компьютеру.
- Учетная запись внешнего пользователя должна быть добавлена в список удаленных пользователей.

Установка программного обеспечения для удаленного управления

Если вы хотите осуществлять удаленное подключение к сетевым узлам ViPNet с помощью внешних программ Remote Administrator (Radmin), VNC или Remote Desktop Connection, то убедитесь, что указанные программы установлены на вашем компьютере.

Получить установочные комплекты данных программ вы можете, загрузив их со следующих страниц:

- Remote Administrator — со страницы Radmin http://www.radmin.com/download/. Пакет Remote Administrator включает клиентскую и серверную части.
- VNC — со страницы RealVNC http://www.realvnc.com/download.html. Пакет VNC включает клиентскую и серверную части.
- Remote Desktop Connection — с веб-сайта Microsoft http://www.microsoft.com/ru-ru/download/details.aspx?id=856. Программа Remote Desktop Connection установлена

по умолчанию в операционных системах Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8. Устанавливать подключения можно с компьютеров, использующих любые версии указанных операционных систем. Однако подключаться можно только к компьютерам, использующим версии «Корпоративная», «Профессиональная» и «Максимальная». Подробная информация содержится на веб-сайте Microsoft http://windows.microsoft.com/ru-ru/windows-8/remote-desktop-connection-frequently-asked-questions.

Настройка терминального сервера при удаленном управлении

Во время работы в терминальной сессии (например, при подключении к серверу с помощью программы Remote Desktop Connection) может возникнуть ситуация, когда после выхода из терминальной сессии программа ViPNet Монитор автоматически выгружается из памяти удаленного сервера и защита IP-трафика отключается. Если это произойдет на координаторе, у всех сетевых узлов ViPNet, использующих этот координатор в качестве межсетевого экрана или сервера IP-адресов, возникнут сбои подключения.

Эта проблема возникает, если терминальный сервер настроен таким образом, чтобы завершать все приложения пользователя после его выхода из терминальной сессии. На рисунке ниже показаны настройки в оснастке **Настройка служб терминалов**, которые приводят к нежелательному завершению программы ViPNet Монитор.

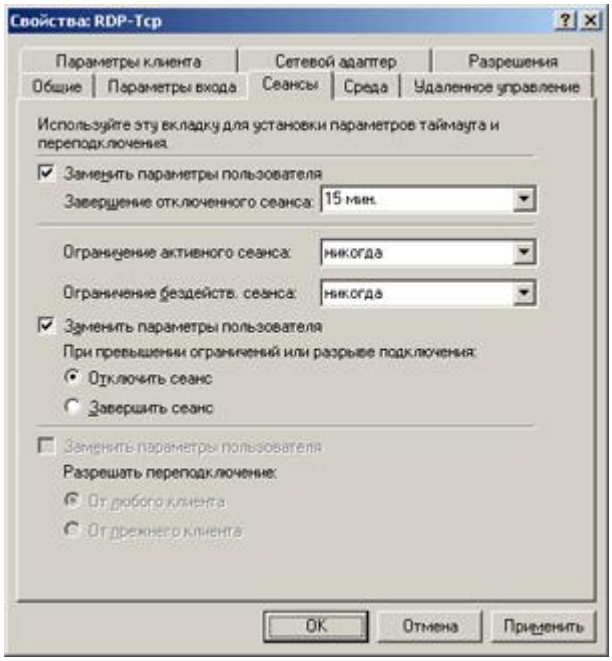


Рисунок 128: Неверные настройки терминального сервера

Для решения проблемы следует вернуть все настройки в состояние по умолчанию, сняв все флажки **Заменить параметры пользователя**.

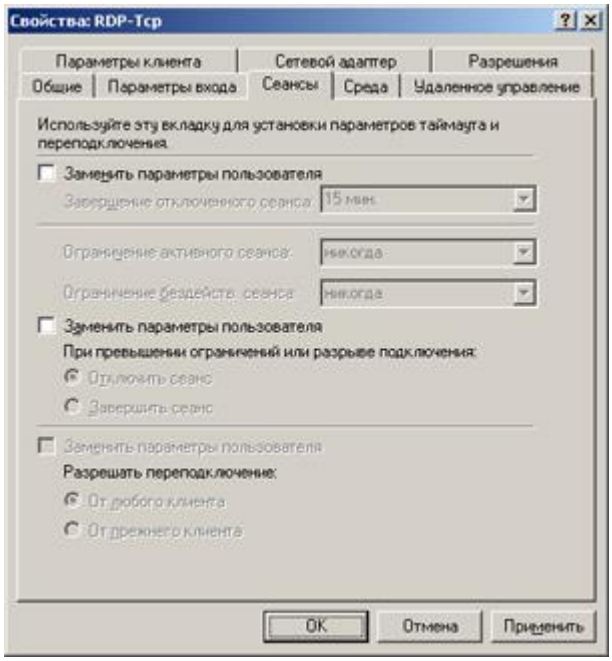


Рисунок 129: Верные настройки терминального сервера

Примечание. В операционной системе Windows Server 2008 R2 службы терминалов называются службами удаленных рабочих столов.

Настройка автоматического входа в ОС и программу ViPNet Монитор

При администрировании удаленных компьютеров или компьютеров, физический доступ к которым по каким-либо причинам затруднен, возникает необходимость после перезагрузки выполнять автоматический вход в операционную систему и запуск программы ViPNet Монитор. Это представляет определенные трудности, так как перед загрузкой операционной системы и инициализацией драйвера ViPNet требуется ввести пароль пользователя сетевого узла.

Чтобы на сетевом узле вход в систему и запуск программы ViPNet Монитор осуществлялся автоматически, выполните на нем следующие действия:

1. Настройте параметры автоматического входа в ОС Windows (см. «Настройка автоматического входа в ОС Windows» на стр. 300).
2. В программе ViPNet Монитор:
   - Настройте параметры сохранения пароля при входе в программу. Для этого войдите в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304). В меню **Сервис** выберите пункт **Настройка параметров безопасности** и в появившемся окне на вкладке **Администратор** установите флажок **Разрешить сохранение пароля в реестре** (см. «Дополнительные настройки параметров безопасности» на стр. 311).

     Примечание. Подразумевается, что на удаленном узле используется аутентификация пользователя по паролю (см. «Способы аутентификации пользователя» на стр. 80).

   - Включите опцию автоматической блокировки компьютера при запуске программы (см. «Настройка параметров запуска и аварийного завершения программы ViPNet Монитор» на стр. 316). Это поможет предотвратить несанкционированный доступ к компьютеру.

Внимание! Данные настройки должен выполнять пользователь, обладающий правами администратора в ОС Windows. При необходимости их можно

выполнить в удаленной сессии.

В результате для загрузки операционной системы и инициализации драйвера ViPNet не требуется никаких действий пользователя.

Настройка автоматического входа в ОС Windows

Для настройки автоматического входа в ОС Windows:

1. Нажмите сочетание клавиш **Win**+**R**.

   В меню **Пуск** (**Start**) также можно выбрать пункт **Выполнить** (**Run**).

2. В появившемся окне в поле **Открыть** (**Open**) введите команду `control userpasswords2` и нажмите кнопку **ОК**.

   При использовании ОС Windows Vista/Server 2008/Windows 7 также можно использовать команду `netplwiz`.

3. В окне **Учетные записи пользователей** (**User Accounts**) выполните следующие действия:

   - На вкладке **Пользователи** (**Users**) в списке выберите пользователя, под учетной записью которого будет осуществляться вход в ОС и снимите флажок **Требовать ввод имени пользователя и пароля** (**Users must enter a username and password to use this computer**).

     Пользователь в данном случае должен принадлежать группе **Administrators** (должен быть зарегистрирован как администратор компьютера).

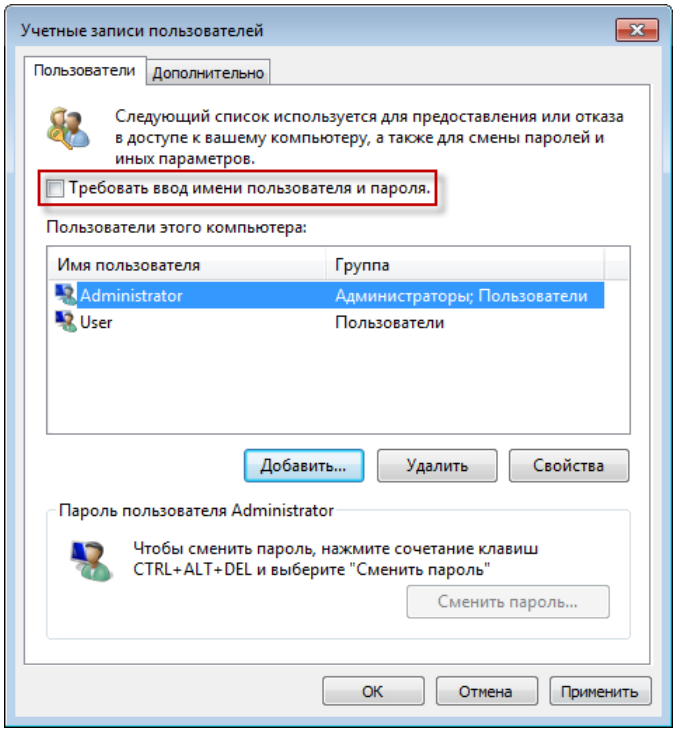


Рисунок 130: Настройка автоматического входа в ОС на вкладке Пользователи

- На вкладке **Дополнительно** (**Advanced**) снимите флажок **Требовать нажатия CTRL+ALT+DELETE** (**Require users to press Ctrl+Alt+Delete**).

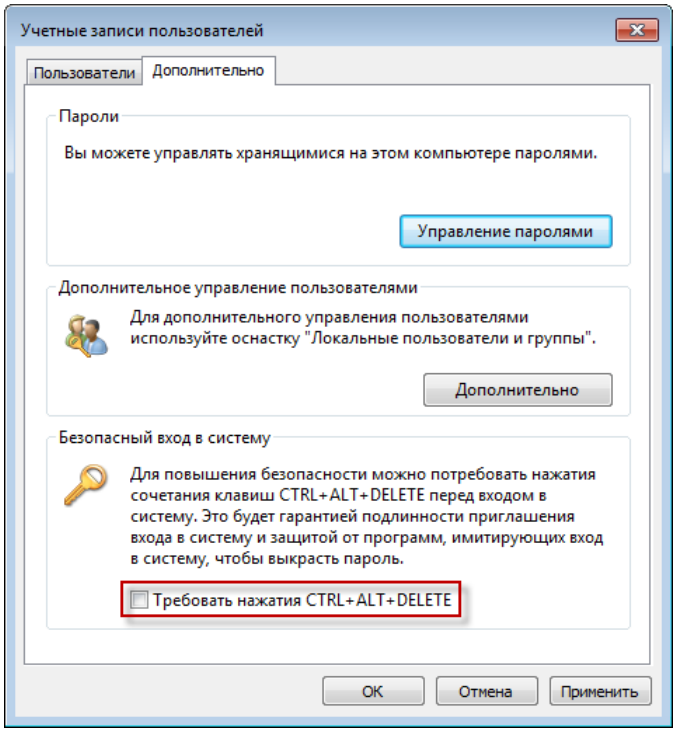


Рисунок 131: Настройка автоматического входа в ОС на вкладке Дополнительно

Примечание. Если компьютер находится в домене, то указанные флажки могут отсутствовать или быть недоступными в соответствии с групповой политикой безопасности. В этом случае для настройки автоматического входа в ОС потребуется правка реестра вручную.

Неправильное редактирование реестра может привести к возникновению неполадок в работе операционной системы, поэтому обязательно создайте резервную копию реестра. Это позволит восстановить реестр при возникновении неполадок.

Если отсутствует или недоступен флажок **Требовать ввод имени пользователя и пароля (Users must enter a username and password to use this computer**), то в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` задайте следующие значения параметрам:

- `AutoAdminLogon` — 1 («истина»). Данный параметр необходим для включения опции автоматического входа в ОС. При значении 0 автоматический вход в ОС выключен.
- `DefaultDomainName` — имя домена, в который входит компьютер пользователя.
- `DefaultUserName` — имя пользователя, под учетной записью которого будет осуществлять автоматический вход в ОС.

- `DefaultPassword` — пароля пользователя. Если значение этому параметру не будет присвоено, то значение параметра `AutoAdminLogon` автоматически изменится на 0 («ложь»), что не позволит осуществлять автоматический вход в ОС.

При отсутствии указанных параметров создайте их вручную, используя строковый тип (**REG_SZ**).

Если отсутствует или недоступен флажок **Требовать нажатия CTRL+ALT+DELETE (Require users to press Ctrl+Alt+Delete)**, то в разделе ветки реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` параметру `Disablecad` присвойте значение 1 («истина»). При отсутствии данного параметра создайте его вручную, используя тип **DWORD**.

- Нажмите кнопку **Применить** (**Apply**).

4 В окне **Автоматический вход в систему** (**Automatically Log On**) введите пароль и нажмите кнопку **ОК**.

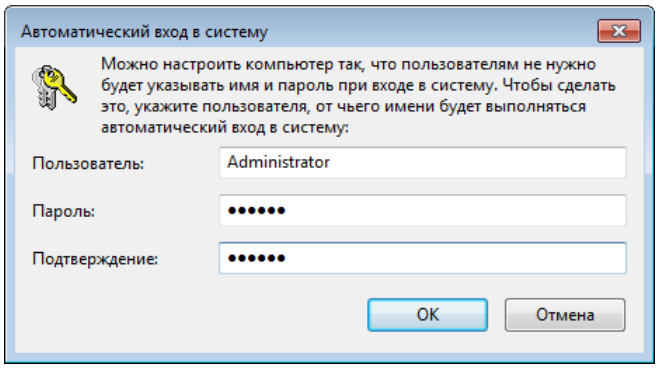


Рисунок 132: Окно ввода пароля для автоматического входа в систему

В результате при последующих запусках компьютера вход в ОС будет производиться под учетной записью выбранного пользователя, без ввода пароля и нажатия сочетания клавиш **Ctrl**+**Alt**+**Delete**.

Работа в программе в режиме администратора

В программе ViPNet Монитор предусмотрена возможность работы в режиме администратора. В данном режиме доступны следующие дополнительные функции и настройки:

- Раздел **Администратор**, который появляется на панели навигации главного окна программы и в котором можно выполнить дополнительную настройку сетевого узла ViPNet (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305).
- Журнал событий, содержащий записи о различных действиях, совершенных пользователем или администратором (см. «Просмотр журнала событий» на стр. 313).
- Возможность просмотреть журнал IP-пакетов определенного сетевого узла ViPNet (см. «Просмотр журнала IP-пакетов другого сетевого узла» на стр. 285).
- Возможность просмотра и изменения конфигураций программы ViPNet Монитор (см. «Управление конфигурациями программы» на стр. 291), созданных всеми пользователями сетевого узла.

При работе в режиме администратора снимаются все ограничения, накладываемые уровнем полномочий пользователя.

Чтобы войти в программу в режиме администратора:

1. Выполните одно из действий:
   - В окне программы ViPNet Монитор в меню **Файл** выберите пункт **Войти в режим администратора**.
   - В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка параметров безопасности**.

     В окне **Настройка параметров безопасности** откройте вкладку **Администратор** и нажмите кнопку **Вход в режим администратора**.
2. В окне **Вход в режим администратора** введите пароль администратора сетевого узла ViPNet.

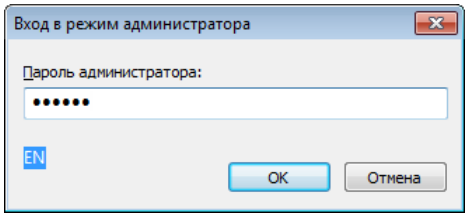


Рисунок 133: Ввод пароля администратора сетевого узла

3 Нажмите кнопку **OK**.

Если введен верный пароль, будет выполнен перезапуск программы и станут доступны дополнительные настройки.

Внимание! В сети ViPNet CUSTOM пароли администратора для каждого сетевого узла создаются в программе ViPNet Удостоверяющий и ключевой центр.

В сети ViPNet VPN пароль администратора для всех сетевых узлов хранится в файле `ViPNet_a.txt`, который автоматически создается в папке с наборами ключей при их сохранении.

Дополнительные настройки программы ViPNet Монитор

После входа в ViPNet Монитор в режиме администратора сетевого узла на панели навигации окна программы появляется раздел **Администратор**. В этом разделе можно настроить ряд дополнительных параметров. Для настройки этих параметров:

1 Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304).

2 В окне программы ViPNet Монитор на панели навигации выберите раздел **Администратор**.

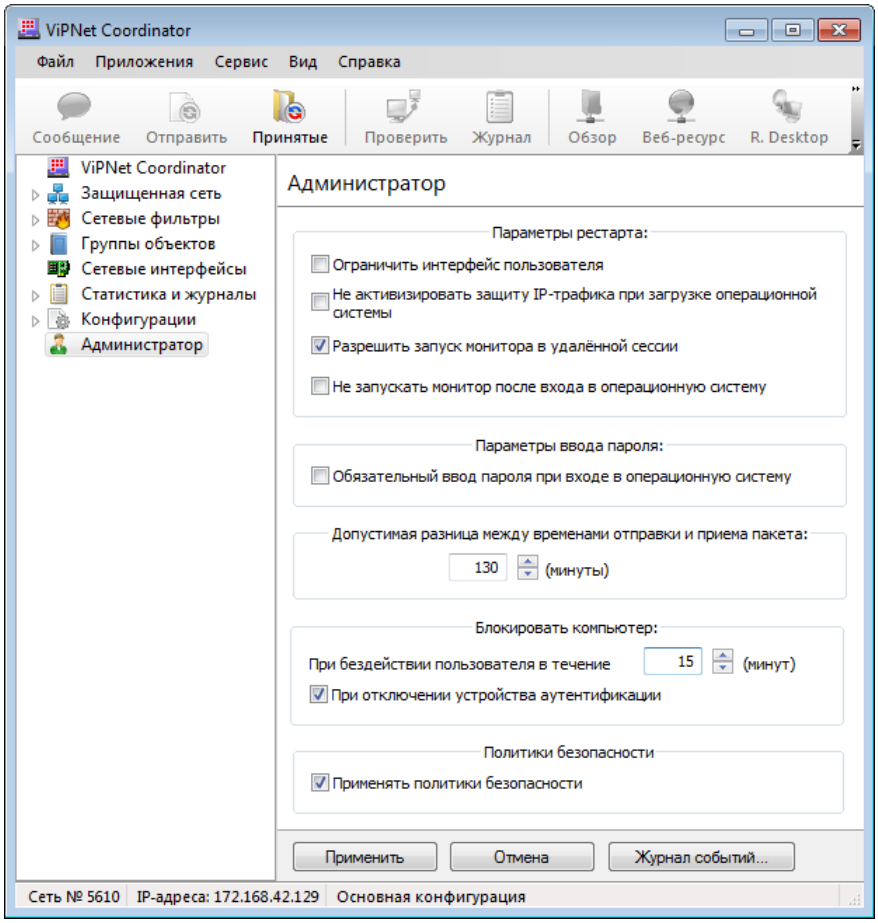


Рисунок 134: Настройка дополнительных параметров в режиме администратора

3 Для изменения параметров программы ViPNet Монитор следуйте указаниям следующих разделов:

- Ограничение интерфейса пользователя (на стр. 306).
- Параметры запуска программы (на стр. 308).
- Параметры блокировки компьютера (на стр. 309).
- Параметры защиты трафика (на стр. 310).

4 Чтобы сохранить настройки, нажмите кнопку **Применить**. Чтобы отказаться от изменений, нажмите кнопку **Отмена**.

Ограничение интерфейса пользователя

Если вы хотите ограничить возможность изменения параметров программы ViPNet Монитор и скрыть панели навигации, в разделе **Администратор** (см. «Дополнительные

настройки программы ViPNet Монитор» на стр. 305) установите флажок **Ограничить интерфейс пользователя**.

Примечание. Если для сетевого узла задан специальный уровень полномочий 3, данный флажок установлен по умолчанию и его невозможно снять.

Если этот флажок установлен, в программе ViPNet Монитор действуют следующие ограничения:

- В окне программы отображается только панель просмотра со списком сетевых узлов ViPNet.
- В меню **Файл** отсутствует пункт **Сменить пользователя**, но при этом доступны пункты **Сменить пароль пользователя** и **Сменить способ аутентификации пользователя**. Сменить пароль можно только на случайный пароль на основе парольной фразы.

  Пункт **Конфигурации** в меню **Файл** присутствует только в том случае, если в программе создано несколько конфигураций. С помощью данного пункта можно только переключать конфигурации. Пункты **Отключить защиту** и **Блокировать IP-трафик** в нем отсутствуют.

  Пользователь не имеет возможности создавать новые конфигурации. Если в режиме администратора сетевого узла будут созданы новые конфигурации, то они будут доступны пользователю. Если сетевой узел имеет связь с сервером открытого Интернета, на этом узле доступна конфигурация «Открытый Интернет».
- Недоступен пункт меню **Сервис**, в связи с этим невозможно изменение, сохранение и восстановление настроек программы ViPNet Монитор, а также изменение настроек параметров безопасности.
- В окне **Проверка соединения** отображаются только столбцы **Узел, Статус** и **Активность на компьютере.**
- Программа ViPNet MFTP запускается и работает в скрытом режиме. Открыть программу из меню **Приложения** нельзя, соответственно, ее настройка также невозможна.

Параметры запуска программы

Чтобы изменить дополнительные параметры запуска программы ViPNet Монитор, в разделе **Администратор** (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305) выполните следующие действия:

- Если вы хотите, чтобы после загрузки операционной системы Windows защита трафика с помощью программного обеспечения ViPNet была отключена, установите флажок **Не активизировать защиту IP-трафика при загрузке операционной системы**. В этом случае при загрузке Windows не будет выполняться аутентификация пользователя ViPNet и автоматический запуск программы ViPNet Монитор, компьютер не будет защищен. Однако для включения защиты трафика вы можете вручную запустить программу ViPNet Монитор.

  Примечание. Не рекомендуется устанавливать этот флажок на координаторах, а также на клиентах, которые имеют динамический IP-адрес или должны взаимодействовать с узлами, имеющими динамический IP-адрес.

- Если вы хотите запретить пользователям, имеющим учетные записи на данном компьютере, запускать программу ViPNet Монитор во время сеанса удаленной работы (например, с помощью Remote Desktop), снимите флажок **Разрешить запуск монитора в удаленной сессии**. По умолчанию этот флажок установлен.

  Эта функция доступна, только если на компьютере установлено программное обеспечение для удаленной работы.

  Примечание. На компьютере может быть запущен только один экземпляр программы ViPNet Монитор. Если программа запущена в сеансе работы другого пользователя, с помощью Диспетчера задач Windows завершите процесс `Monitor.exe`, затем запустите программу ViPNet Монитор.

- Если вы хотите, чтобы после загрузки Windows защита трафика была включена, но программа ViPNet Монитор не запускалась, установите флажок **Не запускать монитор после входа в операционную систему**. В этом случае после загрузки Windows будет загружен только ViPNet-драйвер, защита компьютера будет активна.
- Если вы хотите, чтобы при загрузке Windows пользователь не мог отказаться от запуска программы ViPNet Монитор, установите флажок **Обязательный ввод пароля при входе в операционную систему**. В этом случае в окне входа в программу кнопка **Отмена** будет недоступна.

Примечание. Если установлен флажок **Не активизировать защиту IP-трафика при загрузке операционной системы**, параметр **Обязательный ввод пароля при входе в операционную систему** не учитывается.

Параметры блокировки компьютера

Если требуется, в разделе **Администратор** (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305) в группе **Блокировать компьютер** вы можете изменить параметры блокировки компьютера:

- По умолчанию в программе ViPNet Монитор включена автоматическая блокировка компьютера в случае бездействия пользователя. Если в течение заданного интервала времени не будут использоваться клавиатура и мышь, компьютер будет автоматически заблокирован.

  При необходимости в поле **При бездействии пользователя в течение** измените продолжительность интервала блокировки в минутах (по умолчанию задано значение 15 минут). Чтобы отключить автоматическую блокировку компьютера, укажите значение интервала блокировки, равное 0.

- По умолчанию в программе ViPNet Монитор включена автоматическая блокировка компьютера при отключении внешнего устройства, которое было использовано для аутентификации пользователя. Если вы хотите отключить блокировку компьютера при отключении внешнего устройства, снимите флажок **При отключении устройства аутентификации**.

  Блокировка компьютера при отключении устройства аутентификации действуют только в случае использования способов аутентификации «Пароль на устройстве» и «Устройство» (см. «Способы аутентификации пользователя» на стр. 80). Если используются внешние устройства iButton, Smartcard Athena, Аккорд-5MX (см. «Внешние устройства» на стр. 438), то функция автоматической блокировки не действует.

  Чтобы продолжить работу после автоматической блокировки, необходимо подключить внешнее устройство, ввести пароль пользователя Windows и, не изменяя способ аутентификации, ввести ПИН-код и пароль (если требуется).

Внимание! Для снятия блокировки требуется подключить именно то устройство, которое использовалось для входа в программу, и использовать тот же способ аутентификации. При подключении другого устройства или выборе другого способа аутентификации снять блокировку будет невозможно.

Параметры защиты трафика

При необходимости в разделе **Администратор** (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305) вы можете изменить дополнительные параметры защиты IP-трафика:

- Программное обеспечение ViPNet автоматически блокирует входящие IP-пакеты, если разница между временем их отправки и временем приема больше заданного значения. Действие данной функции распространяется на сетевые узлы ViPNet, с которыми у данного узла есть связь (эти узлы отображаются в разделе **Защищенная сеть**).

  Если требуется, в поле **Допустимая разница между временами отправки и приема пакета** измените допустимый интервал времени между отправкой и приемом пакета в минутах (по умолчанию 120 минут).

Внимание! В результате действия данной функции могут быть заблокированы входящие IP-пакеты от сетевых узлов, на которых неправильно установлено системное время.

- При необходимости вы можете отменить на сетевом узле действие политик безопасности, полученных из программы ViPNet Policy Manager. Для этого в группе **Политики безопасности** снимите флажок **Применять политики безопасности.** Например, вы можете отменить действие политик безопасности, чтобы временно отключить ошибочно отправленные на узел сетевые фильтры.

  Если флажок **Применять политики безопасности** будет снят, действие уже принятых политик безопасности будет прекращено (сетевые фильтры, которые были получены в составе политик, будут скрыты и перестанут использоваться), на узел ViPNet Policy Manager будет отправлена информация о том, что на данном узле не будут приниматься новые политики безопасности.

  Если флажок **Применять политики безопасности** впоследствии будет повторно установлен, то действие уже принятых политик и получение новых политик из программы ViPNet Policy Manager будет возобновлено.

Дополнительные настройки параметров безопасности

Помимо дополнительных параметров настройки в разделе **Администратор**, во время работы в режиме администратора сетевого узла (см. «Работа в программе в режиме администратора» на стр. 304) доступны следующие параметры на вкладке **Администратор** в окне **Настройка параметров безопасности**:

- **Разрешить сохранение пароля в реестре** — позволяет пользователю сетевого узла установить флажок **Сохранить пароль** при входе в программу ViPNet Монитор. Если этот флажок установлен, пароль пользователя хранится в реестре Windows и автоматически подставляется в поле ввода пароля при запуске программы ViPNet Монитор.

Примечание. Если для управления сетью ViPNet используется программа ViPNet Network Manager, изменить состояние флажка **Разрешить сохранение пароля в реестре** невозможно. Чтобы изменить этот параметр, обратитесь к администратору сети ViPNet.

Для сетей ViPNet CUSTOM такая функциональность не предусмотрена.

- **Автоматически входить в ViPNet** — позволяет выполнять вход в ПО ViPNet Монитор без необходимости подтверждения пароля пользователя ViPNet в окне входа в программу. Если флажок установлен, при запуске программы на текущем сетевом узле окно входа в программу не появляется и вход в ПО ViPNet Монитор выполняется автоматически. Это происходит в следующих случаях:
  - при использовании способа аутентификации **Пароль** — если пароль сохранен в реестре, то есть установлен флажок **Разрешить сохранение пароля в реестре**, а в окне входа в программу указан верный пароль и установлен флажок **Сохранить пароль**;
  - при использовании способов аутентификации **Пароль на устройстве** и **Устройство** — если внешнее устройство подключено к компьютеру и в окне входа в программу указан верный ПИН-код и установлен флажок **Сохранить ПИН-код**.
- **Разрешить использование внешних сертификатов** — позволяет использовать сертификаты не только из личного хранилища (хранилища программы), но также из хранилища операционной системы. Это может понадобиться в том случае, если в ПО ViPNet предполагается использовать криптопровайдер другого производителя (например, КриптоПро), а также сертификаты, изданные внешними Удостоверяющими центрами (вне сети ViPNet).

- **Доверять только сертификатам администраторов УЦ ViPNet** — если этот флажок снят, при проверке сертификата поиск корневого сертификата выполняется не только во внутреннем хранилище ПО ViPNet, но и в системных хранилищах **Доверенные корневые центры сертификации** и **Промежуточные центры сертификации**.

- **Игнорировать отсутствие списков отозванных сертификатов** — этот флажок следует установить, если в системе используются сертификаты, изданные внешними Удостоверяющими центрами, так как в таких сертификатах информация о списках отозванных сертификатов может отсутствовать.

Изменение способа аутентификации пользователя

Способ аутентификации определяет, какие данные должен предоставить пользователь для входа в программу ViPNet Монитор. Чтобы изменить способ аутентификации пользователя, выполните следующие действия:

1 Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304).

2 В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите кнопку **Изменить**.

3 В окне **Способ аутентификации** выберите один из способов аутентификации. Описание возможных способов аутентификации пользователя приведено в разделе Способы аутентификации пользователя (на стр. 80).

Примечание. Способ **Пароль на устройстве** выбрать нельзя, поскольку он перестал отвечать требованиям безопасности.

При выборе способа аутентификации по сертификату подключите внешнее устройство и укажите нужный сертификат в списке сертификатов, обнаруженных на устройстве. При возникновении затруднений в выборе сертификата см. раздел Не удается выполнить аутентификацию с помощью сертификата (на стр. 371).

При выборе способа аутентификации по персональному ключу подключите внешнее устройство для сохранения на нем персонального ключа пользователя (см. «Симметричные ключи в ПО ViPNet» на стр. 413). При сохранении персонального ключа (ключа защиты (см. «Ключ защиты» на стр. 485)) на устройство стоит учитывать следующую особенность. Если пользователь производит процедуры подписи и шифрования внутри сторонних приложений (например, в Microsoft Office), то в этом случае настоятельно рекомендуется его контейнер ключей (на стр.

485) сохранять также на этом устройстве. Иначе подписание и шифрование в сторонних приложениях будет невозможно из-за проблемы с доступом к ключу защиты. Контейнер ключей можно также перенести из текущей папки в другую папку на диске, но в этом случае каждый раз при подписании и шифровании в стороннем приложении вам потребуется вводить пароль.

Внимание! Если при использовании способа аутентификации **Устройство** внешнее устройство будет отключено, компьютер может быть автоматически заблокирован — в соответствии с настройками, заданными в режиме администратора (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305). Для продолжения работы необходимо вновь подключить это внешнее устройство. При необходимости параметры автоматической блокировки компьютера и IP-трафика могут быть изменены.

4 Нажмите кнопку **OK**.

На вкладке **Ключи** в группе **Аутентификация** значения полей **Способ аутентификации** и **Тип носителя** изменятся в соответствии с выбранным режимом.

В сетях ViPNet CUSTOM способ аутентификации также может изменить администратор сети в программе ViPNet Удостоверяющий и ключевой центр. Если администратор назначает пользователю способ аутентификации по сертификату, то пользователь в данном случае должен предоставить администратору внешнее устройство с сертификатом и закрытым ключом для регистрации. При этом должны быть соблюдены условия, описанные в примечании в разделе Устройство (на стр. 84). После назначения пользователю нового способа аутентификации администратор вышлет обновление ключей узла. Приняв данное обновление ключей, пользователь сможет выполнить аутентификацию на узле только выбранным способом.

Просмотр журнала событий

В журнале событий регистрируются действия по изменению настроек программы ViPNet Coordinator:

- Изменение сетевых фильтров.
- Вход пользователя в программу и его выход.
- Вход в режиме администратора.
- Смена конфигурации.

- Другие события.

Данная информация позволяет администратору контролировать соблюдение безопасности.

Для просмотра журнала событий:

1. Выполните вход в программу в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304).
2. В окне программы ViPNet Монитор на панели навигации выберите раздел **Администратор**.
3. В разделе **Администратор** нажмите кнопку **Журнал событий**.

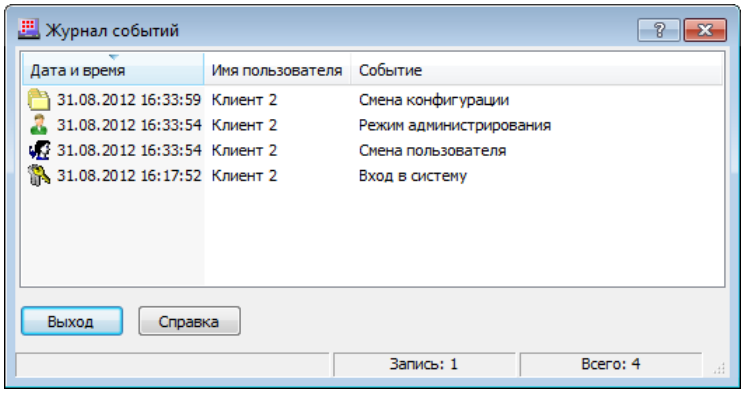


Рисунок 135: Просмотр журнала событий

4. Для просмотра журнала событий в формате HTML или XLS в окне **Журнал событий** щелкните любую строку правой кнопкой мыши и в контекстном меню выберите **Просмотр в HTML-формате** или **Просмотр в XLS-формате** (для просмотра журнала в формате XLS на компьютере должна быть установлена программа Microsoft Excel).

Информация о фиксируемых в журнале событиях представлена в таблице ниже:

Столбец	Описание
Дата и время	Когда произошло событие.
Имя пользователя	Кто являлся инициатором события.
Событие	Расшифровка событий: • Вход в систему.

-  Выход из системы.
-  Режим администратора — при входе в программу в режиме администратора.
-  Попытка входа в систему отвергнута (имя пользователя не установлено) — появляется в случае трехкратного неверного ввода пароля пользователя.
-  Попытка входа администратора в систему отвергнута (имя пользователя не установлено) — появляется в случае трехкратного неверного ввода пароля администратора.
-  Технологический перезапуск — перезагрузка программы после принятия файлов обновления.
-  Технологический перезапуск — перезагрузка программы после аварийного завершения.
-  Смена пользователя — вход в программу другого пользователя, зарегистрированного на данном сетевом узле.
-  Смена конфигурации — смена конфигурации программы в разделе **Конфигурации**.
-  Изменение фильтра — любые действия по созданию, редактированию или удалению фильтров.
-  Включение или выключение функции «Блокировать все протоколы кроме IP, ARP» — установка или снятие флажка **Блокировать все протоколы, кроме IP, ARP** в окне **Настройка** в разделе **Управление трафиком**.
-  Включение или выключение функции «Блокировать компьютер» — установка или снятие флажка **Блокировать компьютер** в окне **Настройка** в разделе **Общие > Запуск и аварийное завершение**..
-  Изменение правила NAT — любые действия по созданию, редактированию или удалению правила трансляции IP-адресов.
-  Изменение порядка правил NAT — изменение приоритета выполнения правил трансляции адресов.
-  Включение или выключение антиспуфинга.

Настройка параметров запуска и аварийного завершения программы ViPNet Монитор

Для настройки параметров запуска и экстренного завершения программы:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.

2. В окне **Настройка** на панели навигации выберите раздел **Общие** > **Запуск и аварийное завершение**.

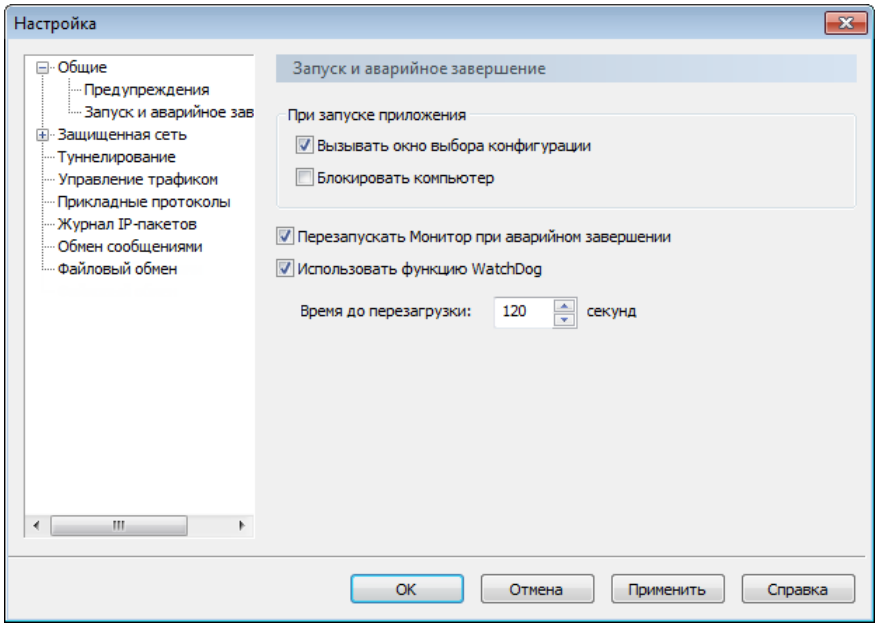


Рисунок 136: Настройка параметров запуска и аварийного завершения работы программы

3. Чтобы при запуске программы не производить выбор конфигурации (см. «Управление конфигурациями программы» на стр. 291), снимите флажок **Вызывать окно выбора конфигурации**. При этом запуск программы будет происходить в той конфигурации, которая использовалась в последнем сеансе работы.

Если в программе настроена только одна конфигурация, окно выбора появляться не будет независимо от установки флажка.

4 Чтобы при запуске программы блокировать доступ к рабочему столу компьютера, установите флажок **Блокировать компьютер**. Для разблокирования компьютера введите пароль пользователя Windows.

Данная функция полезна для предотвращения несанкционированной работы с компьютером после его перезагрузки, если настроен автоматический вход пользователя Windows в операционную систему. При этом программа ViPNet Монитор выполняет все функции по защите компьютера.

5 Чтобы отключить возможность перезапуска ViPNet Монитор после аварийного завершения работы программы, снимите флажок **Перезапускать Монитор при аварийном завершении**.

6 Для включения автоматической перезагрузки ОС при сбоях установите флажок **Использовать функцию WatchDog** и в поле **Время до перезагрузки** введите время (в секундах), по истечении которого будет происходить перезагрузка.

Функция WatchDog отслеживает работоспособность программы ViPNet Монитор. Если программа теряет работоспособность в результате какого-либо системного сбоя, WatchDog перезагружает ОС компьютера. Использование WatchDog особенно важно на удаленных компьютерах, доступ к которым проблематичен.

Примечание. В 64-разрядных операционных системах функция WatchDog не поддерживается.

18

Настройка параметров безопасности

Смена пароля пользователя

Пароль пользователя рекомендуется менять раз в 3 месяца. В целом же частота смены пароля пользователя определяется регламентом безопасности организации.

Смена текущего пароля пользователя требуется в следующих случаях:

- По истечении срока действия текущего пароля (в случае, если этот срок действия ограничен).
- При поступлении на сетевой узел обновления ключей из программы ViPNet Удостоверяющий и ключевой центр, содержащего новый пароль пользователя. В этом случае появится окно с сообщением «Рекомендуется сменить пароль пользователя», однако пароль не будет изменен автоматически, поэтому процедуру смены пароля необходимо выполнить вручную.
- Если контейнер ключей защищен с использованием не пароля, а персонального ключа пользователя, пароль к контейнеру ключей будет совпадать с паролем пользователя. Поэтому при необходимости смены пароля к контейнеру ключей (см. «Смена пароля к контейнеру» на стр. 359), следует сменить пароль пользователя.

Кроме того, рекомендуется менять пароль пользователя при первом входе в программу после установки справочников и ключей. Это повысит надежность пароля, поскольку он не будет известен администратору.

Для того чтобы сменить пароль пользователя:

1 В окне **Настройка параметров безопасности** откройте вкладку **Пароль.**

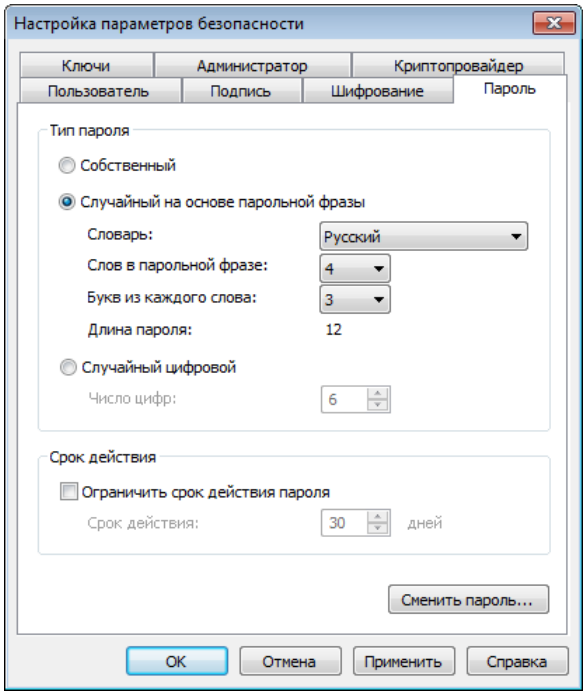


Рисунок 137: Смена текущего пароля пользователя

2 В группе **Тип пароля** выберите тот тип, которому должен соответствовать новый пароль:

- **Собственный** — пароль, определяемый пользователем (см. «Выбор собственного пароля» на стр. 321);
- **Случайный на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы, по заданным параметрам (см. «Выбор пароля на основе парольной фразы» на стр. 321);
- **Случайный цифровой** — пароль, формируемый автоматически из заданного числа цифр (см. «Выбор цифрового пароля» на стр. 322).

3 Нажмите кнопку **Сменить пароль.** Дальнейшие действия по смене пароля зависят от выбранного типа пароля и описаны в соответствующем разделе.

4 При необходимости ограничения срока действия нового пароля установите флажок **Ограничить срок действия пароля**, после чего укажите желаемое число дней.

5 Нажмите кнопку **ОК.**

Выбор собственного пароля

Для того чтобы сменить текущий пароль пользователя на собственный:

1. На вкладке **Пароль** (см. Рисунок 137 на стр. 320) выберите **Собственный.**
2. Нажмите кнопку **Сменить пароль.**
3. Выполните действия, предлагаемые в окне **Электронная рулетка.**

> **Примечание.** Если в рамках текущего сеанса электронная рулетка уже была запущена, данное окно не появится.

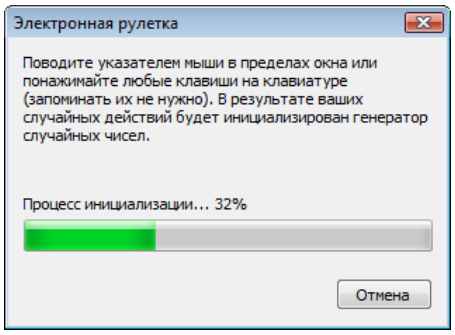


Рисунок 138: Электронная рулетка

4. В окне **Смена пароля** введите новый пароль (длиной не менее шести символов) поочередно в каждом из полей, учитывая регистр и раскладку клавиатуры.

   Нажмите кнопку **ОК.**

Теперь при запуске программы ViPNet Монитор от имени того же пользователя следует вводить указанный пароль.

Выбор пароля на основе парольной фразы

Для того чтобы сменить текущий пароль на случайный, составленный на основе парольной фразы:

1. На вкладке **Пароль** (см. Рисунок 137 на стр. 320) выберите **Случайный на основе парольной фразы**, после чего задайте параметры нового пароля:
   - В списке **Словарь** выберите язык парольной фразы.

- В списке **Слов в парольной фразе** выберите число слов (3, 4, 6 или 8), из которых будет состоять парольная фраза. Чем больше число слов, тем длиннее и, соответственно, надежнее будет пароль.
- В списке **Букв из каждого слова** выберите число начальных букв каждого слова (3 или 4), которые войдут в пароль.

В строке **Длина пароля** отобразится количество букв в пароле, который будет сформирован с учетом указанных параметров.

2 Нажмите кнопку **Сменить пароль**.

3 Запомните пароль (или парольную фразу), отображенный в окне **Смена пароля**.

При необходимости измените парольную фразу и пароль на другие, также соответствующие указанным параметрам, с помощью кнопки **Другой пароль**.

Нажмите кнопку **ОК**.

Теперь при запуске программы ViPNet Монитор от имени того же пользователя следует, используя английскую раскладку клавиатуры, вводить указанное число букв каждого слова русской парольной фразы, без пробелов. Например, для парольной фразы «тенор победил горемыку» с параметрами пароля по умолчанию (3 буквы из каждого слова) при запуске программы следует, используя английскую раскладку клавиатуры, вводить буквы «тенпобгор».

Выбор цифрового пароля

Для того чтобы сменить текущий пароль пользователя на цифровой:

1 На вкладке **Пароль** (см. Рисунок 137 на стр. 320) выберите **Случайный цифровой**, после чего в поле **Число цифр** укажите длину пароля.

2 Нажмите кнопку **Сменить пароль**.

3 Запомните цифровой пароль, предложенный в окне **Смена пароля**.

При необходимости измените этот пароль на другой, также содержащий указанное число цифр, с помощью кнопки **Другой ПИН-код**.

Нажмите кнопку **ОК**.

Теперь при запуске программы ViPNet Монитор от имени того же пользователя следует вводить предложенный цифровой пароль.

Настройка параметров шифрования

Вы можете настроить параметры шифрования исходящей информации. Для этого выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Шифрование**.

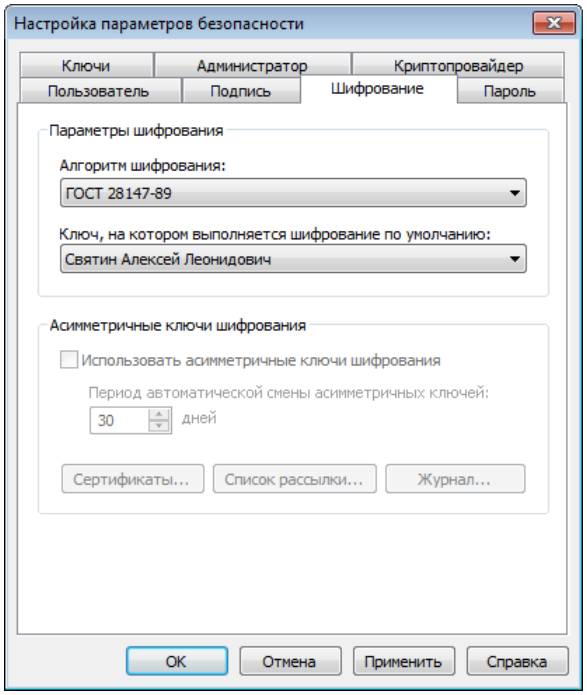


Рисунок 139: Настройка параметров шифрования

2 В списке **Алгоритм шифрования** выберите алгоритм, по которому будет осуществляться шифрование исходящей информации:

- ГОСТ 28147-89 (длина ключа 256 бит) — российский стандарт симметричного шифрования.
- AES (256 бит) — принятый в США стандарт симметричного шифрования на основе алгоритма Rijndael.

По умолчанию выбран алгоритм ГОСТ 28147-89. В соответствии с выбранным алгоритмом будет осуществляться как шифрование исходящего трафика, так и шифрование информации, передаваемой с помощью встроенных приложений ViPNet (например, программой ViPNet Деловая почта).

Внимание! В сертифицированной версии программы алгоритм AES не поддерживается, возможность его выбора отсутствует.

3 В следующем списке укажите ключи, на которых должно выполняться шифрование информации, передаваемой с помощью встроенных приложений ViPNet. Для шифрования могут быть выбраны как ключи, доступ к которым имеете только вы, так и ключи, доступные другим пользователям вашего узла (если такие есть). Просмотреть список пользователей, имеющих доступ к каким-либо ключам шифрования, вы можете на вкладке **Пользователь.**

Выбор ключей шифрования позволяет разграничить доступ пользователей, работающих на одном сетевом узле, к зашифрованной информации (например, письмам программы ViPNet Деловая почта). То есть если исходящее сообщение было зашифровано на ключах, доступных только вам, то другие пользователи, зарегистрированные на вашем узле, его прочитать не смогут.

4 Нажмите кнопку **OK**.

Настройка параметров криптопровайдера ViPNet CSP

В состав программного обеспечения ViPNet Coordinator включена программа ViPNet CSP. ViPNet CSP представляет собой криптопровайдер, который обеспечивает вызов криптографических функций, реализованных в соответствии с российскими стандартами, через интерфейс Microsoft CryptoAPI 2.0. Это позволяет использовать российские криптографические алгоритмы в различных приложениях Microsoft и других программах, использующих данный интерфейс. Кроме этого, программа ViPNet CSP обеспечивает работу с контейнерами ключей (см. «Контейнер ключей» на стр. 485) и поддержку различных внешних устройств хранения ключей (см. «Внешние устройства» на стр. 438).

Чтобы настроить программу ViPNet CSP или задать параметры автоматической установки сертификатов в системное хранилище, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Криптопровайдер**.

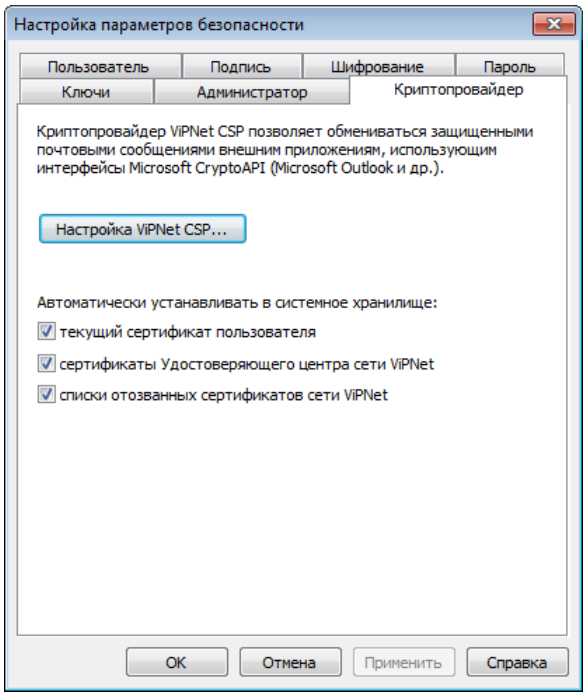


Рисунок 140: Настройка параметров криптопровайдера

2 Чтобы настроить программу ViPNet CSP, нажмите кнопку **Настройка ViPNet CSP**. Откроется окно **ViPNet CSP**, в котором вы можете:

- Задать необходимые параметры криптопровайдера.
- Выполнить операции с контейнерами ключей.
- Настроить параметры использования внешних устройств хранения данных — задать типы устройств, которые могут использоваться, выполнить инициализацию или изменить ПИН-код устройства.

Подробнее о настройке и работе с программой ViPNet CSP см. документ «ViPNet CSP. Руководство пользователя».

3 При необходимости укажите, какие сертификаты и списки отозванных сертификатов следует устанавливать в системное хранилище автоматически (см. «Установка в хранилище автоматически» на стр. 334), установив нужные флажки:

- **текущий сертификат пользователя** — для установки в системное хранилище Windows сертификата, который был назначен текущим;
- **сертификаты Удостоверяющего центра сети ViPNet —** для установки в системное хранилище Windows сертификатов издателей (корневых сертификатов), получаемых из программы ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager в составе обновления ключей;
- **списки отозванных сертификатов сети ViPNet** — для установки в системное хранилище списков отозванных сертификатов, получаемых из программы ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager в составе обновления ключей.

4 Выполнив необходимые настройки, нажмите кнопку **OK**.

19

Работа с сертификатами и ключами

Просмотр сертификатов

Просмотр сертификата может потребоваться при необходимости получения более подробной информации о сертификате — о назначении сертификата, о его издателе, составе полей, причине недействительности сертификата и так далее.

В программе ViPNet Coordinator можно просматривать следующие типы сертификатов:

- текущий сертификат пользователя (см. «Просмотр текущего сертификата пользователя» на стр. 329),
- личные сертификаты пользователя (см. «Просмотр личных сертификатов пользователя» на стр. 329),
- доверенные корневые сертификаты (см. «Просмотр доверенных корневых сертификатов» на стр. 330),
- изданные сертификаты (см. «Просмотр изданных сертификатов» на стр. 330).

Основная информация о выбранном сертификате отображается в окне **Сертификат** на вкладке **Общие**:

- назначение сертификата или (для недействительных сертификатов) причина недействительности сертификата;
- имя владельца открытого ключа, которому выдан сертификат;
- имя издателя сертификата;
- срок действия сертификата;
- срок действия закрытого ключа, соответствующего данному сертификату (только для сертификатов пользователей);
- информация о политиках применения сертификата, отображаемая при нажатии кнопки **Заявление издателя**.

Примечание. В сертификате пользователя сети ViPNet CUSTOM кнопка **Заявление издателя** доступна только в том случае, если политики применения были присвоены сертификату при его издании в программе ViPNet Удостоверяющий и ключевой центр.

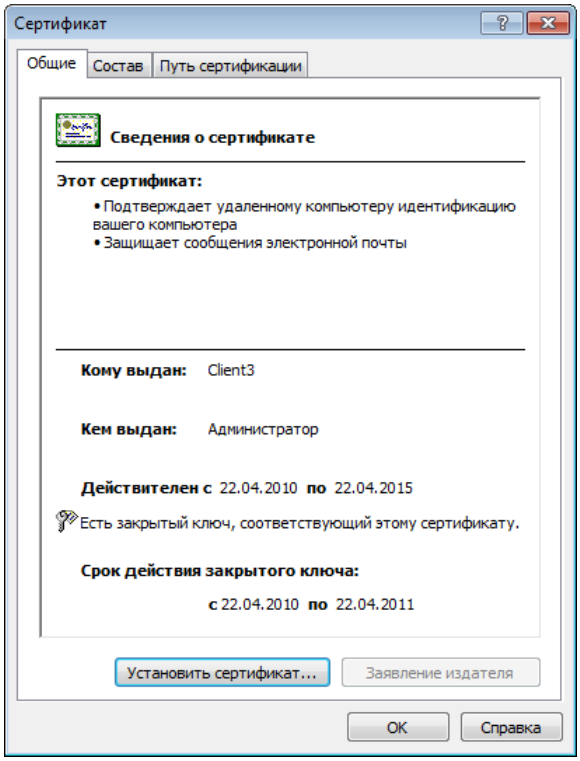


Рисунок 141: Просмотр основной информации о сертификате

Просмотр текущего сертификата пользователя

Для просмотра текущего сертификата пользователя в окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Подробнее**.

Откроется окно **Сертификат** с информацией о сертификате, который используется в качестве текущего.

Просмотр личных сертификатов пользователя

Для просмотра личных сертификатов пользователя:

1. В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Сертификаты**.

   Откроется окно **Менеджер сертификатов** с информацией обо всех личных сертификатах пользователя, а также о сертификатах, установленных в хранилище операционной системы. Все данные сертификаты введены в действие.

Примечание. Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 311).

2 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или дважды щелкните этот сертификат.

Откроется окно **Сертификат** с информацией о выбранном личном сертификате.

Просмотр доверенных корневых сертификатов

Для просмотра доверенных корневых сертификатов:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Сертификаты**.

2 В окне **Менеджер сертификатов** откройте вкладку **Доверенные корневые сертификаты**.

3 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или дважды щелкните этот сертификат.

Откроется окно **Сертификат** с информацией о выбранном корневом сертификате.

Просмотр изданных сертификатов

Для просмотра изданных сертификатов:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Изданные сертификаты.**

Откроется окно **Менеджер сертификатов** с информацией о сертификатах, которые изданы в программе ViPNet Удостоверяющий и ключевой центр по запросам пользователей или по инициативе администратора УКЦ, но еще не введены в действие.

2 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите кнопку **Свойства** или дважды щелкните этот сертификат.

Откроется окно **Сертификат** с информацией о выбранном изданном сертификате.

Просмотр цепочки сертификации

Для просмотра цепочки сертификации (см. «Цепочка сертификации» на стр. 493) определенного сертификата:

1. Вызовите окно **Сертификат** для того сертификата, цепочку сертификации которого необходимо просмотреть.
2. Откройте вкладку **Путь сертификации**.

   На данной вкладке отображаются сертификаты, образующие иерархию издателей того сертификата, для которого вызвано окно **Сертификат**, а также информация об их статусе.
3. При необходимости просмотра более подробной информации о сертификате одного из издателей выберите нужный сертификат, после чего нажмите кнопку **Просмотр сертификата** или выполните двойной щелчок мыши для этого сертификата.

   Откроется окно **Сертификат** с информацией о выбранном сертификате.

Просмотр полей сертификата и печать сертификата

Для просмотра полей определенного сертификата:

1. Вызовите окно **Сертификат** для того сертификата, состав полей которого необходимо просмотреть.
2. Откройте вкладку **Состав**.

   По умолчанию на данной вкладке отображается перечень всех полей сертификата.
3. Для ограничения количества просматриваемых полей выберите нужную группу полей в выпадающем списке **Показать**:
   - **Только поля V1** — все поля, кроме расширений;
   - **Только расширения** — дополнительные поля сертификата, соответствующего стандарту X.509 версии 3;

Примечание. Расширение **Срок действия закрытого ключа** отображается в том случае, если срок действия сертификата превышает 1 год. Если срок действия сертификата превышает 1 год, то срок действия закрытого ключа составляет ровно 1 год.

- **Только критические расширения** — только те расширения, которые признаны издателем критическими;
- **Только свойства** — параметры, которые не являются полями сертификата, но присваиваются сертификату при хранении его в системном хранилище используемой рабочей станции.

4 Выберите в таблице нужное поле, после чего в нижней части окна ознакомьтесь с содержимым этого поля.

Для отправки сертификата на принтер, используемый по умолчанию на текущей рабочей станции, нажмите кнопку **Печать**.

Управление сертификатами

Возможности программы ViPNet Coordinator по управлению сертификатами с помощью окна **Настройка параметров безопасности** представлены в таблице.

Функциональная возможность	Ссылка
Установка сертификатов в хранилище. Возможна настройка параметров автоматической установки сертификатов в хранилище, а также установка сертификатов в хранилище вручную	Установка в хранилище автоматически (на стр. 334) Установка в хранилище вручную (на стр. 336)
Смена текущего сертификата. Можно выбрать другой сертификат (из числа действительных личных сертификатов пользователя) в качестве текущего.	Смена текущего сертификата (на стр. 339)
Обновление закрытого ключа и сертификата. Можно настроить параметры автоматического оповещения об истечении срока действия текущего сертификата и соответствующего ему закрытого ключа, а также, при необходимости, сформировать запрос на обновление этого сертификата и закрытого ключа.	Настройка оповещения об истечении срока действия закрытого ключа и сертификата (на стр. 342) Процедура обновления закрытого ключа и сертификата (на стр. 342)
Ввод сертификата в действие. Если требуется использовать сертификат, переданный на данный сетевой узел, необходимо ввести этот сертификат в действие. Можно настроить параметры автоматического ввода сертификатов в действие или выполнить ввод в действие вручную.	Ввод сертификата в действие (на стр. 349) Ввод в действие автоматически (на стр. 350) Ввод в действие вручную (на стр. 350)
Просмотр и удаление запросов на сертификаты. Можно просмотреть состояние запросов на сертификаты, сформированных текущим пользователем, а также удалить ненужные запросы.	Работа с запросами на сертификаты (на стр. 351) Просмотр запроса на сертификат (на стр. 351) Удаление запроса на сертификат (на стр. 352)
Экспорт сертификата. В зависимости от целей использования сертификата за пределами ПО ViPNet, сертификат может быть экспортирован в файлы различных форматов.	Экспорт сертификата (на стр. 353)

Установка сертификатов в хранилище

Установка сертификатов в хранилище позволяет использовать сертификаты во внешних приложениях (таких как Windows Live Mail, Microsoft Outlook, Microsoft Word и других). Можно установить сертификат в хранилище операционной системы или хранилище программы ViPNet Coordinator (в папку `D_STATION`, находящуюся в папке установки).

Установку можно выполнить автоматически или вручную.

Внимание! При установке сертификата в хранилище ОС Windows Vista или Windows Server 2008 следует запускать программу ViPNet Coordinator от имени администратора ОС (с помощью команды **Запуск от имени администратора** (**Run as Administrator**) контекстного меню ярлыка).

Установка в хранилище автоматически

Установка сертификатов запускается автоматически при соблюдении следующих двух условий:

- сертификаты (текущий сертификат пользователя, корневой сертификат и списки отозванных сертификатов) отсутствуют в хранилище;
- в окне **Настройка параметров безопасности** на вкладке **Криптопровайдер** установлены флажки группы **Автоматически устанавливать в системное хранилище.**

Примечание. В автоматическом режиме выполняется установка сертификатов в хранилище текущего пользователя.

Следует иметь в виду, что автоматическая установка корневого сертификата может занимать продолжительное время в зависимости от используемой программы ViPNet:

- В программе ViPNet Монитор опрос параметров выполняется через пять минут после запуска и далее с 2-часовым интервалом. При открытом окне **Настройка параметров безопасности** интервал опроса сокращается до 10–15-ти минут.
- В программах ViPNet Деловая почта и ViPNet CryptoService опрос параметров выполняется с интервалом 30–60 минут.

Для автоматической установки текущего сертификата пользователя и списков отозванных сертификатов (при соблюдении приведенных выше условий) не требуется никаких дополнительных действий со стороны пользователя.

Для автоматической установки корневого сертификата:

1 При появлении окна **Установка корневого сертификата**:

Примечание. Окно **Установка корневого сертификата** появляется тогда, когда корневой сертификат отсутствует в хранилище сертификатов Windows. Это может произойти в следующих случаях:

- При первичном запуске ПО ViPNet после развертывания сетевого узла.
- Если получено обновление текущего сертификата пользователя, содержащее новый корневой сертификат.

- чтобы выполнить автоматическую установку сертификата, нажмите кнопку **OK**;
- если автоматическая установка корневого сертификата и других сертификатов не требуется, установите флажок **Отключить автоматическую установку сертификатов**, после чего нажмите кнопку **OK**.

Примечание. В окне **Настройка параметров безопасности** на вкладке **Криптопровайдер** флажки группы **Автоматически устанавливать в системное хранилище** будут также сняты.

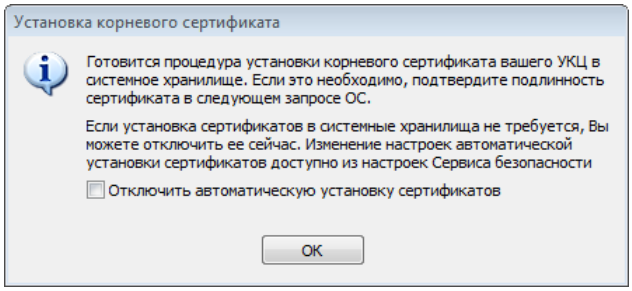


Рисунок 142: Установка корневого сертификата

2 Если автоматическая установка сертификатов не была прервана, в окне запроса на добавление сертификата в хранилище проверьте подлинность сертификата, после чего нажмите кнопку **Да**.

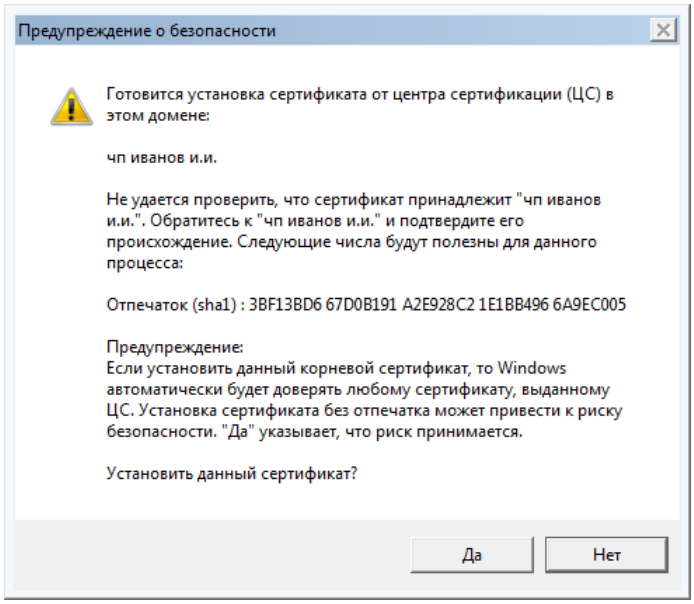


Рисунок 143: Подтверждение подлинности корневого сертификата

Корневой сертификат установлен в хранилище сертификатов текущего пользователя.

Установка в хранилище вручную

Для работы с защищенными документами необходим закрытый ключ и соответствующий ему сертификат. Установка ключа и сертификата может выполняться путем установки одного контейнера или путем установки сертификата и контейнера ключей по отдельности.

Если у вас имеется закрытый ключ и вам необходимо сформировать на его базе сертификат (или обновить уже имеющийся) — направьте в Удостоверяющий центр запрос на сертификат.

Внимание! Для работы с защищенными документами, помимо сертификата пользователя, необходимо также установить в хранилище корневой сертификат (издателя) и СОС.

Сертификат можно установить отдельно и сопоставить его с персональным закрытым ключом.

Для установки сертификата в хранилище пользователя:

1. Вызовите окно **Сертификаты** для того сертификата, который необходимо установить в хранилище (см. «Просмотр сертификатов» на стр. 328).
2. Нажмите кнопку **Установить сертификат**.
3. На странице приветствия мастера установки сертификатов нажмите кнопку **Далее**.
4. На странице **Выбор хранилища сертификатов** выполните следующие действия:
   - Укажите, в какое хранилище будет установлен ваш сертификат.
   - Если в файле с расширением `*p7b` или `*p7s` помимо сертификата также содержатся сертификаты издателей и СОС для их установки установите соответствующие флажки.

   Нажмите кнопку **Далее**.

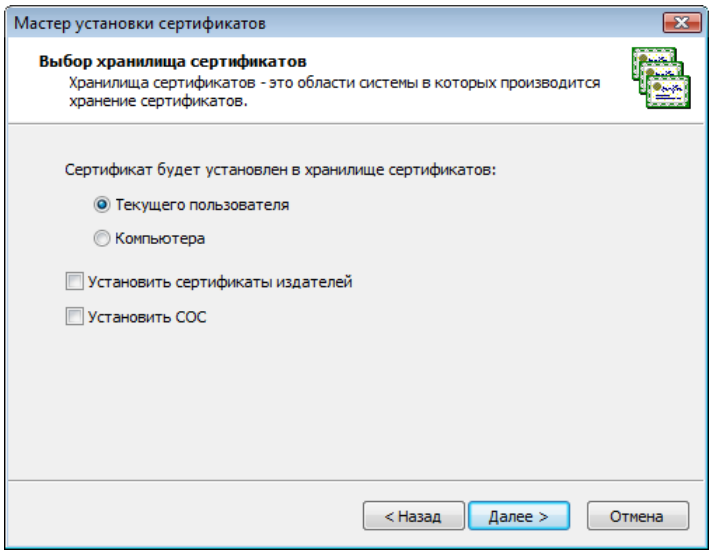


Рисунок 144: Выбор хранилища сертификатов

Примечание. Сертификат следует устанавливать в хранилище текущего пользователя для целей шифрования, расшифрования и подписания файлов, а также для доступа к защищенным ресурсам через веб-браузер. В хранилище компьютера следует устанавливать сертификаты, которые будут использоваться службами данного компьютера.

Сертификат следует устанавливать в хранилище компьютера при использовании ViPNet Coordinator на веб-сервере для организации доступа к защищенным ресурсам.

Если возможность установки сертификата в хранилище компьютера недоступна, войдите в систему с правами администратора.

---

5 На странице **Готовность к установке сертификата**:

- Проверьте правильность выбранных параметров. При необходимости вернитесь на предыдущую страницу мастера с помощью кнопки **Назад** и выберите другие параметры.

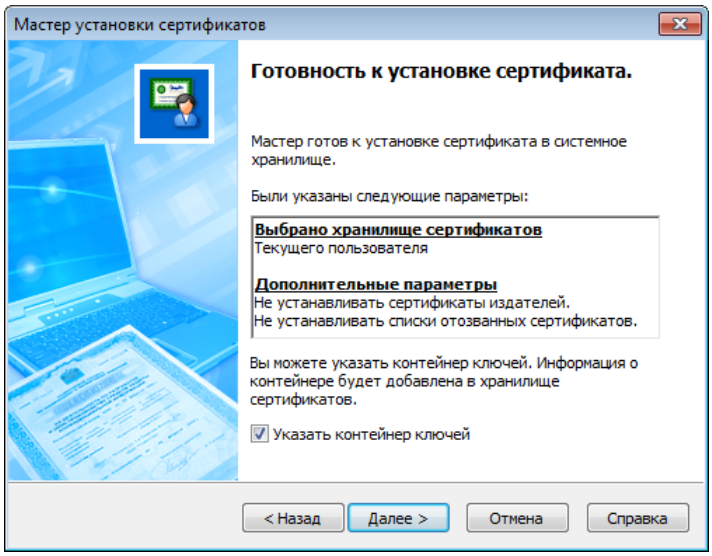


Рисунок 145: Сертификат готов к установке

- Если сертификат хранится в файле отдельно от закрытого ключа, установите флажок **Указать контейнер ключей**.

Примечание. Флажок **Указать контейнер ключей** можно не устанавливать. В этом случае необходимо указать расположение контейнера позже, после завершения работы мастера установки сертификата.

- Нажмите кнопку **Далее**.

6 Если флажок **Указать контейнер ключей** установлен и контейнер не найден либо недоступен, в появившемся окне **ViPNet CSP – инициализация контейнера ключей** укажите расположение контейнера ключей:

- папку на диске;
- устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 438).

После этого нажмите кнопку **OK**.

7 В окне подтверждения нажмите кнопку **Да**, чтобы добавить сертификат в контейнер ключей, или кнопку **Нет**, чтобы оставить сертификат в виде отдельного файла.

Совет. Сохранение сертификата в одном контейнере с закрытым ключом удобно, если контейнер планируется переносить и устанавливать на другом компьютере.

8 Если флажок **Указать контейнер ключей** установлен и контейнер доступен, в появившемся окне **ViPNet CSP – пароль контейнера ключей** в поле **Пароль** введите пароль доступа к контейнеру, после чего нажмите кнопку **OK**.

Примечание. Окно **ViPNet CSP – пароль контейнера ключей** не отображается в том случае, если ранее был сохранен пароль и установлен флажок **Не показывать больше это окно**.

9 На странице **Завершение работы мастера установки сертификата** нажмите кнопку **Готово**.

Сертификат установлен в выбранное хранилище сертификатов. В случае если в процессе установки сертификата ему не был сопоставлен закрытый ключ, необходимо установить контейнер ключей, соответствующий этому сертификату (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 363).

Смена текущего сертификата

Если у вас есть несколько действительных личных сертификатов, вы можете использовать любой из них в качестве текущего.

Внимание! Если при обновлении сертификата новый сертификат, изданный по запросу пользователя, передан на сетевой узел в составе ключей пользователя, то для использования такого сертификата необходимо выбрать его в качестве текущего.

Для выбора действительного личного сертификата в качестве текущего:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Выбрать**.

Если у вас есть хотя бы один действительный личный сертификат, появится окно **Выбор сертификата** с информацией обо всех личных сертификатах, а также о сертификатах, установленных в хранилище операционной системы.

Примечание. Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование внешних сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 311).

Если не найден ни один действительный личный сертификат, появится окно с сообщением «Нет действительных сертификатов с действительным закрытым ключом».

2 В окне **Выбор сертификата** выберите нужный сертификат, при необходимости воспользовавшись кнопкой **Свойства** для просмотра подробной информации о сертификате, после чего нажмите кнопку **ОК**.

Примечание. В качестве текущего можно использовать только тот действительный личный сертификат, который введен в действие. Изданный, но не введенный в действие личный сертификат необходимо сначала ввести в действие (см. «Ввод сертификата в действие» на стр. 349), а затем назначить текущим.

При успешном выполнении описанных действий выбранный сертификат назначается текущим. При этом на вкладке **Ключи** (см. Рисунок 155 на стр. 358) в группе **Подпись** меняется информация о контейнере ключей, в котором хранится выбранный сертификат.

Обновление закрытого ключа и сертификата

Сертификат открытого ключа и закрытый ключ имеют ограниченный срок действия, поэтому их требуется регулярно обновлять. При обновлении сертификата также обновляется закрытый ключ.

Обновление сертификата и закрытого ключа, который соответствует данному сертификату, требуется в следующих случаях:

- Истек срок действия сертификата открытого ключа. Срок действия сертификата может составлять до 5 лет.
- Истек срок действия закрытого ключа. Срок действия закрытого ключа составляет 1 год (если срок действия сертификата превышает 1 год) или равен сроку действия сертификата (если срок действия сертификата меньше 1 года).
- Требуется получить сертификат, в котором будут изменены данные о его владельце (должность, подразделение и другие) или добавлены дополнительные атрибуты, расширения. Например, для использования сертификата в системах документооборота в него могут быть добавлены нужные политики применения.

Таким образом, требуется обновлять сертификат открытого ключа и закрытый ключ не реже, чем 1 раз в год.

Обновить сертификат и закрытый ключ вы можете не только в программе ViPNet Coordinator (из окна **Настройка параметров безопасности**), но и с помощью ее компонента — программы ViPNet CSP (см. документ «ViPNet CSP. Руководство пользователя»).

Примечание. Если истек срок действия закрытого ключа, но при этом сертификат открытого ключа остается действительным, можно создать запрос на обновление сертификата. Запрос будет подписан закрытым ключом, но подпись будет недействительной. Она будет использоваться не для подтверждения авторства, а только для проверки целостности запроса. В этом случае потребуется ваше подтверждение корректности запроса согласно регламенту, принятому в удостоверяющем центре.

Если истек срока действия и закрытого ключа и сертификата, запрос на обновление создать невозможно. Новый сертификат в этом случае может быть издан только по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр.

В случае отсутствия закрытого ключа создать запрос на сертификат также невозможно.

Настройка оповещения об истечении срока действия закрытого ключа и сертификата

По умолчанию программа ViPNet Coordinator начинает выдавать предупреждения за 15 дней до истечения срока действия сертификата или закрытого ключа.

Чтобы изменить настройки оповещения, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись.**

В поле **Информация о текущем сертификате** указан срок действия сертификата.

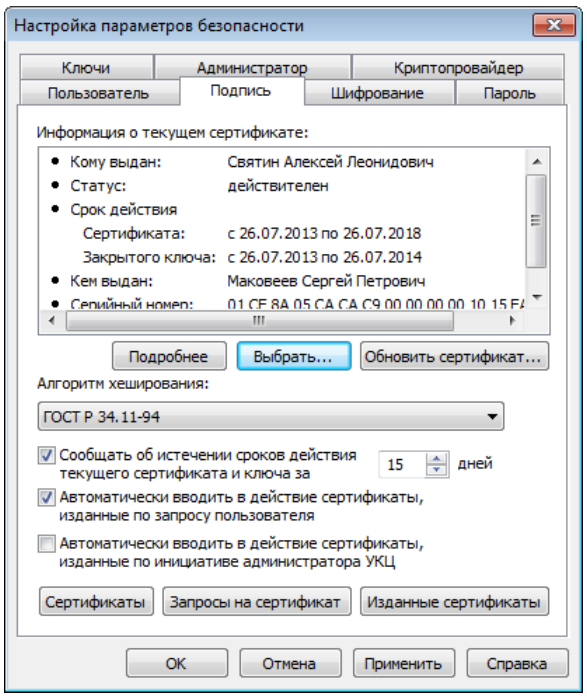


Рисунок 146: Просмотр информации о текущем сертификате и настройка параметров оповещения об истечении сроков действия закрытого ключа и сертификата

2 Установите или снимите флажок **Сообщать об истечении сроков действия текущего сертификата и ключа за** и в поле справа введите число дней не более 30.

Процедура обновления закрытого ключа и сертификата

За несколько дней до истечения срока действия сертификата или закрытого ключа требуется выполнить следующие действия:

- Если включено оповещение об истечении срока действия сертификата и закрытого ключа:

- Когда до истечения срока остается заданное количество дней, программа ViPNet Coordinator выдаст соответствующее сообщение.

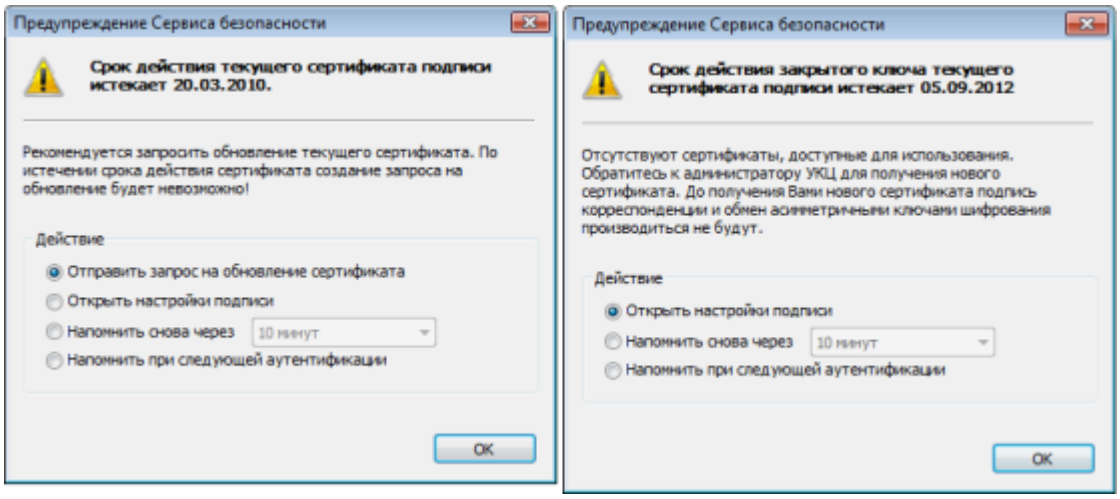


Рисунок 147: Предупреждения о скором истечении срока действия сертификата и закрытого ключа

- Если истекает срок действия сертификата, в окне сообщения выберите **Отправить запрос на обновление сертификата**, после чего нажмите кнопку **ОК**. Будет запущен **Мастер обновления сертификата**.

Примечание. Можно также открыть окно настройки параметров подписи или отложить отправку запроса на обновление сертификата.

- Если истекает срок действия закрытого ключа, в окне сообщения выберите **Открыть настройки подписи**, после чего нажмите кнопку **ОК**. В появившемся окне **Настройка параметров безопасности** на вкладке **Подпись** нажмите кнопку **Обновить сертификат**.

- Если оповещение об истечении срока действия сертификата и закрытого ключа отключено:
  - В окне **Настройка параметров безопасности** откройте вкладку **Подпись**.
  - На вкладке **Подпись** (см. Рисунок 146 на стр. 342) нажмите кнопку **Обновить сертификат**. Будет запущен **Мастер обновления сертификата**.

Чтобы сформировать и отправить запрос на обновление сертификата и закрытого ключа с помощью мастера:

1 На первой странице мастера обновления сертификата нажмите кнопку **Далее**.

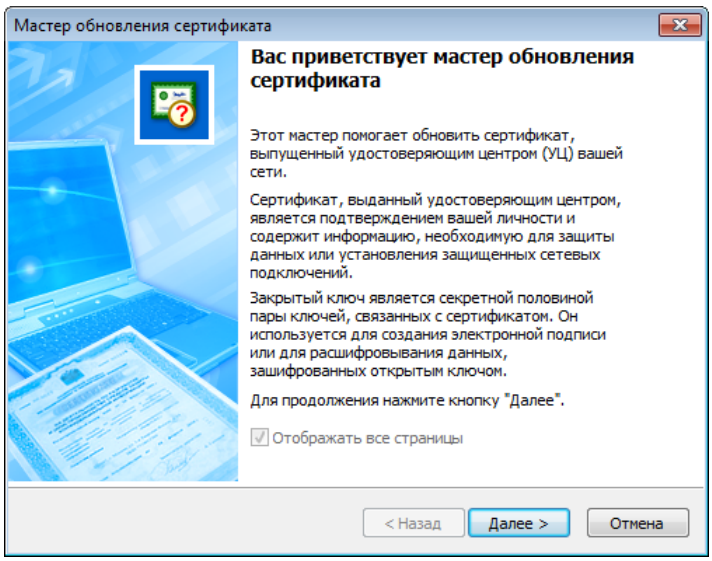


Рисунок 148: Стартовая страница мастера обновления сертификата

2 На странице **Открытый ключ** выполните следующие действия:

2.1 Укажите назначение ключа и сертификата:

- если предполагается их использовать только для подписи — значение **Подпись**;
- если предполагается их использовать как для подписи, так и для шифрования — значение **Подпись и шифрование**.

2.2 Задайте алгоритм формирования ключа и параметры алгоритма в соответствии с приведенной ниже таблицей:

Таблица 12. Характеристики алгоритмов

Алгоритм и его описание	**Параметры алгоритма**	**Длина открытого ключа**
ГОСТ Р 34.10-2001 См. RFC 4357 http://www.ietf.org/rfc/rfc4357.txt	**Для подписи:** ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1»	512

Алгоритм и его описание	Параметры алгоритма	Длина открытого ключа
Стандарт электронной подписи, основанный на арифметике эллиптических кривых OID «1.2.643.2.2.19»	ГОСТ Р 34.10 - 2001 «Оскар» OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи 3 OID «1.2.643.2.2. 35.3» **Для подписи и шифрования:** ГОСТ Р 34.10 - 2001. EDH Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 36.0» ГОСТ Р 34.10 - 2001. EDH Параметры обмена 2 OID «1.2.643.2.2. 36.1»	
ГОСТ Р 34.10-2012/512 Новый стандарт электронной подписи от 2012 года с длиной закрытого ключа 256 бит OID «1.2.643.7.1.1.1.1»	ГОСТ Р 34.10 - 2001. Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 «Оскар» OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001. Параметры подписи 3 OID «1.2.643.2.2. 35.3»	512
ГОСТ Р 34.10-2012/1024 Новый стандарт электронной подписи от 2012 года с длиной закрытого ключа 512 бит OID «1.2.643.7.1.1.1.2»	ГОСТ Р 34.10 - 2012/1024. Набор параметров А	1024

Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки подписи, шифрования и расшифрования.

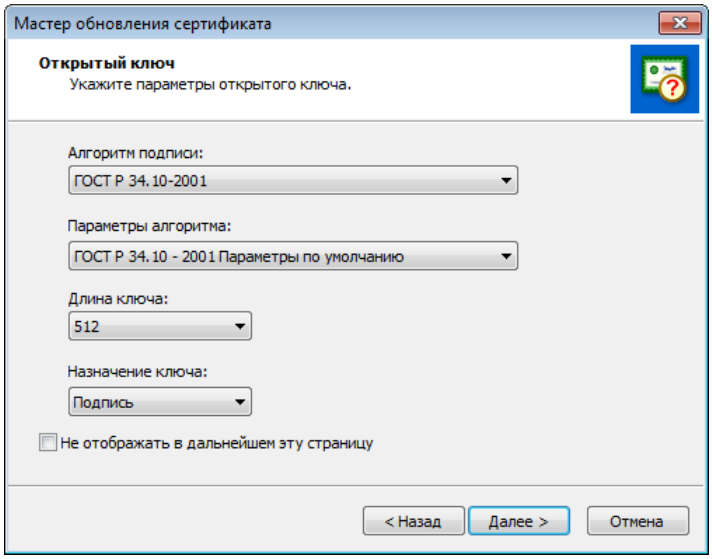


Рисунок 149: Выбор алгоритма и его параметров

2.3 Нажмите кнопку **Далее**.

3 На странице **Контейнер с закрытым ключом** укажите место хранения контейнера ключей:

- папку на диске,
- устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 438).

После этого нажмите кнопку **Далее**.

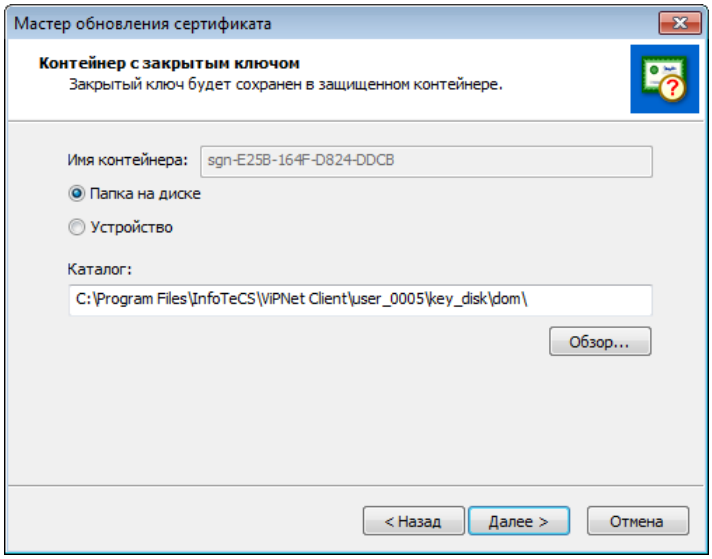


Рисунок 150: Указание места хранения контейнера ключей

4 На странице **Срок действия сертификата** задайте желаемый срок действия обновляемого сертификата удобным для вас способом, после чего нажмите кнопку **Далее**.

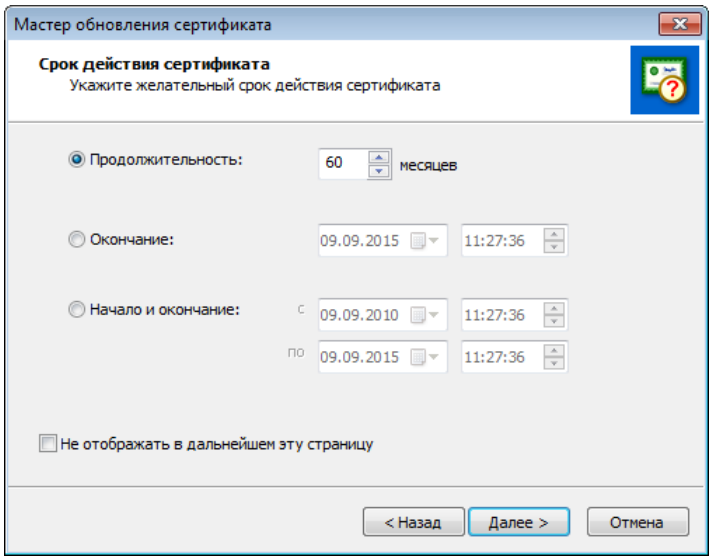


Рисунок 151: Указание желаемого срока действия сертификата

5 На странице **Готовность к созданию запроса на сертификат**:

- Убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

- При необходимости печати информации о запросе на принтере, используемом по умолчанию на данном сетевом узле, убедитесь в том, что установлен флажок **Печатать информацию о запросе**. В противном случае снимите флажок.

После этого нажмите кнопку **Далее.**

6 При появлении электронной рулетки следуйте указаниям окна.

Примечание. В случае если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

7 На странице **Завершение работы мастера обновления сертификата** нажмите кнопку **Готово.**

В результате запрос на обновление сертификата будет передан в программу ViPNet Удостоверяющий и ключевой центр.

Примечание. Время ожидания ответа от программы ViPNet Удостоверяющий и ключевой центр может значительно варьироваться в зависимости от параметров настройки этой программы. Если программа ViPNet Удостоверяющий и ключевой центр настроена на автоматическую обработку запросов на сертификаты, время ожидания ответа не превышает 5 минут. Если обработка запросов в программе ViPNet Удостоверяющий и ключевой центр осуществляется вручную, время ожидания ответа не ограничено. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Если запрос на обновление сертификата в программе ViPNet Удостоверяющий и ключевой центр будет удовлетворен, на сетевой узел поступит обновленный сертификат. Изданный сертификат будет введен в действие и назначен текущим сразу после получения в том случае, если:

- В окне **Настройка параметров безопасности** на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**.
- Доступен контейнер, в котором хранится закрытый ключ, соответствующий сертификату.

Внимание! Если контейнер с закрытым ключом хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет

доступен только в том случае, если устройство подключено и сохранен ПИН-код к нему.

В окне **Менеджер сертификатов** для запроса, по которому был издан сертификат, будет отображаться статус **сертификат введен в действие** (см. «Просмотр запроса на сертификат» на стр. 351).

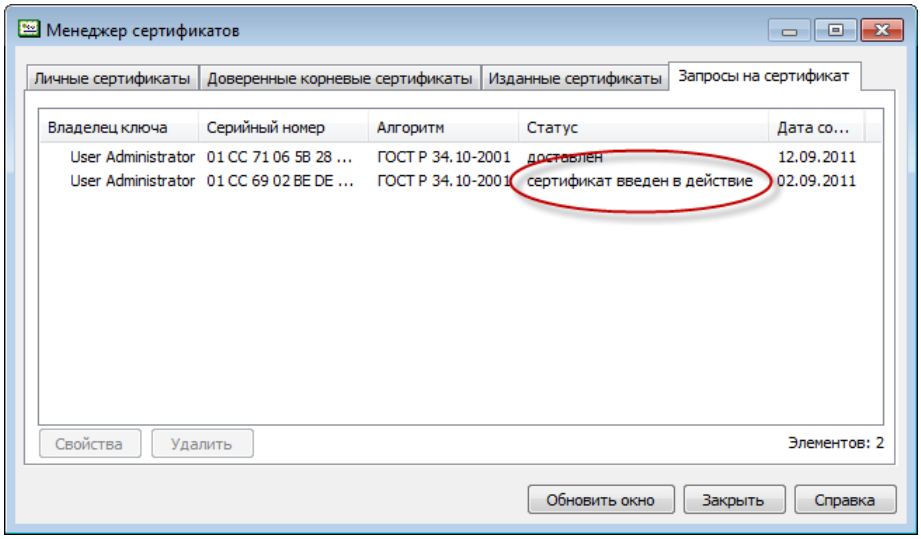


Рисунок 152: Статус запроса в случае ввода сертификата в действие

Если сертификат был получен, но не введен в действие автоматически, для запроса, по которому он был издан, будет отображаться статус **удовлетворен**. Выполните в данном случае ввод сертификата в действие вручную (см. «Ввод в действие вручную» на стр. 350).

Если запрос на обновление сертификата в программе ViPNet Удостоверяющий и ключевой центр будет отклонен, сертификат не будет издан. Запрос на сертификат будет иметь статус **отклонен**. Обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр для уточнения причин отклонения запроса.

Ввод сертификата в действие

Для того чтобы использовать сертификат, полученный из программы ViPNet Удостоверяющий и ключевой центр, необходимо ввести этот сертификат в действие, то есть установить этот сертификат в контейнер путем сопоставления его с соответствующим закрытым ключом.

Ввод в действие автоматически

Для того чтобы ввод в действие сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр, выполнялся автоматически, убедитесь в том, что в окне **Настройка параметров безопасности** на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**, а также флажок **Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ**.

При наличии данных флажков сертификаты будут вводиться в действие автоматически в течение часа с момента их получения. Сертификаты, изданные по вашим запросам, смогут вводиться в действие автоматически только в том случае, если доступны контейнеры с соответствующими закрытыми ключами. В противном случае они могут быть введены в действие только вручную (см. «Ввод в действие вручную» на стр. 350).

Внимание! Если контейнер с закрытым ключом хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет доступен только в том случае, если устройство подключено и сохранен ПИН-код к нему.

При вводе в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, появится окно **Предупреждение сервиса безопасности** с соответствующим сообщением (см. «Сертификат, изданный по инициативе администратора, введен в действие» на стр. 388).

Ввод в действие вручную

Ввод сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр, в действие вручную требуется выполнять в следующих случаях:

- Если не установлены флажки, позволяющие выполнять автоматический ввод сертификатов в действие.
- При автоматическом вводе сертификата в действие был недоступен контейнер с соответствующим закрытым ключом.

Чтобы вручную ввести в действие полученный сертификат, выполните следующие действия:

1. В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Изданные сертификаты**.

2 В окне **Менеджер сертификатов** на вкладке **Изданные сертификаты** выберите полученный сертификат, который необходимо ввести в действие, после чего нажмите кнопку **Ввести в действие**.

В результате введенный в действие сертификат отобразится в окне **Менеджер сертификатов** на вкладке **Личные сертификаты**. Если необходимо использовать этот сертификат для подписания электронных документов, назначьте его текущим (см. «Смена текущего сертификата» на стр. 339).

Работа с запросами на сертификаты

Работа с запросами на сертификаты выполняется в окне **Менеджер сертификатов** на вкладке **Запросы на сертификат**.

Для вызова окна **Менеджер сертификатов**:

1 В окне **Настройка параметров безопасности** откройте вкладку **Подпись**.

2 Нажмите кнопку **Запросы на сертификаты**.

Просмотр запроса на сертификат

Для просмотра подробной информации о запросе на сертификат:

1 В окне **Менеджер сертификатов** на вкладке **Запросы на сертификат** выберите нужный запрос, после чего нажмите кнопку **Свойства** или дважды щелкните по этому запросу.

2 В окне **Запрос на сертификат** просмотрите нужную информацию на соответствующих вкладках.

При необходимости запрос можно распечатать (на принтере, используемом по умолчанию на данном компьютере) с помощью кнопки **Печать**, а также сохранить в файл формата `*.txt` — с помощью кнопки **Копировать в файл**.

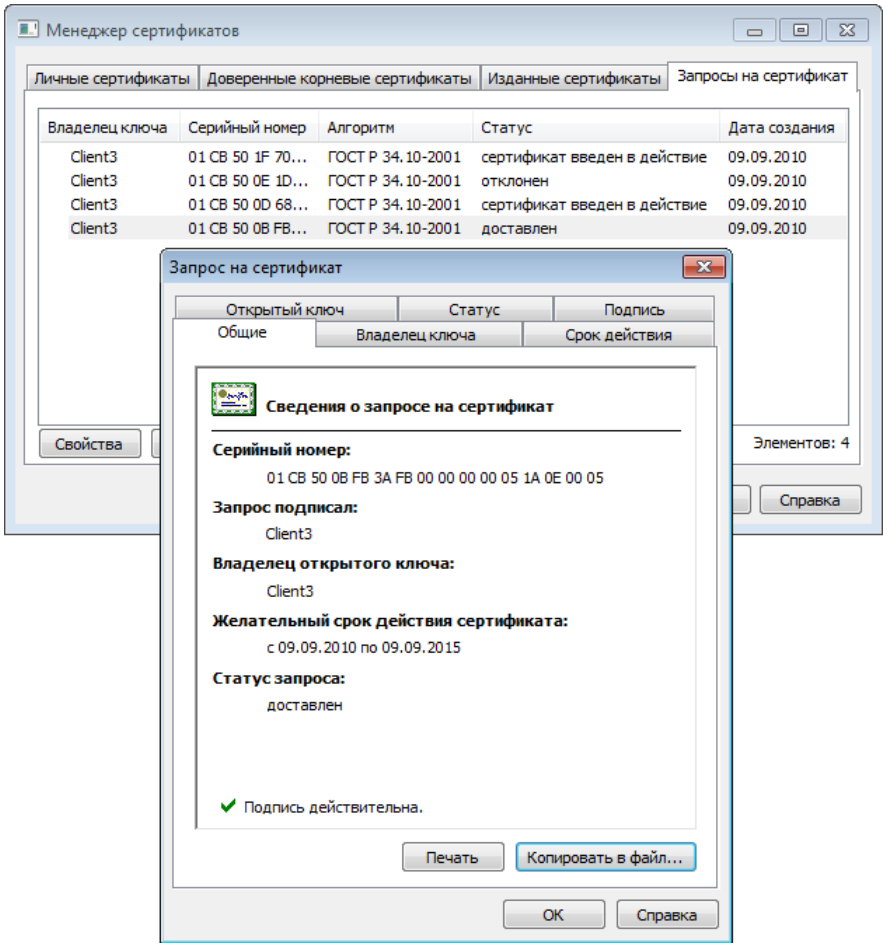


Рисунок 153: Просмотр подробной информации о запросе на сертификат

Удаление запроса на сертификат

Для удаления запроса на сертификат:

1. В окне **Менеджер сертификатов** на вкладке **Запросы на сертификат** выберите нужный запрос (или несколько, удерживая клавишу **Ctrl**), после чего нажмите кнопку **Удалить**.
2. В окне подтверждения нажмите кнопку **Да**.

Информация о запросе будет удалена. Удаленный запрос не будет отображаться на вкладке **Запросы на сертификаты**.

Экспорт сертификата

В программе ViPNet можно выполнить экспорт сертификата пользователя в различные форматы. Выбор формата экспорта зависит от целей, для которых проводится данный экспорт.

Экспорт сертификата может понадобиться для выполнения следующих задач:

- архивирование сертификата;
- копирование сертификата для использования на другом компьютере;
- отправка сертификата другому пользователю для организации обмена зашифрованными сообщениями;
- просмотр сертификата в удобной форме.

Для экспорта сертификата в файл определенного формата:

1. Вызовите окно **Сертификат** для того сертификата, который необходимо экспортировать (см. «Просмотр сертификатов» на стр. 328).
2. Откройте вкладку **Состав**, после чего нажмите кнопку **Копировать в файл**.
3. На начальной странице мастера экспорта сертификатов нажмите кнопку **Далее**.

Совет. Если при последующих запусках мастера желательно пропускать первую страницу, установите на ней флажок **Не отображать в дальнейшем эту страницу**.

4. На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. «Форматы экспорта сертификатов» на стр. 354), после чего нажмите кнопку **Далее**.

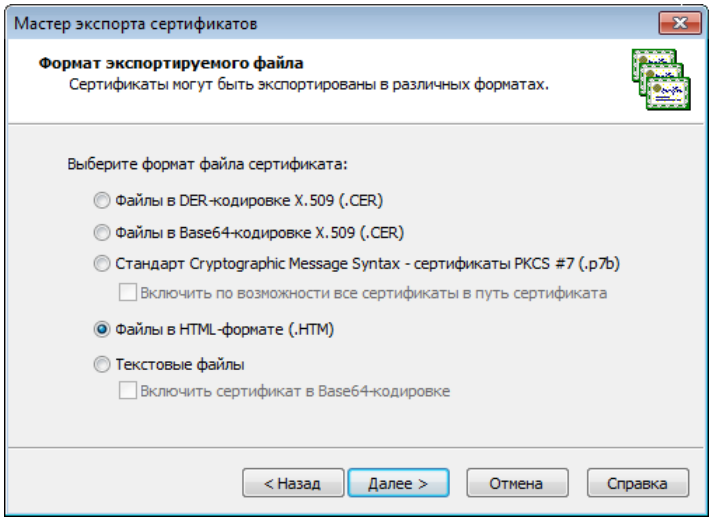


Рисунок 154: Выбор формата файла

5 На странице **Имя файла** укажите полный путь к создаваемому файлу, после чего нажмите кнопку **Далее**.

6 На странице **Завершение работы мастера экспорта сертификатов** убедитесь в правильности параметров экспорта, заданных на предыдущих страницах мастера, после чего нажмите кнопку **Готово**.

7 В окне с сообщением об успешном экспорте нажмите кнопку **ОК**.

Форматы экспорта сертификатов

При выборе формата экспорта сертификата следует руководствоваться перечисленными положениями.

- При экспорте сертификатов для импорта на компьютер с ОС Windows наиболее предпочтительный формат экспорта — PKCS #7, в первую очередь потому, что этот формат обеспечивает сохранение цепочки центров сертификации (пути сертификации) любого сертификата. Некоторые приложения требуют при импорте сертификата из файла представления в виде DER или Base64. Поэтому формат экспорта необходимо выбирать в соответствии с требованиями приложения или системы, в которую этот сертификат предполагается импортировать.

- Для просмотра сертификата и вывода его на печать используются текстовый и HTML-форматы.

Ниже приведена подробная информация о каждом из форматов экспорта сертификатов, поддерживаемых ПО ViPNet.

- **Стандарт Cryptographic Message Syntax (PKCS #7)**

  Формат PKCS #7 позволяет передавать сертификат и все сертификаты в цепочке сертификации с одного компьютера на другой или с компьютера на внешнее устройство. Файлы PKCS #7 обычно имеют расширение `.p7b` и совместимы со стандартом ITU-T X.509. Формат PKCS#7 разрешает такие атрибуты, как удостоверяющие подписи, связанные с обычными подписями. Для таких атрибутов, как метка времени, можно выполнить проверку подлинности вместе с содержимым сообщения. Дополнительные сведения о формате PKCS #7 см. на странице PKCS #7 веб-узла RSA Labs http://www.rsa.com/rsalabs/node.asp?id=2129.

- **Файлы в DER-кодировке X.509**

  DER (Distinguished Encoding Rules) для ASN.1, как определено в рекомендации ITU-T Recommendation X.509, — более ограниченный стандарт кодирования, чем альтернативный BER (Basic Encoding Rules) для ASN.1, определенный в рекомендации ITU-T Recommendation X.209, на котором основан DER. И BER, и DER обеспечивают независимый от платформы метод кодирования объектов, таких как сертификаты и сообщения, для передачи между устройствами и приложениями.

  При кодировании сертификата большинство приложений используют стандарт DER, так как сертификат (сведения о запросе на сертификат) должен быть закодирован с помощью DER и подписан. Файлы сертификатов DER имеют расширение `.cer`.

  Дополнительные сведения см. в документе «ITU-T Recommendation X.509, Information Technology — Open Systems Interconnection — The Directory: Authentication Framework» на веб-узле International Telecommunication Union (ITU) http://www.itu.int/ru/Pages/default.aspx.

- **Файлы в Base64-кодировке X.509**

  Этот метод кодирования создан для работы с протоколом S/MIME, который популярен при передаче бинарных файлов через Интернет. Base64 кодирует файлы в текстовый формат ASCII, при этом в процессе прохождения через шлюз файлы практически не повреждаются. Протокол S/MIME обеспечивает работу некоторых криптографических служб безопасности для приложений электронной почты, включая механизм неотрекаемости (с помощью электронных подписей), секретность и безопасность данных (с помощью кодирования, процесса проверки подлинности и целостности сообщений). Файлы сертификатов Base64 имеют расширение `.cer`.

  MIME (Multipurpose Internet Mail Extensions, спецификация RFC 1341 и последующие) определяет механизмы кодирования произвольных двоичных данных для передачи по электронной почте.

Дополнительные сведения см. в документе «RFC 2633 S/MIME Version 3 Message Specification, 1999» на веб-узле Internet Engineering Task Force (IETF) http://www.ietf.org/rfc/rfc2633.txt?number=2633.

- **Файлы в HTML-формате**

  Файлы для просмотра и печати в любом веб-браузере, а также в офисных и других программах, поддерживающих язык разметки гипертекста HTML.

- **Текстовые файлы**

  Файлы кодировки ANSI для просмотра в любом текстовом редакторе и вывода на печать.

Работа с контейнером ключей

Контейнер ключей содержит закрытый ключ подписи (см. «Закрытый ключ» на стр. 484) и сертификат (см. «Сертификат открытого ключа подписи пользователя» на стр. 490), соответствующий закрытому ключу.

В программе ViPNet Coordinator доступны следующие операции с контейнером ключей:

- Установка (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 363).

  Устанавливать новый или выполнять смену контейнера ключей с текущим сертификатом может потребоваться в следующих случаях:

  - Если сертификат не был сопоставлен закрытому ключу, который хранится в контейнере, — например, вследствие того, что сертификат хранится отдельно от закрытого ключа. Контейнер ключей может быть установлен как совместно с сертификатом (см. «Установка сертификатов в хранилище» на стр. 334), так и отдельно (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 363) (например, в случае если закрытый ключ хранится в контейнере, а сертификат сформирован по запросу пользователя в программе ViPNet Удостоверяющий и ключевой центр).
  - Если контейнер был сформирован другим приложением или перенесен с другого компьютера.

- Смена и удаление сохраненного пароля к контейнеру (см. «Смена пароля к контейнеру» на стр. 359).

  Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль. Удалять сохраненный пароль к контейнеру ключей может потребоваться в том случае, если изменились условия эксплуатации пароля или регламент вашей организации, вследствие чего хранение пароля на компьютере стало недопустимым.

- Удаление закрытого ключа, который хранится в контейнере (см. «Удаление закрытого ключа» на стр. 363).

  Удаление закрытого ключа из контейнера ключей требуется в следующих случаях:

  - в том случае, если в этом закрытом ключе нет больше необходимости — например, вследствие истечения срока его действия;
  - при компрометации или отзыве сертификата, соответствующего закрытому ключу.

- Изменение расположения контейнера (см. «Перенос контейнера ключей» на стр. 365).

  Перенос текущего контейнера ключей требуется в следующих случаях:

  - если расположение контейнера было изменено, например, вследствие того, что хранение контейнера по прежнему пути было признано небезопасным;
  - при переходе на способ аутентификации **Устройство** в случае, если используются процедуры подписи и шифрования внутри сторонних приложений и при этом контейнер ключей изначально не хранился на внешнем устройстве, используемом для аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 312).

Внимание! В рамках ПО ViPNet CUSTOM выполнять различные операции с контейнером ключей может только пользователь, который обладает правом подписи. Такое право предоставляется пользователям сети ViPNet в программе ViPNet Центр управления сетью.

Для работы с контейнером ключей (см. «Контейнер ключей» на стр. 485):

1 Откройте вкладку **Ключи**.

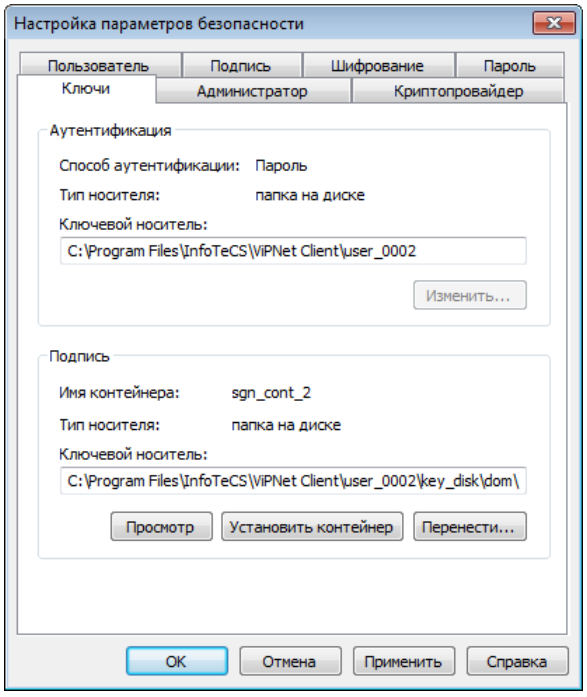


Рисунок 155: Работа с контейнером ключей

2 В группе **Подпись** нажмите одну из следующих кнопок:

- **Просмотр** — для просмотра подробной информации об используемом контейнере ключей, а также для изменения свойств контейнера:
  - смены пароля (см. «Смена пароля к контейнеру» на стр. 359);
  - удаления пароля (см. «Удаление сохраненного на компьютере пароля к контейнеру ключей» на стр. 361);
  - проверки соответствия закрытого ключа сертификату (см. «Проверка контейнера ключей» на стр. 362);
  - удаления закрытого ключа (см. «Удаление закрытого ключа» на стр. 363).
- **Установить контейнер** — для установки нового и смены контейнера ключей с текущим сертификатом (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 363).
- **Перенести** — для изменения расположения контейнера ключей (см. «Перенос контейнера ключей» на стр. 365).

Примечание. В группе **Подпись** отображается информация о закрытом ключе, соответствующем текущему сертификату. При установке нового контейнера ключей (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 363) информация о текущем сертификате, отображаемая на вкладке **Подпись**, меняется автоматически.

Смена пароля к контейнеру

Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль.

Для смены пароля к контейнеру ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 155 на стр. 358) нажмите кнопку **Просмотр.**
2. В окне **Свойства контейнера ключей** нажмите кнопку **Сменить пароль.**

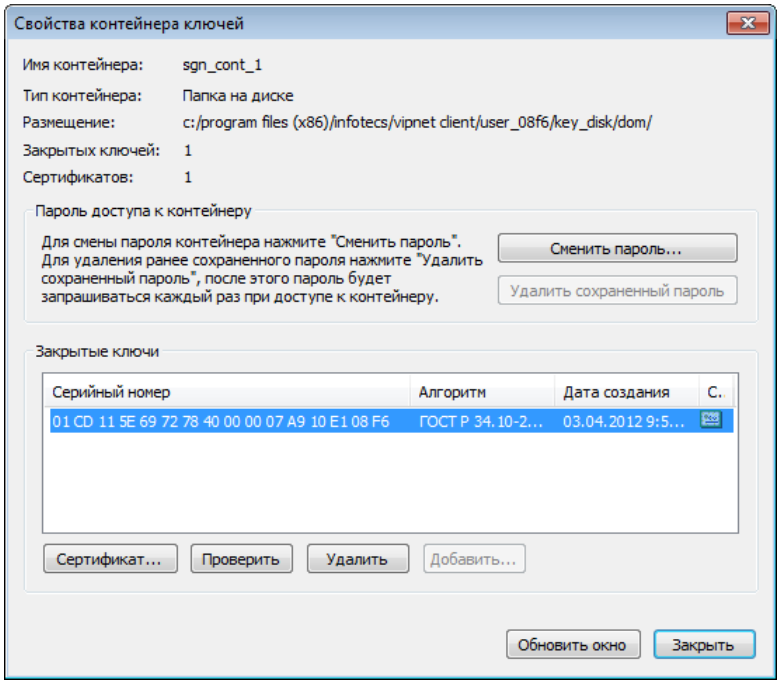


Рисунок 156: Информация о контейнере ключей

3 При появлении сообщения «Для данного контейнера смена пароля возможна только в настройке безопасности приложений ViPNet» нажмите кнопку **OK**, после чего завершите работу с окном **Свойства контейнера ключей** и измените пароль пользователя (см. «Смена пароля пользователя» на стр. 319).

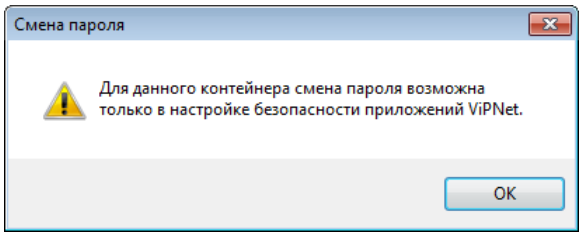


Рисунок 157: Сообщение о невозможности смены пароля для доступа к контейнеру

Примечание. Появление данного окна связано с тем, что контейнер ключей защищен с использованием не пароля, а персонального ключа пользователя. В этом случае пароль к контейнеру совпадает с паролем пользователя, поэтому изменение пароля к контейнеру возможно только вместе с изменением пароля пользователя.

4 Если контейнер ключей пользователя создан в программе ViPNet Registration Point либо был перенесен (см. «Перенос контейнера ключей» на стр. 365) из папки

ключей пользователя (по умолчанию `C:\Program Files (x86)\InfoTeCS\ViPNet Coordinator\user_<идентификатор пользователя>\key_disk\dom`) в другую папку, после нажатия на кнопку **Сменить пароль** появится окно **Пароль**. В окне **Пароль** введите текущий пароль доступа к контейнеру ключей и нажмите кнопку **OK**.

Примечание. Если ранее был установлен режим **Сохранить пароль**, то окно **Пароль** не появится.

5 В окне **ViPNet CSP - пароль контейнера ключей** укажите и подтвердите новый пароль. Нажмите кнопку **OK**.

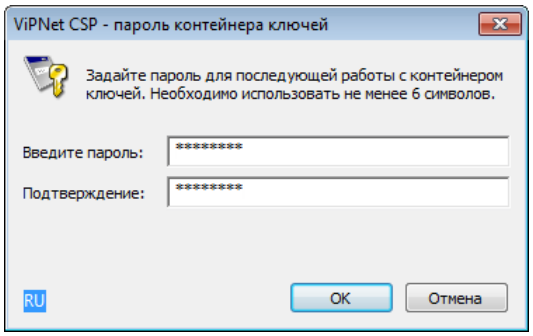


Рисунок 158: Смена пароля доступа к контейнеру ключей

Пароль доступа к контейнеру ключей изменен.

Удаление сохраненного на компьютере пароля к контейнеру ключей

Удалять сохраненный пароль к контейнеру ключей может потребоваться в том случае, если изменились условия эксплуатации пароля или регламент вашей организации, вследствие чего хранение пароля на компьютере стало недопустимым.

Для удаления сохраненного пароля к контейнеру ключей и отображения окна ввода пароля при доступе к контейнеру:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 155 на стр. 358) нажмите кнопку **Просмотр**.

2 В окне **Свойства контейнера ключей** (см. Рисунок 156 на стр. 360) нажмите кнопку **Удалить сохраненный пароль**.

Сохраненный пароль удален. Теперь пароль необходимо вводить всякий раз при доступе к контейнеру ключей.

Проверка контейнера ключей

Проверка контейнера ключей позволяет убедиться, что файл контейнера не поврежден, хранящиеся в контейнере сертификат и закрытый ключ соответствуют друг другу и могут быть использованы для работы с защищенными документами.

Чтобы проверить контейнер ключей:

1. В окне **Свойства контейнера ключей** (см. Рисунок 156 на стр. 360) в списке **Закрытые ключи** выберите нужный закрытый ключ.
2. Нажмите кнопку **Проверить**.
3. В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите кнопку **OK**.

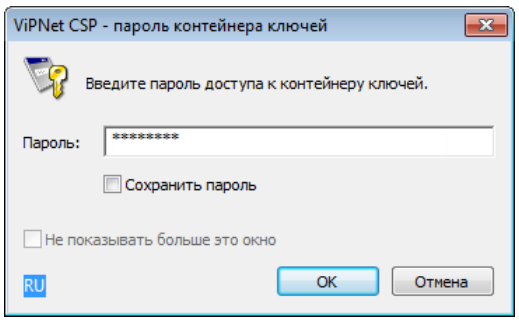


Рисунок 159: Ввод пароля доступа к контейнеру ключей

4. Будет сформирован фрагмент данных, который будет подписан с помощью закрытого ключа, после чего будет выполнена проверка электронной подписи с помощью сертификата открытого ключа. Таким образом, будет проверена пригодность закрытого ключа и его соответствие сертификату, хранящемуся в контейнере.

Примечание. Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий закрытому ключу. Сертификат может отсутствовать в контейнере ключей, если он размещен отдельно. Сертификат размещается отдельно от контейнера ключей, если запрос на обновление сертификата сформирован в ПО ViPNet CSP. Если запрос сформирован в другой программе, сертификат автоматически помещается в контейнер ключей.

При проверке закрытого ключа проверка действительности сертификата (срок его действия, отсутствие в списках отозванных сертификатов и прочее) не выполняется.

Удаление закрытого ключа

Удаление закрытого ключа (и сертификата, при его наличии) из контейнера ключей требуется в следующих случаях:

- если в этом закрытом ключе нет больше необходимости — например, вследствие истечения срока его действия;
- при компрометации или отзыве сертификата, соответствующего закрытому ключу.

Чтобы удалить закрытый ключ и сертификат из контейнера ключей:

1. В окне **Свойства контейнера ключей** (см. Рисунок 156 на стр. 360) в списке **Закрытые ключи** выберите строку закрытого ключа.
2. Нажмите кнопку **Удалить**. Появится предупреждение о том, что удаленный закрытый ключ невозможно восстановить.
3. В окне предупреждения нажмите кнопку **Да.**

Выбранный закрытый ключ и соответствующий ему сертификат будут удалены из контейнера ключей. После этого необходимо удалить контейнер.

Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом

Устанавливать новый контейнер ключей или выполнять смену контейнера ключей с текущим сертификатом может потребоваться в следующих случаях:

- если при установке сертификата в системное хранилище или хранилище программы ViPNet Coordinator (см. «Установка сертификатов в хранилище» на стр. 334) ему не был сопоставлен соответствующий закрытый ключ — например, вследствие того, что сертификат хранится отдельно от закрытого ключа, то есть не в контейнере ключей;
- если контейнер ключей был сформирован в другом приложении или перенесен с другого компьютера.

Примечание. Установить или сменить можно только контейнер с ключами, сформированными в ПО ViPNet версии не ниже 3.2.x.

Для установки нового или смены текущего контейнера ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 155 на стр. 358) нажмите кнопку **Установить контейнер**.
2. В окне **ViPNet CSP – инициализация контейнера ключа** укажите место хранения контейнера ключей:
   - папку на диске;
   - устройство с указанием его параметров и ПИН-кода.

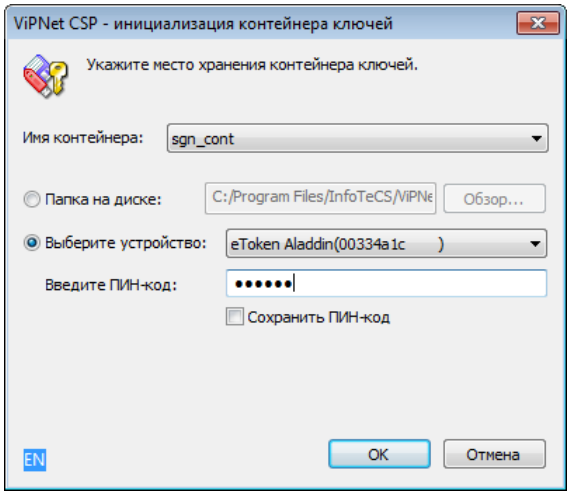


Рисунок 160: Инициализация контейнера ключей с внешнего устройства

   Нажмите кнопку **ОК**.

3. Если в контейнере отсутствует закрытый ключ, в окне с сообщением нажмите кнопку **ОК**, затем выберите другой контейнер.
4. В окне **Выбор сертификата** укажите, какой из сертификатов, находящихся в контейнере, требуется назначить текущим. Затем нажмите кнопку **ОК**.

В результате закрытый ключ и сертификат, которые хранятся в выбранном контейнере, будут назначены текущими. Информация о сертификате, который хранится в установленном контейнере, отобразится на вкладке **Подпись**.

Перенос контейнера ключей

Перенос текущего контейнера ключей может потребоваться для изменения расположения контейнера, например, если хранение контейнера по прежнему пути было признано небезопасным.

Примечание. Перенести можно только контейнер с ключами, сформированными в ПО ViPNet версии не ниже 3.2.x.

Не поддерживается перенос контейнера ключей на устройства eToken ГОСТ, ruToken, Shipka, Kaztoken (см. «Внешние устройства» на стр. 438).

Для того чтобы поменять расположение контейнера ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 155 на стр. 358) нажмите кнопку **Перенести**.
2. В окне **ViPNet CSP – инициализация контейнера ключа** укажите новое место хранения контейнера ключей:
   - папку на диске;
   - устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства (на стр. 438).

Контейнер ключей будет перенесен по указанному пути.

Возможные неполадки и способы их устранения

Сбор диагностической информации при возникновении неполадок

При обращении в службу технического сопровождения компании «ИнфоТеКС» в случае возникновения каких-либо неполадок в работе ПО ViPNet вам, как правило, потребуется предоставить информацию о компьютере, на котором данное ПО установлено. На основе этой информации сотрудники отдела сопровождения смогут выявить причины возникновения неполадок и определить способы их устранения.

Информацию о компьютере вы можете получить с помощью утилиты lumpdiag, встроенной в ПО ViPNet Coordinator. Для работы с утилитой вы должны обладать правами администратора операционной системы.

Утилита собирает информацию о компьютере (например, информацию о системе, криптографическом окружении и так далее) независимо от работоспособности ПО ViPNet Coordinator.

Примечание. В процессе работы утилиты сбор вашей конфиденциальной информации не производится. ОАО «ИнфоТеКС» ответственно подходит к защите вашей личной информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

С помощью утилиты вы можете собрать необходимую информацию либо в архив, либо в папку `\SysEnv`, которая автоматически создается в папке установки ПО ViPNet Coordinator.

Для получения справочной информации по использованию утилиты в командной строке введите: `lumpdiag -h`, где `h` — ключ, который вызывает справку. Если утилита вызвана без указания каких-либо ключей, считается, что она вызвана с данной опцией.

Для сбора информации в командной строке введите:

`lumpdiag -a [<archive file>]`, где:

- `-a` — ключ, который запускает процесс сбора информации на компьютере;
- `<archive file>` — путь к архиву, в который будут упакованы файлы, собранные в результате работы утилиты.

Если при сборе информации параметр `<archive file>` не был указан, то собранная информация будет сохранена в папке `\SysEnv` папки установки ПО ViPNet Coordinator (по умолчанию: `c:\Program Files (Program Files (x86))\InfoTeCS\ViPNet Coordinator`). Если папка `\SysEnv` уже существует, то утилита запросит у вас разрешение на перезапись содержимого папки.

Возможные неполадки

Невозможно проверить сертификат, которым подписан файл установки программы

На компьютере с операционной системой Windows XP или Windows Vista при установке программы может появиться предупреждение системы безопасности о невозможности проверить сертификат, которым подписан данный файл установки.

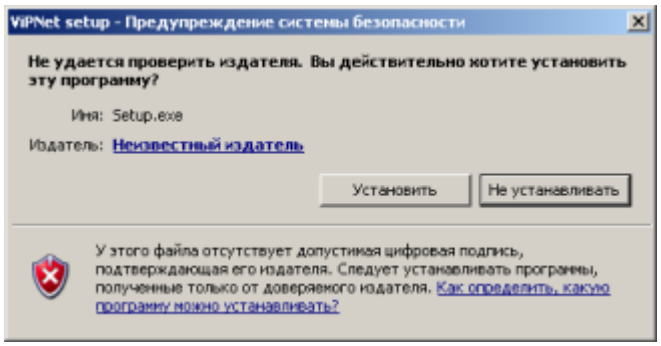


Рисунок 161: Невозможно проверить сертификат

Это может произойти, если отсутствует или недействителен корневой сертификат или какой-либо сертификат из цепочки сертификации.

Возможные варианты решения проблемы:

- С помощью кнопки **Не устанавливать** прервите установку программы, затем установите обновление операционной системы KB931125 (либо просто установите все обновления текущей версии вашей операционной системы). В результате цепочка сертификации будет обновлена, и сертификат, которым подписан файл установки, можно будет проверить.

  После обновления заново начните установку ViPNet Coordinator.

- При необходимости вы можете установить программу без обновления операционной системы. В этом случае в окне предупреждения системы безопасности нажмите кнопку **Установить**.

Установка программы не выполняется в неинтерактивном режиме

Если вы устанавливаете программу в неинтерактивном режиме на компьютер с операционной системой Windows XP или Windows Vista, вы можете обнаружить, что установка не выполняется: через несколько минут после запуска установки не проявляются признаки установки программы (например, возникновение ярлыка программы на рабочем столе). Это может быть связано с невозможностью проверить сертификат, которым подписан файл установки программы, из-за того что отсутствует или недействителен корневой сертификат или какой-либо сертификат из цепочки сертификации.

Для решения проблемы установите обновление операционной системы KB931125 (либо просто установите все обновления текущей версии вашей операционной системы). В результате цепочка сертификации будет обновлена, и сертификат, которым подписан файл установки, можно будет проверить. После обновления заново начните установку ViPNet Coordinator.

Невозможно запустить программу

Вероятно, программа ViPNet Монитор была удалена с компьютера либо были удалены файлы, необходимые для ее работы. Убедитесь в том, что программа ViPNet Монитор установлена и в случае необходимости переустановите ее либо обратитесь за помощью к администратору сети ViPNet.

Не найдены ключи пользователя или неверный пароль

В этом случае программа выдает следующее сообщение:

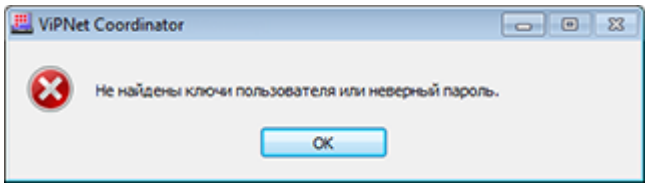


Рисунок 162: Сообщение о неверном пароле

Возможные варианты решения проблемы:

- Проверьте состояние клавиши **Caps Lock**.

- Проверьте раскладку клавиатуры, используя соответствующий индикатор в окне ввода пароля. Если используется случайный пароль, его следует набирать в английской раскладке клавиатуры.

- Проверьте правильность пароля и еще раз внимательно наберите пароль.

- Возможно, ключи пользователя установлены в папку, которая отличается от папки ключей пользователя по умолчанию.

  В этом случае в окне ввода пароля щелкните значок  справа от кнопки **Настройка**, в меню выберите пункт **Папка ключей пользователя** и укажите путь к папке ключей пользователя.

  Если операционная система еще не загружена, в окне ввода пароля ViPNet нажмите кнопку **Отмена**. После загрузки операционной системы запустите ViPNet Монитор и укажите путь к папке ключей пользователя.

Не удается выполнить аутентификацию с помощью сертификата

Если вам не удается войти в программу ViPNet Coordinator, используя для аутентификации сертификат и соответствующий ему закрытый ключ, которые хранятся на внешнем устройстве, это может быть вызвано одной из следующих причин:

- Внешнее устройство хранения данных не поддерживает стандарт PKCS#11. Проверить, поддерживает ли ваше устройство этот стандарт, можно по разделу Внешние устройства (на стр. 438).

- Срок действия выбранного сертификата истек. При выборе недействительного сертификата появится соответствующее сообщение. В этом случае следует передать сертификат администратору вашего удостоверяющего центра для обновления.

- Выбранный сертификат присутствует в списке отозванных сертификатов, который установлен в хранилище данного узла. При выборе отозванного сертификата появится соответствующее сообщение. В этом случае следует обратиться к администратору вашего удостоверяющего центра.

- Выбранный сертификат не имеет расширения «Проверка подлинности клиента». Это расширение должно отображаться в окне **Сертификат**, на вкладке **Состав**, в поле **Расширенное использование ключа**. В этом случае следует обратиться к администратору вашего удостоверяющего центра для переиздания сертификата.

- Сертификат издателя не установлен в системное хранилище **Доверенные корневые центры сертификации**. В этом случае следует получить сертификат издателя у администратора вашего удостоверяющего центра и установить его в указанное

системное хранилище. Для этого дважды щелкните по сертификату и следуйте указаниям мастера установки сертификатов.

Невозможно сохранить пароль

Чтобы предоставить возможность сохранения пароля, войдите в программу ViPNet Монитор в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304).

Невозможно подключиться к ресурсам в Интернете

Возможно, соединение с ресурсами Интернета заблокировано фильтрами открытой сети или заблокирован IP-трафик компьютера. Убедитесь, что настроены сетевые фильтры, разрешающие соединение с требуемыми адресами (см. «Создание локальных фильтров для открытой сети» на стр. 186), а также в том, что IP-трафик компьютера не заблокирован (об этом свидетельствует, например, наличие в меню **Файл** > **Конфигурации** команды **Блокировать IP-трафик**).

Невозможно установить соединение с защищенным узлом

Возможные причины:

- Сетевой узел выключен или на нем не запущена программа ViPNet Монитор.
- Нет ключей, необходимых для связи с сетевым узлом. Обратитесь к администратору сети ViPNet.
- Ваш компьютер физически не подключен к сети или не имеет выхода в Интернет.

Невозможно обратиться к узлам домена по DNS-имени

Если в сети ViPNet вашей организации используется служба Active Directory и при этом контроллеры домена с DNS-серверами, которые в рамках домена синхронизируются между собой, находятся на разных узлах ViPNet или туннелируются разными координаторами, то могут возникнуть проблемы разрешения IP-адресов при обращении к ним с других защищенных узлов. В этом случае выполните указания раздела Использование DNS-серверов на контроллерах домена (на стр. 154).

Невозможно установить соединение с открытым узлом в локальной сети

Возможные причины:

- IP-адрес открытого узла присутствует в списке защищенных узлов. В этом случае ViPNet-драйвер пытается послать зашифрованный пакет на открытый компьютер, установить соединение не удается. Для устранения данной проблемы необходимо удалить адрес открытого узла из списка адресов защищенных узлов.
- Неправильно настроены фильтры для работы с открытой сетью. Для нормальной работы в сетях Microsoft убедитесь, что включены и настроены нужные фильтры открытой сети (см. «Общие сведения о сетевых фильтрах» на стр. 159).

Невозможно установить соединение по протоколу SSL

Возможно, причиной неполадки является сбой одного из компонентов программы ViPNet Coordinator. Для решения данной проблемы выполните действия, описанные в разделе Невозможно запустить службу MSSQLSERVER (на стр. 376).

Невозможно установить соединение по протоколу PPPoE

Соединение по протоколу PPPoE может быть заблокировано программой ViPNet Монитор. Для решения данной проблемы выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройка приложения**.
2. В окне **Настройка** откройте раздел **Управление трафиком**.
3. Снимите флажок **Блокировать все протоколы, кроме IP, ARP**.
4. Нажмите кнопку **OK**.

Трафик от туннелируемых узлов не проходит через координатор

Данная проблема может возникать, когда туннелируемые узлы находятся в одной локальной подсети с координатором. При этом на сетевом интерфейсе координатора, за которым стоят туннелируемые узлы, задан шлюз по умолчанию.

Когда трафик от туннелируемых узлов, передаваемый на удаленные защищенные узлы, поступает на координатор, туннелируемым узлам по стеку TCP/IP координатора

посылаются сообщения по протоколу ICMP 5 о необходимости направлять трафик не на него, а напрямую на шлюз, заданный на координаторе. В результате туннелируемый трафик перестает передаваться на координатор и отправляется напрямую на шлюз по умолчанию.

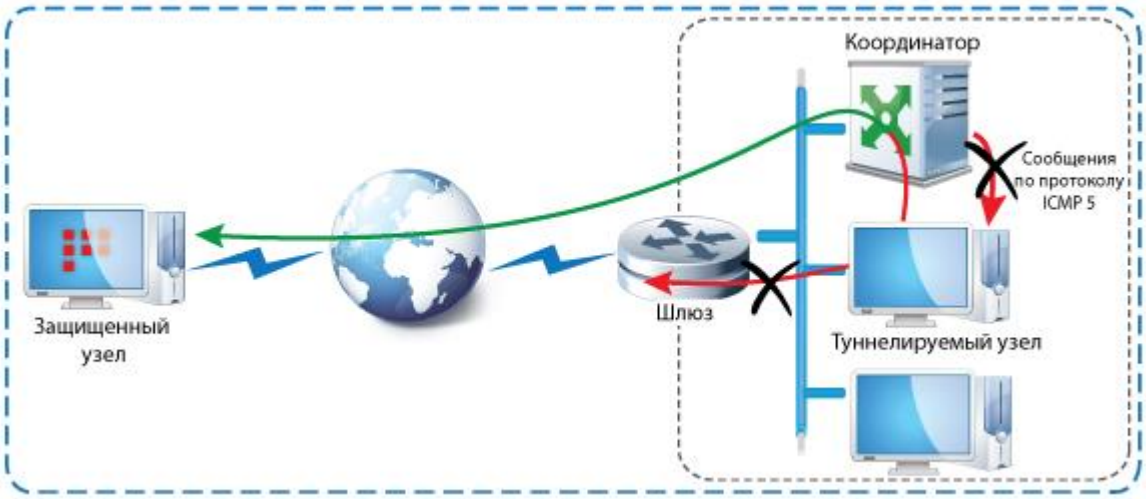


Рисунок 163: Блокирование сообщений по протоколу ICMP 5 для правильного прохождения туннелируемого трафика

Для устранения этой проблемы необходимо заблокировать отправку координатором сообщений по протоколу ICMP 5. Для этого в программе ViPNet Coordinator Монитор требуется создать фильтры открытой сети, блокирующие отправку данных сообщений. Вместе с этим также рекомендуется создать и аналогичные фильтры защищенной сети.

Примечание. Если вы установили программу ViPNet Coordinator на компьютере впервые (не обновляли программу с более ранних версий), данные фильтры в программе ViPNet Монитор будут заданы по умолчанию в предустановленных фильтрах защищенной и открытой сети (см. «Общие сведения о сетевых фильтрах» на стр. 159).

В сети зарегистрирован узел с таким же идентификатором, как у вашего узла

В этом случае:

- В журнале событий регистрируется событие с номером 95 (см. «Блокированные IP-пакеты» на стр. 419).
- Полностью блокируется весь IP-трафик.

- В программе ViPNet Монитор появляется следующее сообщение:

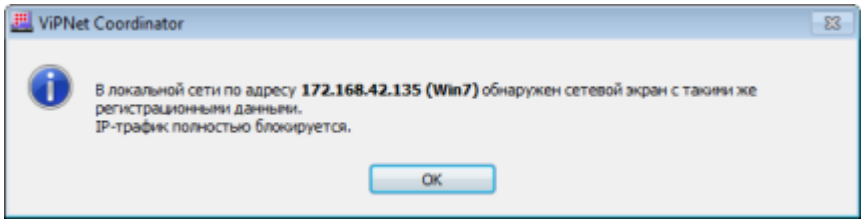


Рисунок 164: Сообщение о том, что в сети обнаружен узел с таким же идентификатором

Для устранения данной проблемы требуется удалить дубликат вашего узла из сети ViPNet (удалить на нем текущие ключи или установить новые ключи). После этого требуется перезагрузить ваш компьютер.

Обнаружен конфликт IP-адресов

При добавлении IP-адреса в процессе настройки доступа к защищенному или туннелируемому узлу может оказаться, что он совпадает с IP-адресом, заданным ранее для другого узла. Тогда появится следующее сообщение:

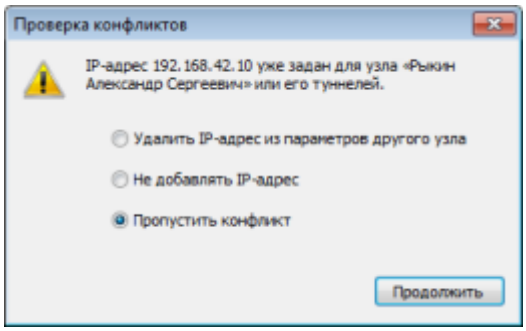


Рисунок 165: Действия при обнаружении пересечения IP-адресов

Конфликт IP-адресов также может быть обнаружен в ходе их проверки с помощью кнопки  . В этом случае появится такое сообщение:

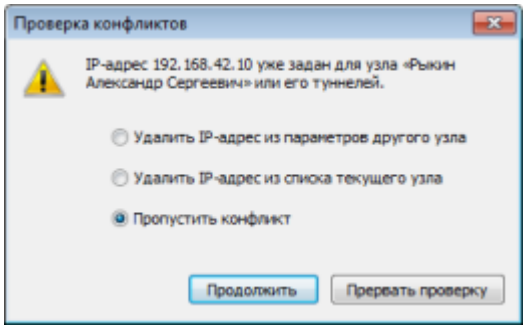


Рисунок 166: Действия при обнаружении пересечения IP-адресов

Для устранения конфликта IP-адресов вы можете:

- удалить повторяющийся IP-адрес из параметров другого узла (в списке IP-адресов доступа или IP-адресов туннелируемых узлов);
- не добавлять IP-адрес в первом случае, удалить IP-адрес из списка текущего узла — во втором.

Кроме этого, вы можете не учитывать возникший конфликт (в первом случае будет добавлен указанный IP-адрес), а также во втором случае прервать проверку.

Невозможно запустить службу MSSQLSERVER

Возможно, причиной неполадки является сбой одного из компонентов программы ViPNet Coordinator. Для решения данной проблемы выполните следующие действия:

1. В командной строке Windows выполните команду: `regsvr32 /u C:\Windows\System32\itcssp.dll`.
2. Измените имя файла `itcssp.dll`, находящегося в папке `C:\Windows\System32`, на любое другое.

   Если на компьютере была установлена программа ViPNet CSP с поддержкой 64-разрядных операционных систем, в папке `C:\Windows\SysWOW64` также существует файл `itcssp.dll`, который требуется переименовать.
3. Перезагрузите компьютер.

Невозможно изменить настройки в программе ViPNet Монитор

Изменение настроек программы ViPNet Монитор может быть невозможно по одной из следующих причин:

- На сетевом узле ограничены полномочия пользователя. Изменить настройки программы ViPNet Монитор может только пользователь с максимальным уровнем полномочий. Обратитесь к администратору сети ViPNet с просьбой повысить уровень полномочий в программе ViPNet Центр управления сетью.

Примечание. В сетях ViPNet VPN на клиентских узлах по умолчанию ограничен интерфейс программы ViPNet Client. Настройки программы можно выполнить только в режиме администратора сетевого узла.

- Установлены ограничения интерфейса в режиме администратора (см. «Работа в программе в режиме администратора» на стр. 304). Обратитесь к администратору сети ViPNet с просьбой снять ограничение.

Не удается использовать аппаратный датчик случайных чисел

Если требуется использовать в программном обеспечении ViPNet аппаратный датчик случайных чисел, выполните следующие действия:

1. На компьютере, на котором требуется использовать аппаратный датчик случайных чисел, в зависимости от используемой операционной системы выполните одно из следующих действий:
   - В Windows Vista и более поздних — создайте папку `C:\ProgramData\InfoTeCS\ViPNet CSP`.
   - В Windows XP и Windows Server 2003 — создайте папку `C:\Documents and Settings\All Users\Application Data\InfoTeCS\ViPNet CSP`.
2. В указанной папке создайте текстовый файл следующего содержания:

```
[Common]
EnableCspSupport=Yes
[Devices]
RandomNumberGeneratorType=<тип датчика>
```

3 В качестве значения параметра `RandomNumberGeneratorType` укажите тип датчика случайных чисел, который требуется использовать. Этот параметр может иметь следующие значения:

- `accord` — Аккорд-АМДЗ.
- `sobol` — электронный замок «Соболь».
- `bio` — электронная рулетка (используется в программном обеспечении ViPNet по умолчанию).
- `tokenJava` — eToken PRO (Java).
- `ruToken` — Rutoken ЭЦП.

4 Сохраните созданный файл, затем измените его имя и расширение на `csp_config.ini`.

При следующем вызове датчика случайных чисел будет использоваться указанный датчик.

Нарушение работоспособности сторонних приложений

Из-за специфики работы программного обеспечения ViPNet может быть нарушена работа сторонних приложений.

Для устранения конфликта ПО ViPNet со сторонними приложениями внесите изменения в системный реестр Windows:

1 В меню **Пуск** выберите пункт **Выполнить**.

2 В окне **Выполнить** в поле **Открыть** введите `regedit` и нажмите кнопку **OK**. Откроется окно **Редактор реестра**.

Внимание! Неправильное редактирование реестра может привести к возникновению неполадок в работе операционной системы, поэтому обязательно создайте резервную копию реестра. Это позволит восстановить реестр при возникновении неполадок.

3 В разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Infotecs\PatchEngine` присвойте параметру `Flags` значение 0.

4 Перезагрузите компьютер.

Если после выполнения указанных действий проблема не будет решена, обратитесь в службу технической поддержки компании «ИнфоТеКС».

Проверка статуса принятых обновлений

В случае, когда нет уверенности в том, были ли получены нужные обновления для ViPNet Coordinator и каков статус их выполнения, можно воспользоваться файлом, в котором хранятся записи обо всех обновлениях. Для этого:

1. В папке установки ПО ViPNet Coordinator (по умолчанию `c:\Program Files\InfoTeCS\ViPNet Coordinator\`) найдите файл `\CCC\log\update.log`.
2. Откройте этот файл с помощью текстового редактора и найдите записи о нужных обновлениях.

Ниже приведен пример файла `update.log`.

`Now is Tue Sep 01 14:19:16 2010`	Дата обновления
`Key upgrade done. Updated files` `C:\Program Files\InfoTeCS\ViPNet Coordinator\ccc\key\abn_06f2\353a5237 \ABN_06F2.KE`	Вид обновления — обновление ключевой информации. Статус — успешно.
`Now is Mon Oct 02 13:33:13 2006`	

`Address book upgrade done. Updated files`
`C:\Program Files\InfoTeCS\ViPNet Coordinator \EXTNET.DOC`
`C:\Program Files\InfoTeCS\ViPNet Coordinator \IPLIRADR.DOC`
	Вид обновления — обновление справочной информации. Статус — успешно.

Предупреждения сервиса безопасности

Предупреждения сервиса безопасности предназначены для своевременного информирования пользователя о таких событиях, как истечение сроков действия пароля, текущего сертификата, закрытого ключа и списка отозванных сертификатов, а также ввод в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр.

Проверка статуса пароля, текущего сертификата и закрытого ключа выполняется каждые 5 минут.

Срок действия пароля истек

Окно с сообщением об истечении срока действия пароля пользователя появляется в следующих случаях:

- Если в окне **Настройка параметров безопасности** на вкладке **Пароль** (см. Рисунок 137 на стр. 320) установлен флажок **Ограничить срок действия пароля** и задан срок действия пароля.

  Появление окна свидетельствует о том, что указанный срок подошел к концу.

- Если от программы ViPNet Удостоверяющий и ключевой центр получены ключи пользователя с новым паролем пользователя.

  При этом автоматической смены пароля не происходит, поэтому пароль необходимо сменить вручную (см. «Смена пароля пользователя» на стр. 319).

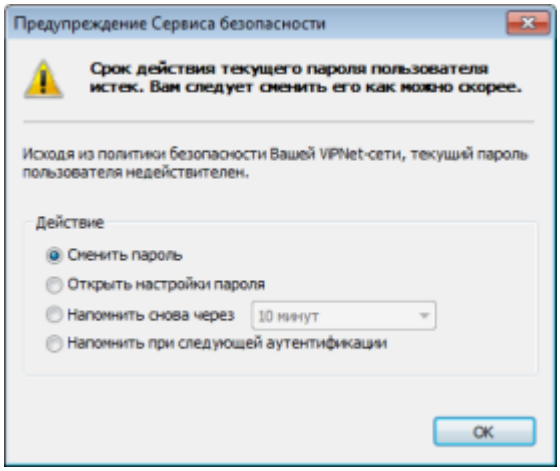


Рисунок 167: Предупреждение об истечении срока действия пароля пользователя

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий:
   - **Сменить пароль** — для указания нового пароля в соответствии с настройками, заданными в окне **Настройка параметров безопасности** на вкладке **Пароль** (см. Рисунок 137 на стр. 320);
   - **Открыть настройки пароля** — для вызова окна **Настройка параметров безопасности** на вкладке **Пароль** (см. Рисунок 137 на стр. 320), с помощью которой можно сперва задать параметры пароля, а затем сменить его;
   - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя);
   - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Coordinator.
2. Нажмите кнопку **ОК**.

Текущий сертификат не найден или недействителен

Окно с сообщением о том, что текущий сертификат не найден либо недействителен, появляется в следующих случаях:

- Если текущий сертификат не найден либо недействителен, однако найдены другие действительные личные сертификаты.

  В этом случае вы можете назначить один из них текущим, выбрав **Выбрать другой сертификат в качестве текущего**.

- Если не найден ни один действительный личный сертификат.

  В этом случае обратитесь к администратору вашей сети ViPNet для получения нового сертификата.

> **Внимание!** Пока не получен и не введен в действие новый сертификат, подписание электронных документов невозможно.

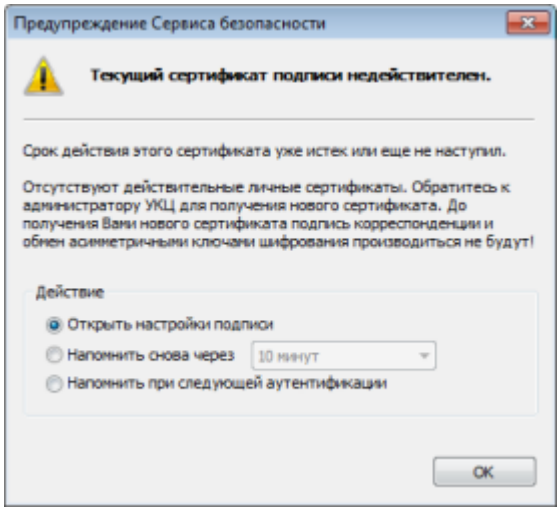


Рисунок 168: Предупреждение о том, что текущий сертификат недействителен

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий:
   - **Выбрать другой сертификат в качестве текущего** — для назначения другого действительного личного сертификата текущим с помощью окна **Выбор сертификата**.

> **Примечание.** Данное положение переключателя отображается в окне предупреждения в случае, если в хранилище пользователя найдены другие действительные личные сертификаты.

   - **Открыть настройки подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Подпись**, с помощью которой можно управлять сертификатами.

- **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временно*г*о промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
- **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Coordinator.

2 Нажмите кнопку **ОК**.

Срок действия текущего закрытого ключа или соответствующего сертификата близок к концу

Предупреждение о скором истечении срока действия закрытого ключа или соответствующего ему сертификата появляется в следующих случаях:

- Если срок действия закрытого ключа или сертификата близок к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворен, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае Вы можете сформировать запрос на обновление сертификата (см. «Процедура обновления закрытого ключа и сертификата» на стр. 342). Для этого:

  - если истекает срок действия сертификата, выберите **Отправить запрос на обновление сертификата**;
  - если истекает срок действия закрытого ключа, выберите **Открыть настройки подписи**, затем в окне **Настройка параметров безопасности** на вкладке **Подпись** нажмите кнопку **Обновить сертификат**.

- Если срок действия закрытого ключа или сертификата близок к концу, при этом последний запрос на обновление текущего сертификата либо отклонен, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

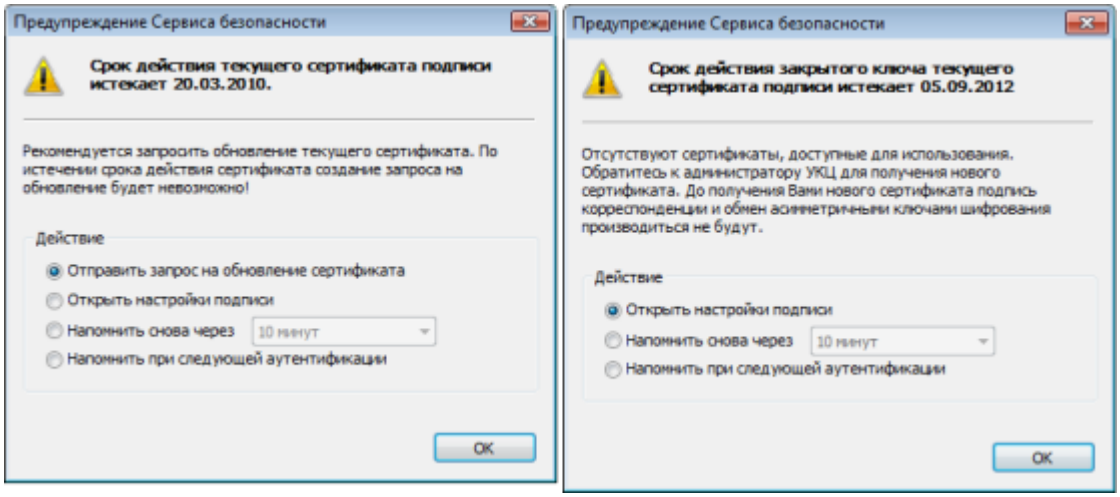


Рисунок 169: Предупреждения о скором истечении срока действия сертификата и закрытого ключа

При появлении окна с таким предупреждением:

1. В зависимости от вида предупреждения выберите одно из предложенных действий:
   - **Выбрать другой сертификат в качестве текущего** — для назначения другого действительного личного сертификата текущим с помощью окна **Выбор сертификата**.
   - **Отправить запрос на обновление сертификата** — для формирования запроса на обновление текущего сертификата с помощью мастера обновления сертификатов (см. «Процедура обновления закрытого ключа и сертификата» на стр. 342).
   - **Открыть настройки подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Подпись**, с помощью которой можно управлять сертификатами.
   - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
   - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Coordinator.
2. Нажмите кнопку **ОК**.

Срок действия текущего закрытого ключа уже истек

Предупреждение об истечении срока действия закрытого ключа появляется в следующих случаях:

- Если срок действия закрытого ключа подошел к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворен, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае вы можете открыть вкладку **Подпись** окна **Настройка параметров безопасности**, выбрав **Открыть настройки подписи**. С помощью соответствующей кнопки на вкладке **Подпись** вы можете обновить текущий сертификат (см. «Процедура обновления закрытого ключа и сертификата» на стр. 342). Однако в программе ViPNet Удостоверяющий и ключевой центр такой запрос не будет обработан автоматически, а будет ожидать решения администратора.

Внимание! Созданный запрос подписывается с использованием закрытого ключа, соответствующего текущему сертификату. Однако эта подпись используется не для подтверждения авторства, а только для проверки целостности запроса. Такие запросы имеют статус **Не подписан** (см. «Просмотр запроса на сертификат» на стр. 351).

- Если срок действия закрытого ключа подошел к концу, при этом последний запрос на обновление текущего сертификата либо отклонен, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

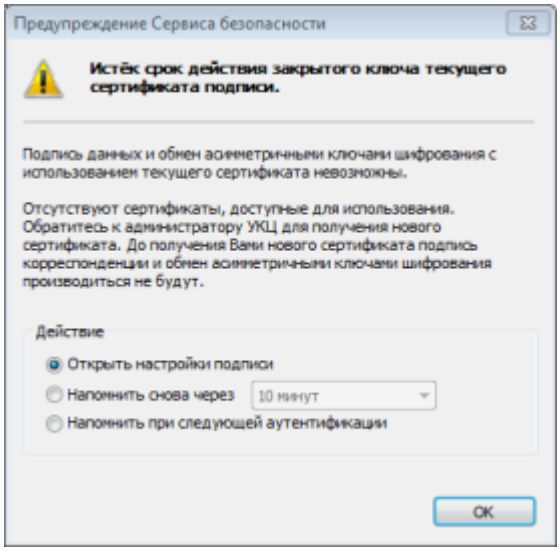


Рисунок 170: Предупреждение о том, что истек срок действия закрытого ключа

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий:
   - **Открыть настройки подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Подпись**, с помощью которой можно управлять сертификатами.
   - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
   - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Coordinator.
2. Нажмите кнопку **ОК**.

Действительный список отозванных сертификатов не найден

Предупреждение о том, что действительный список отозванных сертификатов не найден, появляется при выполнении следующих условий:

- если список отозванных сертификатов не обнаружен в хранилище пользователя или срок его действия истек;

- если в окне **Настройка параметров безопасности** на вкладке **Администратор** снят флажок **Игнорировать отсутствие списков отозванных сертификатов** (см. «Дополнительные настройки параметров безопасности» на стр. 311).

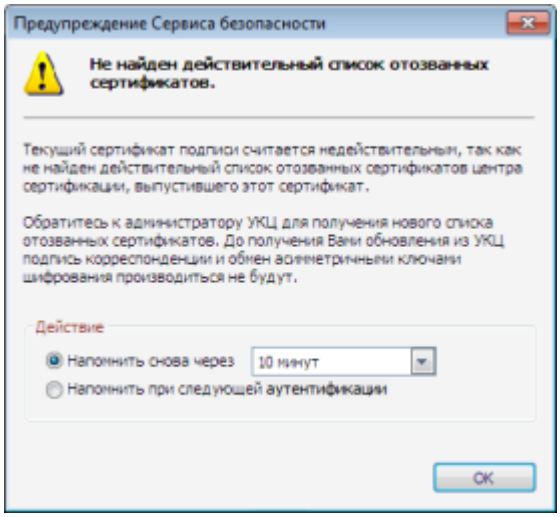


Рисунок 171: Предупреждение о том, что действительный список отозванных сертификатов не найден

При появлении окна с таким предупреждением:

- Обратитесь к администратору вашей сети ViPNet для получения нового списка отозванных сертификатов.
- Выберите одно из предложенных действий:
  - **Напомнить снова через** — для повторного вызова окна предупреждения по истечении указанного временного промежутка (10 минут, 1 час, 6 часов, 1 день, 1 неделя).
  - **Напомнить при следующей аутентификации** — для повторного вызова окна предупреждения при следующем запуске программы ViPNet Coordinator.

  После этого нажмите кнопку **ОК**.

Сертификат, изданный по инициативе администратора, введен в действие

Предупреждение о том, что введен в действие сертификат, изданный по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, появляется при выполнении следующих условий:

- В окне **Настройка параметров безопасности** на вкладке **Подпись** (см. Рисунок 146 на стр. 342) установлен флажок **Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ**.
- В составе обновления получены ключи, сформированные администратором программы ViPNet Удостоверяющий и ключевой центр без запроса со стороны пользователя и содержащие новый сертификат пользователя и закрытый ключ.

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий:
   - **Открыть настройки подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Подпись** (см. Рисунок 146 на стр. 342), с помощью которой можно просмотреть сведения о текущем сертификате, а также управлять сертификатами.
   - **Отправить запрос на обновление сертификата** — для формирования запроса на обновление текущего сертификата с помощью мастера обновления сертификатов (см. «Процедура обновления закрытого ключа и сертификата» на стр. 342).

     Отправлять запрос на обновление сертификата следует в том случае, если политика безопасности вашей организации запрещает использовать закрытый ключ, сформированный не вами лично, а на сетевом узле администратора. В результате обновления вам будет доставлен сертификат, которому будет соответствовать закрытый ключ, сформированный на вашем компьютере.
2. Нажмите кнопку **OK**.

Общие сведения о сертификатах и ключах

Основы криптографии

Криптография используется для решения трех основных задач:

- обеспечение конфиденциальности данных;
- контроль целостности данных;
- обеспечение подлинности авторства данных.

Первая задача решается с помощью симметричных алгоритмов шифрования. Для решения второй и третьей задач требуется использование асимметричных алгоритмов и электронной подписи.

В данном разделе содержится упрощенное описание алгоритмов с симметричным ключом, с асимметричным ключом, электронной подписи, а также приводятся примеры использования этих алгоритмов в информационных системах (приведенные примеры не относятся к технологии ViPNet).

Симметричное шифрование

В симметричных алгоритмах для зашифрования и расшифрования применяется один и тот же криптографический ключ. Для того чтобы и отправитель, и получатель могли прочитать исходный текст (или другие данные, не обязательно текстовые), обе стороны должны знать ключ алгоритма.

На схеме ниже изображен процесс симметричного зашифрования и расшифрования.

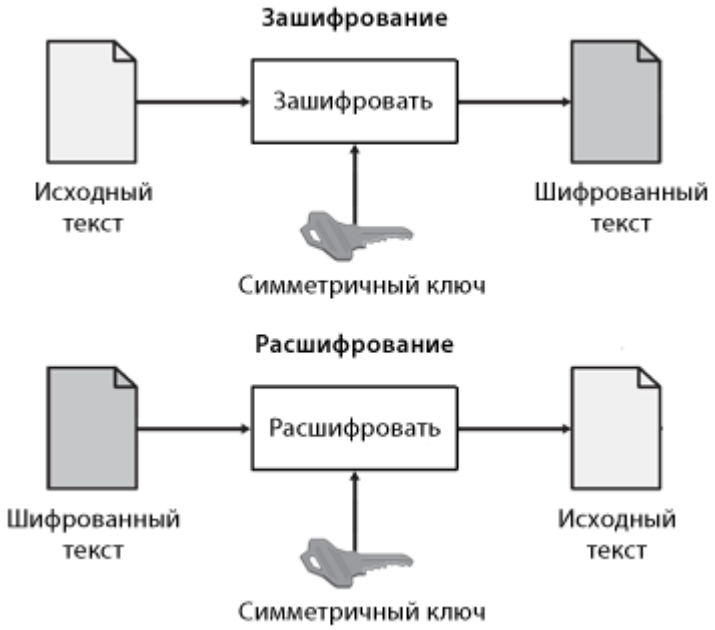


Рисунок 172: Зашифрование и расшифрование на симметричном ключе

Симметричные алгоритмы шифрования способны обрабатывать большое количество данных за короткое время благодаря использованию для зашифрования и расшифрования одного и того же ключа, а также благодаря простоте симметричных алгоритмов по сравнению с асимметричными. Поэтому симметричные алгоритмы часто используют для шифрования больших массивов данных.

Для шифрования данных с помощью симметричного алгоритма криптографическая система использует симметричный ключ. Длина ключа (обычно выражаемая в битах) зависит от алгоритма шифрования и программы, которая использует этот алгоритм.

С помощью симметричного ключа исходный (открытый) текст преобразуется в шифрованный (закрытый) текст. Затем шифрованный текст отправляется получателю. Если получателю известен симметричный ключ, на котором зашифрован текст, получатель может преобразовать шифрованный текст в исходный вид.

Примечание. На практике симметричный ключ нужно передать получателю каким-либо надежным способом. Обычно создается симметричный ключ парной связи, который передается получателю лично. Затем для шифрования используются случайные (сессионные) симметричные ключи, которые зашифровываются на ключе парной связи и в таком виде предаются по различным каналам вместе с шифрованным текстом.

Наибольшую угрозу безопасности информации при симметричном шифровании представляет перехват симметричного ключа парной связи. Если он будет перехвачен, злоумышленники смогут расшифровать все данные, зашифрованные

на этом ключе.

Асимметричное шифрование

Асимметричные алгоритмы шифрования используют два математически связанных ключа: открытый ключ и закрытый ключ. Для зашифрования применяется открытый ключ, для расшифрования — закрытый ключ.

Открытый ключ распространяется свободно. Закрытым ключом владеет только пользователь, который создает пару асимметричных ключей. Закрытый ключ следует хранить в секрете, чтобы исключить возможность его перехвата.

Использование двух различных ключей для зашифрования и расшифрования, а также более сложный алгоритм делают процесс шифрования с помощью асимметричных ключей гораздо более медленным, чем шифрование с помощью симметричных ключей.

Открытый ключ может быть использован любыми лицами для отправки зашифрованных данных владельцу закрытого ключа. При этом парой ключей владеет только получатель зашифрованных данных. Таким образом, только получатель может расшифровать эти данные с помощью имеющегося у него закрытого ключа.

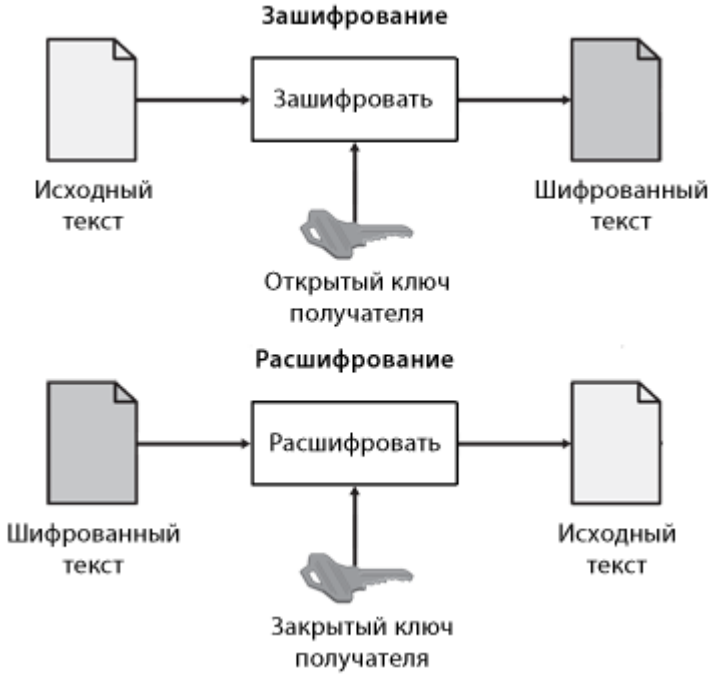


Рисунок 173: Зашифрование и расшифрование на асимметричном ключе

Примечание. На практике асимметричные алгоритмы в чистом виде используются очень редко. Обычно данные зашифровываются с помощью симметричного алгоритма, а затем с помощью асимметричного алгоритма зашифровывается только симметричный ключ. Комбинированные (гибридные) криптографические алгоритмы рассматриваются ниже (см. «Сочетание симметричного и асимметричного шифрования» на стр. 393).

Сочетание симметричного и асимметричного шифрования

В большинстве приложений симметричные и асимметричные алгоритмы применяются совместно, что позволяет использовать преимущества обоих алгоритмов.

В случае совместного использования симметричного и асимметричного алгоритмов:

- Исходный текст преобразуется в шифрованный с помощью симметричного алгоритма шифрования. Преимущество этого алгоритма заключается в высокой скорости шифрования.
- Для передачи получателю симметричный ключ, на котором был зашифрован текст, зашифровывается с помощью асимметричного алгоритма. Преимущество асимметричного алгоритма заключается в том, что только владелец закрытого ключа сможет расшифровать симметричный ключ.

На следующем рисунке изображен процесс шифрования с помощью комбинированного алгоритма.

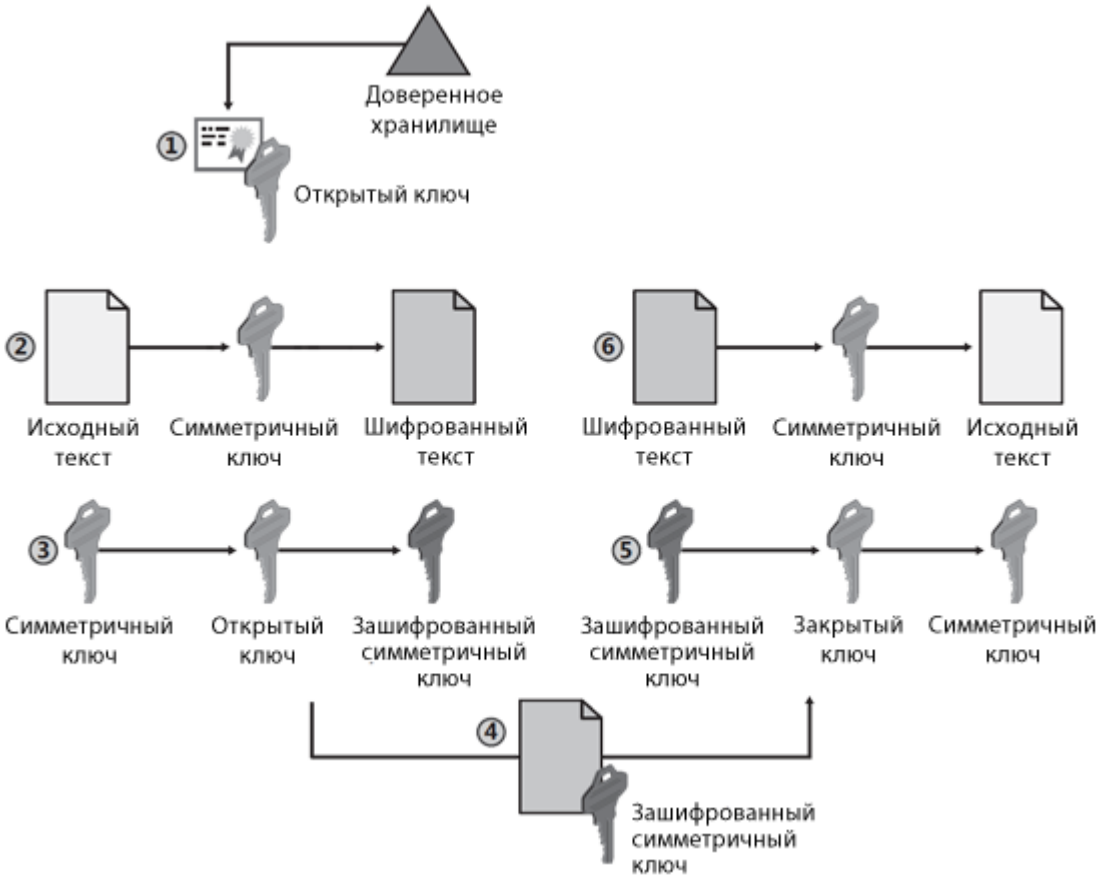


Рисунок 174: Шифрование с помощью комбинированного алгоритма

1 Отправитель запрашивает открытый ключ получателя из доверенного хранилища.

2 Отправитель создает симметричный ключ и зашифровывает с его помощью исходный текст.

3 Симметричный ключ зашифровывается на открытом ключе получателя, чтобы предотвратить перехват ключа во время передачи.

4 Зашифрованный симметричный ключ и шифрованный текст передаются получателю.

5 С помощью своего закрытого ключа получатель расшифровывает симметричный ключ.

6 С помощью симметричного ключа получатель расшифровывает шифрованный текст, в результате он получает исходный текст.

Сочетание хэш-функции и асимметричного алгоритма электронной подписи

Электронная подпись защищает данные следующим образом:

- Для подписания данных используется хэш-функция, с помощью которой определяется хэш-сумма исходных данных. По хэш-сумме можно определить, имеют ли место какие-либо изменения в этих данных.
- Полученная хэш-сумма подписывается электронной подписью, позволяя подтвердить личность подписавшего. Кроме того, электронная подпись не позволяет подписавшему лицу отказаться от авторства, так как только оно владеет закрытым ключом, использованным для подписания. Невозможность отказаться от авторства называется неотрекаемостью.

Большинство приложений, осуществляющих электронную подпись, используют сочетание хэш-функции и асимметричного алгоритма подписи. Хэш-функция позволяет проверить целостность исходного сообщения, а электронная подпись защищает полученную хэш-функцию от изменения и позволяет определить личность автора сообщения.

Приведенная ниже схема иллюстрирует применение хэш-функции и асимметричного алгоритма в электронной подписи.

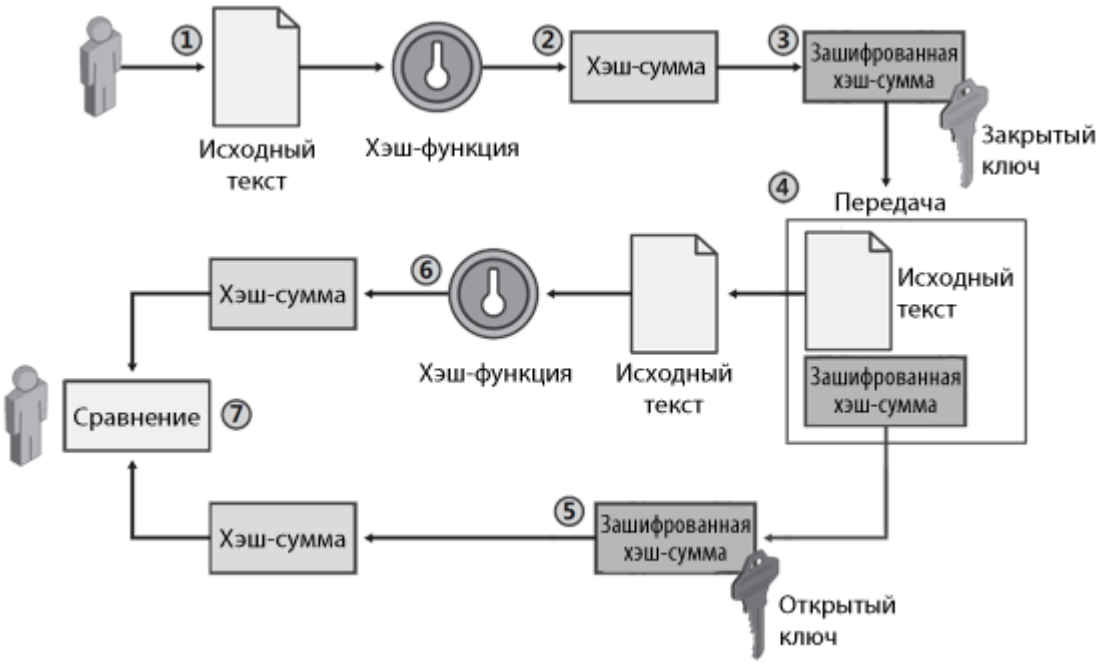


Рисунок 175: Применение хэш-функции и асимметричного алгоритма в электронной цифровой подписи

1 Отправитель создает файл с исходным сообщением.

2 Программное обеспечение отправителя вычисляет хэш-сумму исходного сообщения.

3 Полученная хэш-сумма зашифровывается с помощью закрытого ключа отправителя.

4 Исходное сообщение и зашифрованная хэш-функция передаются получателю.

Примечание. При использовании электронной подписи исходное сообщение не зашифровывается. Само сообщение может быть изменено, но любые изменения сделают хэш-сумму, передаваемую вместе с сообщением, недействительной.

---

5 Получатель расшифровывает хэш-сумму сообщения с помощью открытого ключа отправителя. Открытый ключ может быть передан вместе с сообщением или получен из доверенного хранилища.

6 Получатель используют ту же хэш-функцию, что и отправитель, чтобы вычислить хэш-сумму полученного сообщения.

7 Вычисленная хэш-сумма сравнивается с хэш-суммой, полученной от отправителя. Если эти хэш-суммы различаются между собой, то сообщение или хэш-сумма были изменены при передаче.

Общие сведения о сертификатах открытых ключей

Определение и назначение

Сертификат открытого ключа является одним из объектов криптографии с открытым ключом, в которой для прямого и обратного преобразований используются разные ключи:

- Закрытый ключ — для формирования электронной подписи (см. «Электронная подпись» на стр. 494) и расшифрования сообщения. Закрытый ключ хранится в тайне и не подлежит распространению.
- Открытый ключ — для проверки электронной подписи и зашифрования сообщения. Открытый ключ известен всем участникам информационного обмена и может передаваться по незащищенным каналам связи.

Таким образом, криптография с открытым ключом позволяет выполнять следующие операции:

- Подписание сообщения — формирование электронной подписи, прикрепление ее к сообщению и проверка электронной подписи на стороне получателя;
- Шифрование — зашифрование документа с возможностью расшифрования на стороне получателя.

Открытый и закрытый ключи являются комплементарными по отношению друг к другу — только владелец закрытого ключа может подписать данные, а также расшифровать данные, которые были зашифрованы открытым ключом, соответствующим закрытому ключу владельца. Простой аналогией может служить почтовый ящик: любой может кинуть письмо в почтовый ящик («зашифровать»), но только владелец секретного (закрытого) ключа может извлечь письма из ящика («расшифровать»).

Поскольку открытый ключ распространяется публично, существует опасность того, что злоумышленник, подменив открытый ключ одного из пользователей, может выступать от его имени. Для обеспечения доверия к открытым ключам создаются удостоверяющие

центры (согласно Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года), которые играют роль доверенной третьей стороны и заверяют открытые ключи каждого из пользователей своими электронными подписями — иначе говоря, сертифицируют эти открытые ключи.

Сертификат открытого ключа (далее — сертификат) представляет собой цифровой документ, заверенный электронной подписью удостоверяющего центра и призванный подтверждать принадлежность открытого ключа определенному пользователю.

Примечание. Несмотря на то, что защита сообщений выполняется фактически с помощью открытого ключа, в профессиональной речи используются выражения «подписать сертификатом (с помощью сертификата)», «зашифровать на сертификате (с помощью сертификата)».

Сертификат включает открытый ключ и список дополнительных атрибутов, принадлежащих пользователю (владельцу сертификата). К таким атрибутам относятся: имена владельца и издателя сертификата, номер сертификата, время действия сертификата, предназначение открытого ключа (электронная подпись, шифрование) и так далее. Структура и протоколы использования сертификатов определяются международными стандартами (см. «Структура» на стр. 400).

Различаются следующие виды сертификатов:

- Сертификат пользователя — для зашифрования исходящих сообщений и для проверки электронной подписи на стороне получателя.
- Сертификат издателя — сертификат, с помощью которого был издан текущий сертификат пользователя. Помимо основных возможностей, которые предоставляет сертификат пользователя, сертификат издателя позволяет также проверить все сертификаты, подписанные с помощью закрытого ключа, соответствующего этому сертификату.
- Корневой сертификат — самоподписанный сертификат издателя, являющийся главным из вышестоящих сертификатов. Корневой сертификат не может быть проверен с помощью другого сертификата, поэтому пользователь должен безусловно доверять источнику, из которого получен данный сертификат.
- Кросс-сертификат — это сертификат администратора удостоверяющего центра, изданный администратором другого удостоверяющего центра. Таким образом, для кросс-сертификата значения полей «Издатель» и «Субъект» различны и определяют разные удостоверяющие центры. С помощью кросс-сертификатов устанавливаются доверительные отношения между различными удостоверяющими центрами. В зависимости от модели доверительных отношений, установленной между удостоверяющими центрами (см. «Роль PKI для криптографии с открытым

ключом» на стр. 403), может использоваться либо как сертификат издателя (в иерархической модели), либо для проверки сертификатов пользователей другой сети (в распределенной модели).

Рисунок 176: Типы сертификатов

Используя корневой сертификат, каждый пользователь может проверить достоверность сертификата, выпущенного удостоверяющим центром, и воспользоваться его содержимым. Если проверка сертификата по цепочке сертификатов, начиная с корневого, показала, что он является законным, действующим, не был просрочен или отозван, то сертификат считается действительным. Документы, подписанные действительным сертификатом и не изменявшиеся с момента их подписания, также считаются действительными.

Таким образом, криптография с открытым ключом и инфраструктура обмена сертификатами открытых ключей (см. «Роль PKI для криптографии с открытым ключом» на стр. 403) позволяют выполнять шифрование сообщений, а также предоставляют возможность подписывать сообщения с помощью электронной подписи.

Посредством шифрования конфиденциальная информация может быть передана по незащищенным каналам связи. В свою очередь, электронная подпись позволяет обеспечить:

- Подлинность (аутентификация) — возможность однозначно идентифицировать отправителя. Если сравнивать с бумажным документооборотом, то это аналогично собственноручной подписи отправителя.
- Целостность — защиту информации от несанкционированной модификации как при хранении, так и при передаче.
- Неотрекаемость — невозможность для отправителя отказаться от совершенного действия. Если сравнивать с бумажным документооборотом, то это аналогично предъявлению отправителем паспорта перед выполнением действия.

Структура

Чтобы сертификат можно было использовать, он должен обладать доступной универсальной структурой, позволяющей извлечь из него нужную информацию и легко ее понять. Например, благодаря тому, что паспорта имеют простую однотипную структуру, можно легко понять информацию, изложенную в паспорте любого государства, даже если вы никогда не видели раньше таких паспортов. Так же дело обстоит и с сертификатами: стандартизация форматов сертификатов позволяет читать и понимать их независимо от того, кем они были изданы.

Один из форматов сертификата открытого ключа определен в рекомендациях Международного Союза по телекоммуникациям (International Telecommuncations Union, ITU) X.509 | ISO/IEC 9594–8 и документе RFC 3280 Certificate & CRL Profile Организации инженерной поддержки Интернета (Internet Engineering Task Force, IETF). В настоящее время наиболее распространенной версией X.509 является версия 3, позволяющая задать для сертификата расширения, с помощью которых можно разместить в сертификате дополнительную информацию (о политиках безопасности, использовании ключа, совместимости и так далее).

Сертификат содержит элементы данных, сопровождаемые электронной подписью издателя сертификата. В сертификате имеются обязательные и дополнительные поля.

К обязательным полям относятся:

- номер версии стандарта X.509,
- серийный номер сертификата,
- идентификатор алгоритма подписи издателя,

- идентификатор алгоритма подписи владельца,
- имя издателя,
- период действия,
- открытый ключ владельца,
- имя владельца сертификата.

Примечание. Под владельцем понимается сторона, контролирующая закрытый ключ, соответствующий данному открытому ключу. Владельцем сертификата может быть конечный пользователь или удостоверяющий центр.

К необязательным полям относятся:

- уникальный идентификатор издателя,
- уникальный идентификатор владельца,
- расширения сертификата.

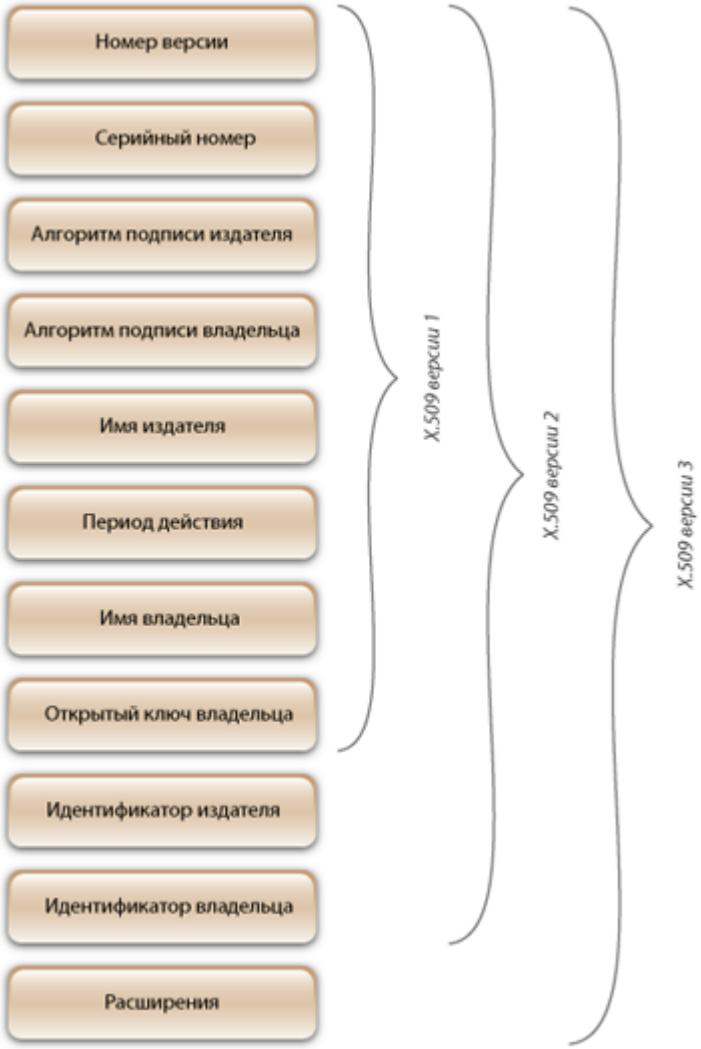
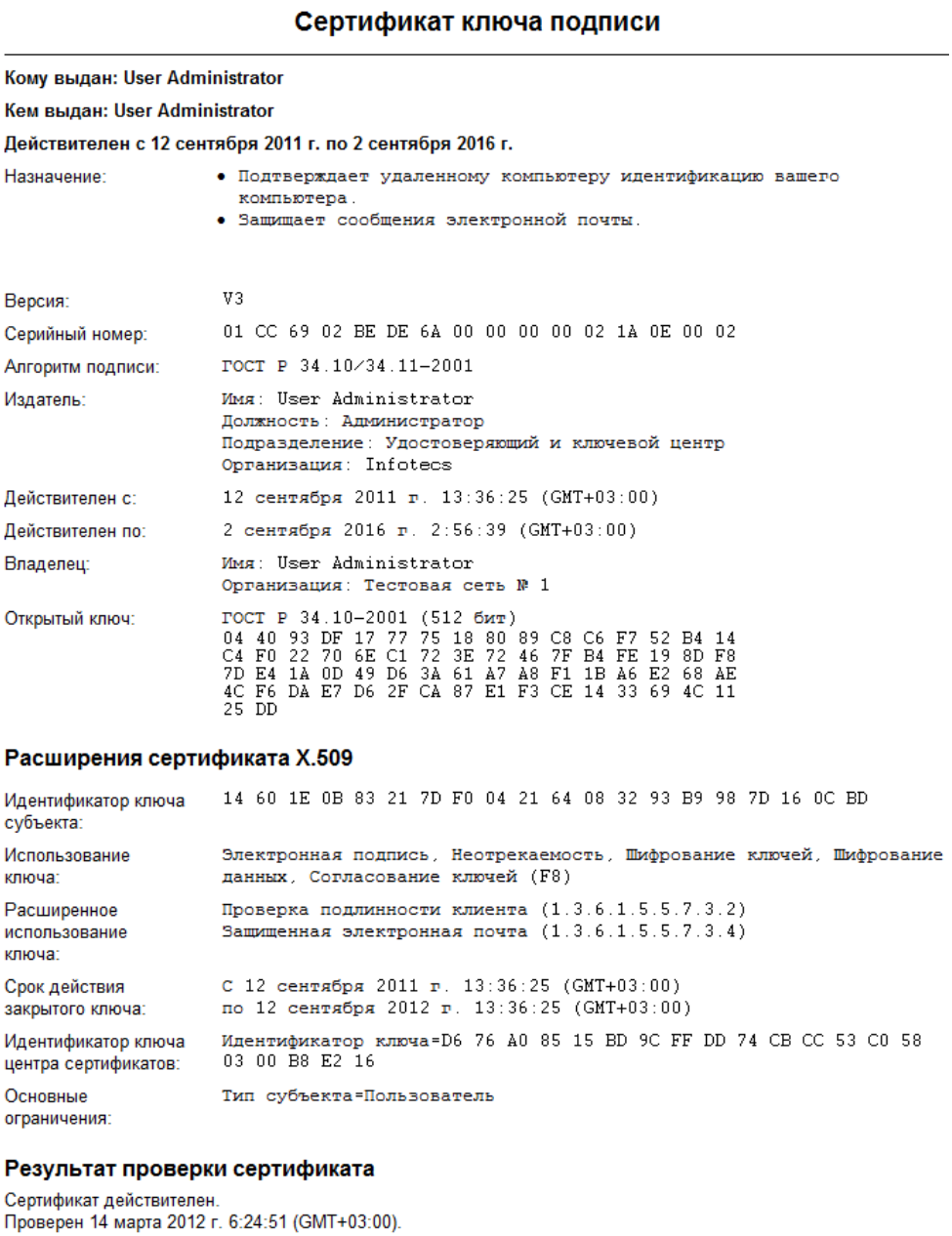


Рисунок 177: Структура сертификата, соответствующего стандарту X.509 версий 1, 2 и 3



Сертификат ключа подписи

Кому выдан: User Administrator

Кем выдан: User Administrator

Действителен с 12 сентября 2011 г. по 2 сентября 2016 г.

Назначение:
- Подтверждает удаленному компьютеру идентификацию вашего компьютера.
- Защищает сообщения электронной почты.

Версия:	V3
Серийный номер:	01 CC 69 02 BE DE 6A 00 00 00 00 02 1A 0E 00 02
Алгоритм подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: User Administrator Должность: Администратор Подразделение: Удостоверяющий и ключевой центр Организация: Infotecs
Действителен с:	12 сентября 2011 г. 13:36:25 (GMT+03:00)
Действителен по:	2 сентября 2016 г. 2:56:39 (GMT+03:00)
Владелец:	Имя: User Administrator Организация: Тестовая сеть № 1
Открытый ключ:	ГОСТ Р 34.10-2001 (512 бит) 04 40 93 DF 17 77 75 18 80 89 C8 C6 F7 52 B4 14 C4 F0 22 70 6E C1 72 3E 72 46 7F B4 FE 19 8D F8 7D E4 1A 0D 49 D6 3A 61 A7 A8 F1 1B A6 E2 68 AE 4C F6 DA E7 D6 2F CA 87 E1 F3 CE 14 33 69 4C 11 25 DD

Расширения сертификата X.509

Идентификатор ключа субъекта:	14 60 1E 0B 83 21 7D F0 04 21 64 08 32 93 B9 98 7D 16 0C BD
Использование ключа:	Электронная подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8)
Расширенное использование ключа:	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Срок действия закрытого ключа:	С 12 сентября 2011 г. 13:36:25 (GMT+03:00) по 12 сентября 2012 г. 13:36:25 (GMT+03:00)
Идентификатор ключа центра сертификатов:	Идентификатор ключа=D6 76 A0 85 15 BD 9C FF DD 74 CB CC 53 C0 58 03 00 B8 E2 16
Основные ограничения:	Тип субъекта=Пользователь

Результат проверки сертификата

Сертификат действителен.
Проверен 14 марта 2012 г. 6:24:51 (GMT+03:00).

Рисунок 178: Пример сертификата ViPNet, соответствующего стандарту X.509 версии 3

Роль PKI для криптографии с открытым ключом

Для сертификатов требуется инфраструктура, которая позволяла бы управлять ими в той среде, в которой эти сертификаты предполагается использовать. Одной из реализаций такой инфраструктуры является технология PKI (Public Key Infrastructure — инфраструктура открытых ключей). PKI обслуживает жизненный цикл сертификата:

издание сертификатов, хранение, резервное копирование, печать, взаимную сертификацию, ведение списков отозванных сертификатов (СОС), автоматическое обновление сертификатов после истечения срока их действия.

Основой технологии PKI являются отношения доверия, а главным управляющим компонентом — удостоверяющий центр. Удостоверяющий центр предназначен для регистрации пользователей, выпуска сертификатов, их хранения, выпуска СОС и поддержания его в актуальном состоянии. В сетях ViPNet удостоверяющий центр издает сертификаты как по запросам от пользователей, сформированным в специальной программе (например, ViPNet CSP или ViPNet Client), так и без запросов (в процессе создания пользователей ViPNet).

Для сетей с большим количеством пользователей создается несколько удостоверяющих центров. Доверительные отношения между этими удостоверяющими центрами могут выстраиваться по распределенной или иерархической модели.

- В иерархической модели доверительных отношений удостоверяющие центры объединяются в древовидную структуру, в основании которой находится головной удостоверяющий центр. Головной удостоверяющий центр выдает кросс-сертификаты подчиненным ему центрам, тем самым обеспечивая доверие к открытым ключам этих центров. Каждый удостоверяющий центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие к сертификату открытого ключа каждого удостоверяющего центра основано на заверении его ключом вышестоящего центра. Сертификат головного удостоверяющего центра (корневой сертификат (на стр. 486)) является самоподписанным. В остальных удостоверяющих центрах администраторы не имеют собственных корневых сертификатов и для установления доверительных отношений формируют запросы на кросс-сертификат к своим вышестоящим удостоверяющим центрам.

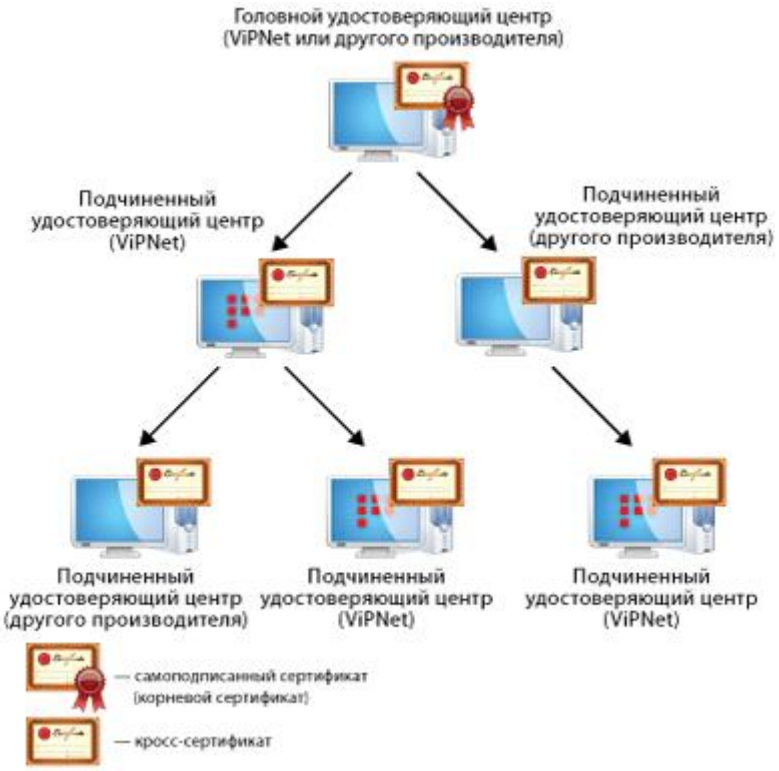


Рисунок 179: Иерархическая модель доверительных отношений

- В распределенной модели доверительных отношений все удостоверяющие центры равнозначны: в каждом удостоверяющем центре администратор имеет свой корневой (самоподписанный) сертификат. Доверительные отношения между удостоверяющими центрами в этой модели устанавливаются обычно путем двусторонней кросс-сертификации, когда два удостоверяющих центра издают кросс-сертификаты друг для друга. Взаимная кросс-сертификация проводится попарно между всеми удостоверяющими центрами. В результате в каждом удостоверяющем центре в дополнение к корневому сертификату имеются кросс-сертификаты, изданные для администраторов в других удостоверяющих центрах.

  Для подписания сертификатов пользователей каждый удостоверяющий центр продолжает пользоваться своим корневым сертификатом, а кросс-сертификат, изданный для другого удостоверяющего центра, использует для проверки сертификатов пользователей другой сети. Это возможно в силу того, кросс-сертификат для доверенного удостоверяющего центра издается на базе его корневого сертификата и содержит сведения о его открытом ключе. Поэтому в сети, отправившей запрос, нет необходимости переиздавать сертификаты пользователей.

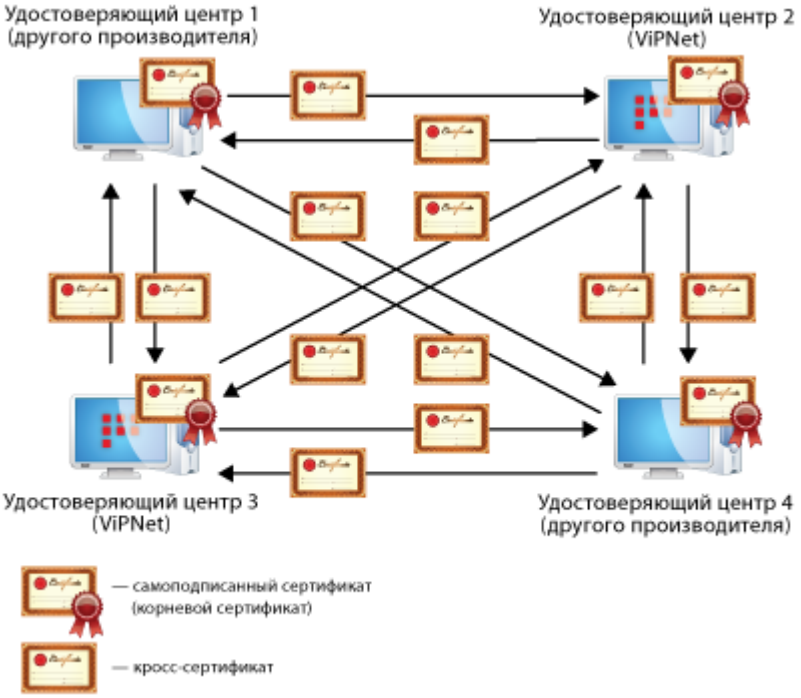


Рисунок 180: Распределенная модель доверительных отношений

Зная иерархию и подчиненность удостоверяющих центров друг другу, можно всегда точно установить, является ли тот или иной пользователь владельцем данного открытого ключа.

Использование сертификатов для шифрования электронных документов

Отправитель может зашифровать документ с помощью открытого ключа получателя, при этом расшифровать документ сможет только сам получатель. В данном случае для зашифрования применяется сертификат получателя сообщения.

Зашифрование

1. Пользователь создает электронный документ.
2. Открытый ключ получателя извлекается из сертификата.
3. Формируется симметричный сеансовый ключ (на стр. 490), для однократного использования в рамках данного сеанса.

4 Подписанный документ зашифровывается с использованием сеансового ключа (в соответствии с алгоритмом ГОСТ 28147–89).

5 Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана (см. «Протокол Диффи — Хеллмана» на стр. 489) с использованием открытого ключа получателя.

6 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

7 Документ отправляется.

Рисунок 181: Процесс зашифрования электронных документов

Расшифрование

1 Пользователь получает электронный документ.

2 Зашифрованное содержимое документа и зашифрованный сеансовый ключ извлекаются из документа.

3 Закрытый ключ получателя документа извлекается из контейнера ключей.

4 Сеансовый ключ расшифровывается с использованием закрытого ключа получателя.

5 Документ расшифровывается с использованием расшифрованного сеансового ключа.

6 Расшифрованный документ доступен получателю.

Рисунок 182: Процесс расшифрования электронных документов

Использование сертификатов для подписания электронных документов

Когда отправитель подписывает документ, он использует закрытый ключ, соответствующий открытому ключу, который хранится в сертификате. Когда получатель проверяет электронную подпись (см. «Электронная подпись» на стр. 494) сообщения, он извлекает открытый ключ из сертификата отправителя.

Подписание

1. Пользователь создает электронный документ.
2. Вычисляется значение хэш-функции документа.

   Хэш-функция документа используется при формировании электронной подписи на стороне отправителя, а также при дальнейшей проверке электронной подписи на стороне получателя.
3. Закрытый ключ отправителя извлекается из контейнера ключей.
4. С использованием закрытого ключа отправителя на основе значения хэш-функции формируется электронная подпись.
5. Электронная подпись прикрепляется к документу.
6. Зашифрованный документ отправляется.

Рисунок 183: Процесс подписания электронного документа

Проверка подписи

1. Пользователь получает электронный документ.
2. Электронная подпись (зашифрованное значение хэш-функции) извлекается из документа.
3. Вычисляется значение хэш-функции документа.
4. Открытый ключ отправителя извлекается из сертификата отправителя.
5. Электронная подпись расшифровывается с использованием открытого ключа отправителя.
6. Значение хэш-функции электронной подписи сравнивается с полученным значением хэш-функции документа.
7. Если значения хэш-функций совпадают, электронная подпись документа считается действительной.

   Если значения хэш-функций не совпадают (то есть полученный документ был изменен с момента подписания), электронная подпись документа считается недействительной. Подпись считается недействительной также в том случае, если сертификат отправителя просрочен, отозван, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

Рисунок 184: Процесс проверки подписи

Использование сертификатов для подписания и шифрования электронных документов

Подписание и зашифрование

1. Пользователь создает электронный документ.
2. Вычисляется значение хэш-функции документа.
3. Закрытый ключ отправителя извлекается из контейнера ключей.
4. Открытый ключ получателя извлекается из сертификата получателя.
5. С использованием закрытого ключа отправителя на основе значения хэш-функции формируется электронная подпись.
6. Электронная подпись прикрепляется к документу.
7. Формируется симметричный сеансовый ключ (на стр. 490), для однократного использования в рамках данного сеанса.
8. Подписанный документ зашифровывается с использованием сеансового ключа (в соответствии с алгоритмом ГОСТ 28147–89).

9 Сеансовый ключ зашифровывается на ключе, который вырабатывается по протоколу Диффи — Хеллмана (см. «Протокол Диффи — Хеллмана» на стр. 489) с использованием открытого ключа получателя.

10 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

11 Документ отправляется.

Рисунок 185: Процесс подписания и зашифрования электронных документов

Расшифрование и проверка

1 Пользователь получает электронный документ.

2 Зашифрованное содержимое документа и зашифрованный сеансовый ключ извлекаются из сообщения.

3 Закрытый ключ получателя документа извлекается из контейнера ключей.

4 Сеансовый ключ расшифровывается с помощью закрытого ключа получателя.

5 Документ расшифровывается с использованием расшифрованного сеансового ключа.

6 Электронная подпись (зашифрованное значение хэш-функции) извлекается из документа.

7 Вычисляется значение хэш-функции документа.

8 Открытый ключ отправителя извлекается из сертификата отправителя.

9 Электронная подпись расшифровывается с использованием открытого ключа отправителя.

10 Значение хэш-функции электронной подписи сравнивается с полученным значением хэш-функции документа.

11 Если значения хэш-функций совпадают, электронная подпись документа считается действительной.

Если значения хэш-функций не совпадают (то есть полученный документ был изменен с момента подписания), электронная подпись документа считается недействительной. Подпись считается недействительной также в том случае, если сертификат отправителя просрочен, отозван, искажен или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

12 Расшифрованный документ доступен получателю.

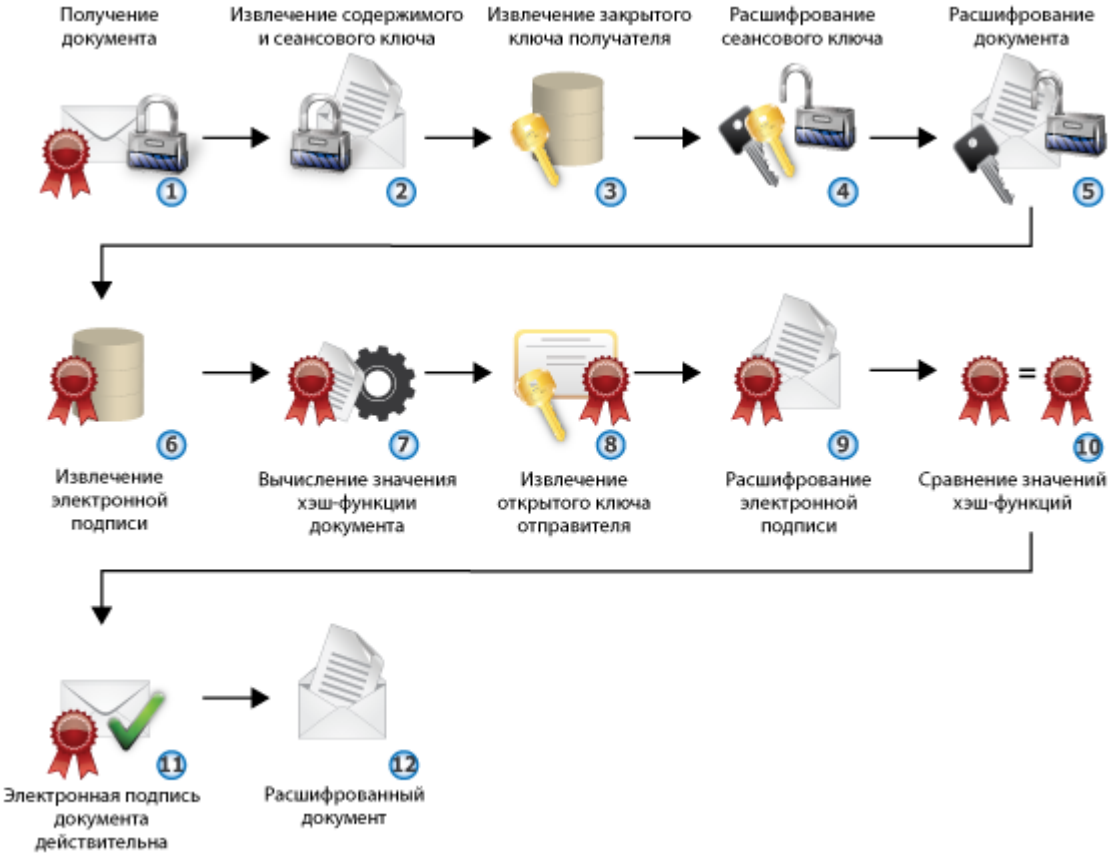


Рисунок 186: Процесс расшифрования и проверки электронного документа

Ключевая система ViPNet

В технологии ViPNet для шифрования применяется комбинация криптографических алгоритмов с симметричными и асимметричными ключами.

Таблица 13. Применение криптографических алгоритмов в ПО ViPNet

Криптографические алгоритмы	
С симметричными ключами	**С асимметричными ключами**
• шифрование IP-трафика • шифрование сообщений программы ViPNet Деловая почта • шифрование прикладных и служебных конвертов	• создание и проверка электронной подписи • шифрование в сторонних приложениях с помощью криптопровайдера ViPNet

Симметричные ключи в ПО ViPNet

Симметричные алгоритмы используются для шифрования информации и контроля ее целостности. Для каждой пары сетевых узлов ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager создается симметричный ключ обмена, предназначенный для шифрования обмена данными между этими сетевыми узлами. Таким образом, формируется матрица симметричных ключей, содержащая данные обо всех созданных для сетевых узлов симметричных ключах обмена. Эта матрица зашифрована, поэтому доступ к ней имеет только программа ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Симметричные ключи обмена следует передавать по защищенным каналам (дистрибутивы для первой установки справочников и ключей передаются лично). Если злоумышленники завладеют симметричными ключами, вся система защиты сетевого узла будет скомпрометирована.

Симметричные ключи обмена используются для шифрования IP-трафика, почтовых сообщений, прикладных и транспортных конвертов.

Рисунок 187: Применение ключей обмена

Для защиты ключей обмена применяется три уровня шифрования:

- ключи обмена зашифрованы на ключах защиты;
- ключи защиты зашифрованы на персональных ключах;
- в свою очередь, персональные ключи зашифрованы на парольных ключах.

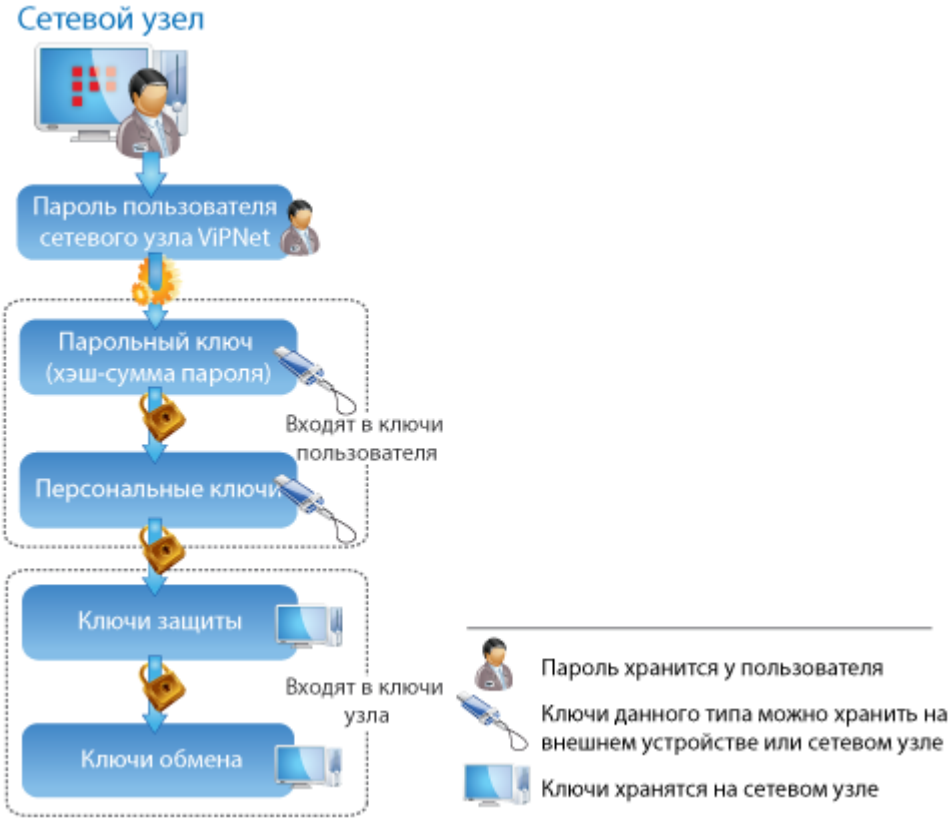


Рисунок 188: Иерархия защиты ключей обмена на сетевом узле

При создании структуры сети ViPNet администратор создает в программе ViPNet Administrator или ViPNet Network Manager файл дистрибутива ключей (`*.dst`) для каждого пользователя сетевого узла ViPNet. Файлы дистрибутивов необходимы для установки справочников и ключей на сетевых узлах. Они содержат ключи пользователя (персональный ключ и ключи электронной подписи), набор ключей обмена с другими сетевыми узлами, адресные справочники, необходимые для связи с другими сетевыми узлами, и регистрационный файл `infotecs.re`. Обновление ключей для сетевых узлов производится по инициативе администратора сети ViPNet.

Примечание. По собственной инициативе пользователь может сделать запрос на обновление сертификата электронной подписи. Для этого в окне **Настройка параметров безопасности** на вкладке **Подпись** нужно нажать кнопку **Обновить сертификат**.

В ПО ViPNet для шифрования используются следующие симметричные алгоритмы:

- ГОСТ 28147-89 (длина ключа 256 бит) — российский стандарт симметричного шифрования.
- AES (256 бит) — принятый в США стандарт симметричного шифрования на основе алгоритма Rijndael.

По умолчанию используется алгоритм ГОСТ 28147-89. При необходимости можно выбрать алгоритм AES. В сертифицированных версиях ПО ViPNet алгоритм шифрования AES не поддерживается, возможность его выбора отсутствует.

Асимметричные ключи в ПО ViPNet

При использовании симметричного алгоритма зашифрование и расшифрование выполняются с помощью одного и того же ключа. При использовании асимметричного алгоритма ключ, с помощью которого шифруется сообщение, является открытым (известен всем отправителям), а ключ, с помощью которого это сообщение расшифровывается, является закрытым (известен только получателю зашифрованного сообщения).

Каждый пользователь имеет пару ключей шифрования — открытый ключ и закрытый ключ. Закрытый ключ необходимо держать в тайне, а открытый ключ можно свободно распространять. Между этими ключами существует математическая связь, однако на практике невозможно за конечное время получить закрытый ключ из открытого.

Асимметричные ключи используются в технологии ViPNet для издания сертификатов и создания электронных подписей (см. «Сочетание хэш-функции и асимметричного

алгоритма электронной подписи» на стр. 395). Если на компьютере установлено ПО ViPNet, в состав которого входит криптопровайдер, асимметричные ключи можно использовать для шифрования (см. «Асимметричное шифрование» на стр. 392). Одна и та же пара асимметричных ключей может использоваться как для шифрования, так и для подписи. Однако, в отличие от шифрования, для подписи используется закрытый ключ, а для проверки подписи — открытый ключ (сертификат ключа подписи). Сертификат содержит открытый ключ, удостоверенный (в том числе подписанный) уполномоченным лицом (администратором УКЦ), информацию о владельце сертификата, сроке его действия и прочее.

Пару асимметричных ключей можно независимо создать на сетевом узле ViPNet. Для этого в окне **Настройка параметров безопасности** на вкладке **Подпись** нужно сделать запрос на обновление сертификата, выбрав в качестве назначения ключа **Подпись и шифрование**.

Примечание. Обновление сертификата требуется в том случае, если истекает срок действия текущего сертификата или закрытого ключа, а также если текущий сертификат не предназначен для шифрования.

Закрытый ключ хранится в зашифрованном виде в файле, который называется контейнером ключей. Его следует хранить в тайне от других пользователей: рекомендуется использовать съемные носители или внешние устройства (на стр. 438). Схема защиты закрытого ключа электронной подписи в зависимости от места его хранения изображена на следующем рисунке.

Рисунок 189: Схема защиты закрытого ключа подписи

Если закрытый ключ подписи хранится на внешнем устройстве, ключом защиты (см. «Ключ защиты» на стр. 485) для него является парольный ключ. Если закрытый ключ подписи хранится на жестком диске или в дистрибутиве ключей, ключом защиты для него является персональный ключ.

Открытые ключи в сетях ViPNet передаются в составе подписанного сообщения программы ViPNet Деловая почта. Также открытые ключи могут храниться в составе

сертификатов в общем хранилище сертификатов, например в службе каталогов Active Directory.

Асимметричное шифрование подразумевает отправку зашифрованного сообщения владельцу выбранного при зашифровании сертификата. Зашифрование сообщений можно выполнять в таких приложениях, как Microsoft Outlook, Outlook Express и так далее. Для этого сертификат получателя должен содержать в соответствующем поле адрес электронной почты.

Примечание. При издании сертификата в программе ViPNet Network Manager адрес электронной почты указать невозможно.

Следует понимать, что технология асимметричного шифрования основана на стандартном использовании интерфейса Microsoft CryptoAPI. Следовательно, при использовании данной технологии пользователи ViPNet могут быть не связаны между собой в смысле топологии сети ViPNet (их сети могут не являться доверенными). Для расшифрования сообщения получателю достаточно закрытого ключа, сертификата и установленного на компьютере программного обеспечения, в состав которого входит криптопровайдер ViPNet.

C

События, отслеживаемые ПО ViPNet

Все события разделены на группы и подгруппы. Иерархическая схема этих групп изображена на следующем рисунке:

Рисунок 190: Классификация событий в журнале IP-пакетов

Блокированные IP-пакеты

*Таблица 14. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные фильтрами защищенной сети***

№ события	Название события	Описание события
1	**Не найден ключ для сетевого узла**	Не найден ключ для связи с пользователем, идентификатор которого указан в пакете
2	**Неверное значение имито**	Защищаемые данные или открытая информация криптосистемы были изменены
3	**IP-пакет блокирован фильтром защищенной сети**	Согласно настройкам фильтров входящий зашифрованный пакет или исходящий предназначенный для шифрования открытый пакет был заблокирован
4	**Слишком большая разница во времени**	Время отправки пакета отличается от времени приема на величину большую, чем указано в настройке допустимого времени отправки принятых пакетов
7	**Неизвестный метод шифрования**	Не поддерживается метод шифрования, код которого указан во входящем пакете
8	**Искаженный IPLIR заголовок**	Недопустимые параметры в расшифрованном пакете
9	**Неизвестный идентификатор сетевого узла**	Идентификатор отправителя в пакете неизвестен
13	**Превышено время жизни IP-пакета**	Пакет уничтожен из-за превышения лимита его нахождения в сети
14	**Получен IP-пакет для другого сетевого узла**	Принят пакет для другого адресата
15	**Слишком много фрагментов для IP-пакета**	Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов
16	**Исчерпана лицензия на количество туннелируемых адресов**	Это событие регистрируется только на координаторе, осуществляющем туннелирование. На координатор одновременно поступили пакеты от большего количества узлов, чем разрешено лицензией

17	**Неверный IP-адрес**	Поступил пакет с некорректным или неизвестным IP-адресом. Чаще всего событие возникает на координаторе в следующем случае: на координатор поступил зашифрованный пакет, предназначенный для туннелируемого узла данного координатора, но IP-адрес этого узла отсутствует в списке туннелируемых адресов координатора
18	**Неизвестный IP-адрес получателя**	В пакете отсутствует или указан неизвестный IP-адрес получателя
19	**Попытка отправителя послать сообщение от имени чужого узла**	Поступил пакет от узла, который не является его отправителем
70	**Пакет заблокирован транзитным фильтром для защищенного узла**	Это событие регистрируется только на координаторе с операционной системой Linux. Пакет заблокирован фильтрами для транзитного зашифрованного трафика

*Таблица 15. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные фильтрами открытой сети***

№ события	Название события	Описание события
22	**Незашифрованный IP-пакет от сетевого узла**	От защищённого адресата пришел открытый пакет
23	**Незашифрованный широковещательный IP-пакет от сетевого узла**	От защищённого адресата пришел открытый широковещательный пакет
24	**Открытый IP-пакет для служб ViPNet**	Служебный трафик ViPNet поступил в открытом виде
30	**Локальный IP-пакет блокирован фильтром открытой сети**	Пакет блокируется локальным фильтром открытой сети или для пакета не удалось найти подходящий фильтр
31	**Транзитный IP-пакет блокирован фильтром открытой сети**	Это событие регистрируется только на координаторе. Пакет блокируется транзитным фильтром открытой сети или для пакета не удалось найти подходящий фильтр
32	**Широковещательный IP-пакет блокирован фильтром открытой сети**	Пакет блокируется фильтром открытого широковещательного трафика или для пакета не удалось найти подходящий фильтр
33	**IP-пакет блокирован фильтром антиспуфинга**	Это событие регистрируется только на координаторе. Найден соответствующий фильтр в таблице антиспуфинга

37	**Пакет блокирован фильтром для туннелируемых узлов**	Это событие регистрируется только на координаторе. Пакет блокируется фильтром трафика туннелируемых узлов или для пакета не удалось найти подходящий фильтр
39	**IP-пакет блокирован фильтрами по умолчанию при загрузке компьютера**	Пакет заблокирован фильтрами по умолчанию при загрузке компьютера

*Таблица 16. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные по другим причинам***

№ события	Название события	Описание события
80	**Размер IP-пакета меньше допустимого**	Размер IP-пакета меньше минимально возможного
81	**Недопустимая версия протокола IP**	В данной версии поддерживается только протокол IP версии 4
82	**Недопустимая длина заголовка IP**	Длина заголовка протокола IP меньше минимально возможного
83	**Недопустимая длина IP-пакета**	Длина пакета меньше, чем указано в заголовке протокола IP
84	**Несовпадение контрольной суммы IP**	Подсчитанное значение контрольной суммы IP-пакета не совпадает со значением, указанным в пакете
85	**Размер заголовка TCP меньше минимально допустимого**	Недопустимо короткий заголовок протокола TCP
86	**Размер заголовка UDP меньше минимально допустимого**	Недопустимо короткий заголовок протокола UDP
87	**Процедура дефрагментации завершилась с ошибкой**	Ошибка при попытке дефрагментации входящего IP-пакета.
88	**Широковещательный адрес отправителя IP-пакета**	Адрес отправителя в пакете указан широковещательный
89	**Процедура дефрагментации завершилась с ошибкой**	Ошибка при попытке дефрагментации входящего IP-пакета.

90	**Недостаточно ресурсов для криптообработки**	Невозможно создать ключ для зашифрования или расшифрования пакета из-за недостаточности свободных ресурсов криптодрайвера. Если эта ошибка стабильно проявляется, обратитесь в службу поддержки компании «ИнфоТеКС». Возможно, потребуется обновление версии драйвера, использующего больше машинных ресурсов, или более совершенная модель компьютера.
91	**IP-пакет получен во время инициализации драйвера**	Блокировка всех пакетов во время инициализации драйвера
92	**Слишком большой размер IP-пакета**	Размер пакета ограничен параметром 48 Кбайт
93	**Превышено время сборки фрагментов IP-пакета**	За допустимое время получены не все фрагменты фрагментированного пакета
95	**Обнаружен сетевой узел с таким же идентификатором**	В сети появился узел с таким же идентификатором, но другим IP-адресом
97	**IP-пакет блокирован фильтром SQL**	Соединение заблокировано фильтром Microsoft SQL
101	**Не найден маршрут для транзитного IP-пакета**	Это событие регистрируется только на координаторе. Не найдено правило для транзитного пакета в таблице маршрутов
103	**Превышено максимальное количество соединений**	Количество уже установленных соединений превышает максимально допустимое ПО ViPNet (не лицензией)
104	**Соединение уже существует**	Если параметры исходящих пакетов для создаваемого соединения совпадают с уже существующими, то такое соединение блокируется
105	**Не удалось выделить динамический порт для правила трансляции адресов**	Это событие регистрируется только на координаторе. Координатор не смог выделить порт для динамического правила трансляции адресов (например, все порты в пуле закончились)
111	**Не найден ключ обмена**	Не найден ключ для связи с сетевым узлом получателя
112	**Нарушена имитовставка открытой части зашифрованного пакета 4.2**	Неверное значение имито для транзитного зашифрованного трафика
113	**Неизвестный ID источника**	Неизвестный идентификатор сетевого узла–источника транзитного зашифрованного пакета

115	**Не удалось найти маршрут для IP-пакета**	По каким-либо причинам не найден маршрут в таблице маршрутизации
116	**Сетевой адаптер не найден**	IP-пакет не может быть отправлен, так как не найден сетевой интерфейс
117	**Не удалось разрешить MAC-адрес по IP-адресу**	Не удалось определить MAC-адрес получателя пакета по его IP-адресу
118	**Не удалось произвести шифрование IP-пакета**	Ошибка при шифровании исходящего IP-пакета для защищенного узла
119	**Неизвестный формат IPLIR заголовка**	Получен зашифрованный IP-пакет неизвестного формата
120	**Несогласованная информация о способе доступа до сетевого узла**	Ошибка при отправке IP-пакета для защищенного узла
121	**Ошибка в работе кластера**	Это событие регистрируется только на кластере ViPNet. Внутренняя ошибка кластера
122	**Неизвестный протокол канального уровня**	Получен IP-пакет неизвестного протокола

Примечание. Если вы используете Windows Server 2003 или более позднюю версию Windows, события 82 и 89 не фиксируются в журнале IP-пакетов, так как операционная система автоматически блокирует соответствующие IP-пакеты.

Пропущенные IP-пакеты и служебные события

*Таблица 17. Группа **Все IP-пакеты\Все пропущенные IP-пакеты\Пропущенные зашифрованные IP-пакеты***

№ события	Название события	Описание события
40	**Пропущен зашифрованный IP-пакет**	Пропущен зашифрованный пакет
41	**Пропущен пакет, зашифрованный на широковещательном ключе**	Пропущен IP-пакет, зашифрованный на ключе для широковещательных пакетов
44	**Осуществлена маршрутизация зашифрованного транзитного IP-пакета с изменением его адреса**	Это событие регистрируется только на координаторе. Пакет направлен на другой узел путём подмены в нём адреса получателя
45	**Зашифрован (расшифрован) пакет туннелируемого узла**	Это событие регистрируется только на координаторе. Зашифрован или расшифрован пакет для туннелируемого узла

*Таблица 18. Группа **Все IP-пакеты\Все пропущенные IP-пакеты\Пропущенные незашифрованные IP-пакеты***

№ события	Название события	Описание события
60	**Пропущен незашифрованный локальный IP-пакет**	Найден разрешающий фильтр открытой сети для локальных IP-пакетов
61	**Пропущен незашифрованный широковещательный IP-пакет**	Найден разрешающий фильтр открытой сети для широковещательных IP-пакетов
62	**Пропущен незашифрованный транзитный IP-пакет**	Это событие регистрируется только на координаторе. Найден разрешающий фильтр открытой сети для транзитных IP-пакетов

63	**Пакет пропущен фильтром для туннелируемых узлов**	Это событие регистрируется только на координаторе. Найден разрешающий фильтр для IP-пакетов от туннелируемых узлов
64	**IP-пакет пропущен фильтрами по умолчанию при загрузке компьютера**	Пакет пропущен фильтрами, которые действуют при загрузке компьютера

*Таблица 19. Группа **Все IP-пакеты\Служебные события** (дополнительная информация, формируемая для IP-пакетов, уже зарегистрированных в журнале)*

№ события	Название события	Описание события
42	**Изменился IP-адрес узла**	Драйвер обнаружил, что IP-адрес узла или параметры доступа к нему через внешнюю сеть изменились, и соответствующим образом скорректировал свои таблицы. При изменении параметров доступа событие регистрируется только для сетевых узлов, не работающих через межсетевой экран с динамической или статической трансляцией адресов.
46	**Изменились параметры доступа к сетевому узлу**	Драйвер обнаружил, что параметры доступа к сетевому узлу через внешнюю сеть изменились, и соответствующим образом скорректировал свои таблицы. Событие регистрируется для сетевых узлов, работающих через межсетевой экран с динамической или статической трансляцией адресов. В качестве IP-адресов и портов регистрируются данные из IP-пакета, поступившего из сети, до его преобразования драйвером.
48	**Адрес сетевого узла зарегистрирован из широковещательного пакета**	Зарегистрировано событие, что от узла поступают широковещательные пакеты
49	**Изменились параметры доступа к своему узлу из внешней сети**	Поступила информация об изменении параметров доступа через внешнюю сеть к своему сетевому узлу. В качестве IP-адресов и портов регистрируются данные по доступу к своему узлу (**Получатель**) и к узлу, от которого получена информация (**Отправитель**)
110	**На DNS-сервере зарегистрирован новый IP-адрес узла**	Поступило сообщение от DNS-сервера, что для узла с именем, указанным в поле **Отправитель**, зарегистрирован IP-адрес, указанный в поле **IP-адрес отправителя**
114	**Имя на DNS (WINS)-сервере не зарегистрировано**	Поступило сообщение от DNS-сервера, что запрошенное DNS-имя защищенного узла не зарегистрировано на данном DNS-сервере

Региональные настройки

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

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

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

Региональные настройки в ОС Windows XP, Server 2003

Для установки поддержки кириллицы на ОС Windows XP, Server 2003:

1. Откройте **Панель управления** (**Control Panel**).
2. Щелкните **Язык и региональные стандарты** (**Regional and Language Options**).
3. В окне **Язык и региональные стандарты** (**Regional and Language Options**) перейдите на вкладку **Дополнительно** (**Advanced**).
4. Далее в списке выберите **Русский** (**Russian**).
5. Установите флажок **Применить эти параметры для текущей учетной записи и для стандартного профиля пользователя** (**Apply all settings to the current user account and to the default user profile**).

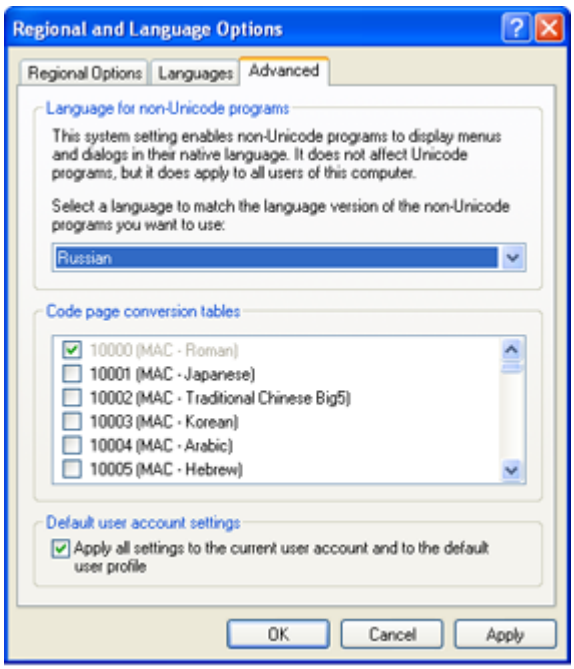


Рисунок 191: Выбор языка для программ, не поддерживающих Юникод, в Windows XP

6. Нажмите кнопку **OK**. Возможно, потребуется перезагрузка.

Региональные настройки в ОС Windows Vista, Server 2008, Windows 7, Server 2008 R2

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

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

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

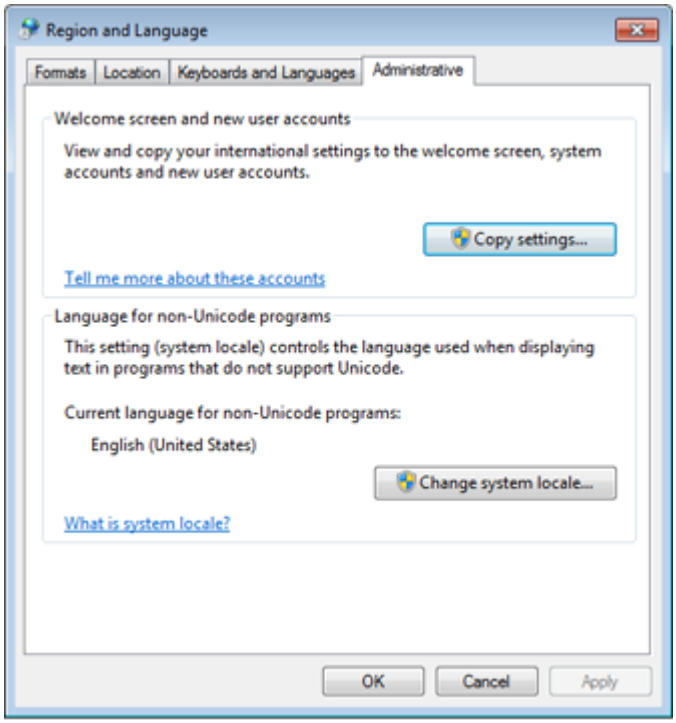


Рисунок 192: Дополнительные языковые параметры

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

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

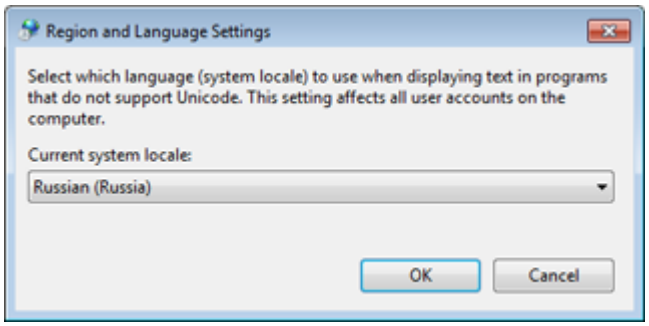


Рисунок 193: Выбор языка системы

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

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

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

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

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

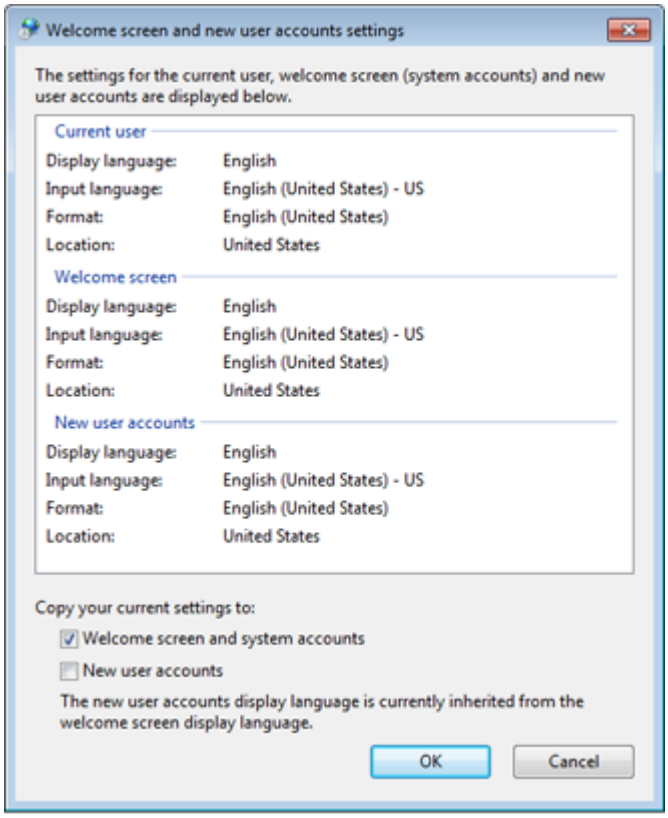


Рисунок 194: Копирование параметров

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

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

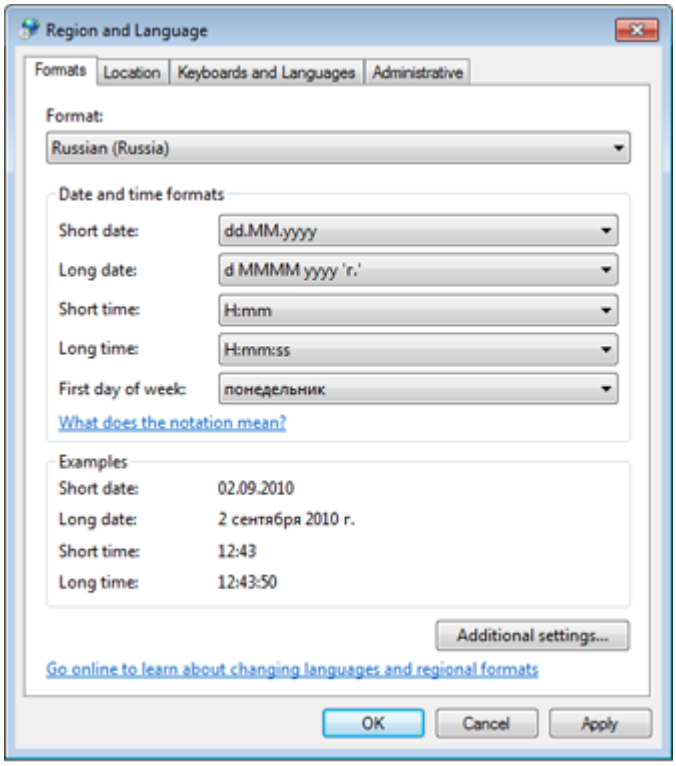


Рисунок 195: Настройка форматов

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

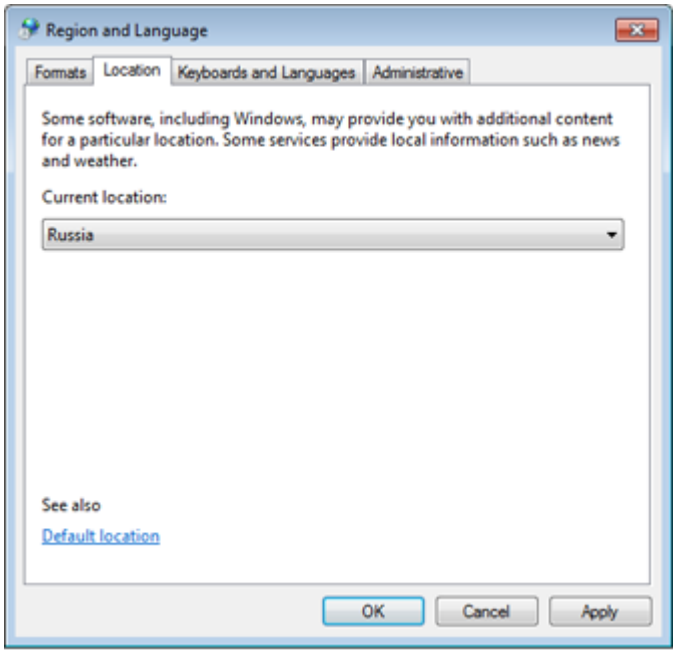


Рисунок 196: Выбор текущего расположения

Региональные настройки в ОС Windows 8, Server 2012

Для установки поддержки кириллицы на ОС Windows 8, Server 2012:

1. Откройте **Панель управления** (**Control Panel**) > **Региональные стандарты** (**Region**).
2. В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

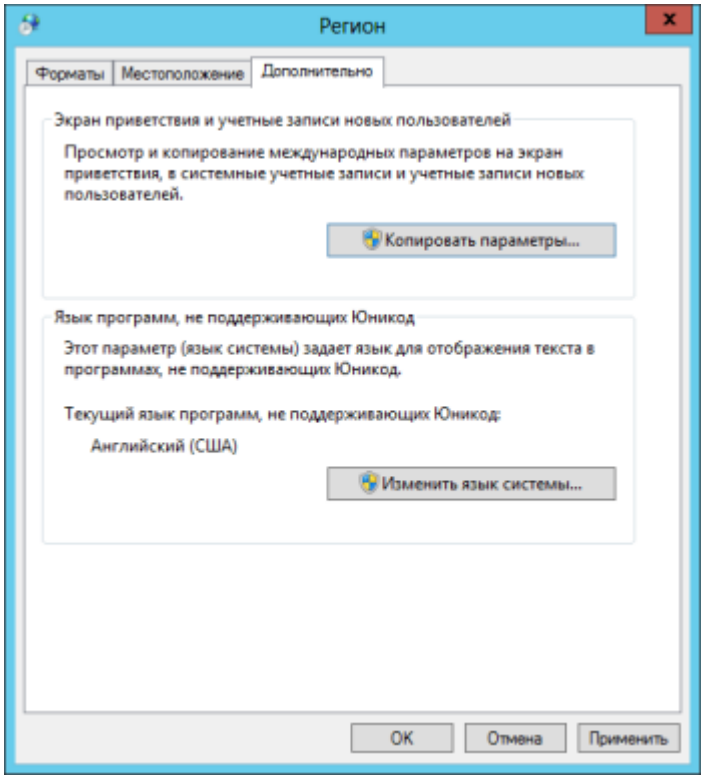


Рисунок 197: Дополнительные языковые параметры

3. На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).
4. В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

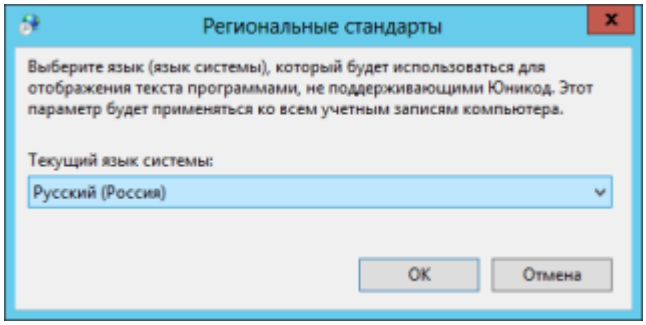


Рисунок 198: Выбор языка системы

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

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

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

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

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

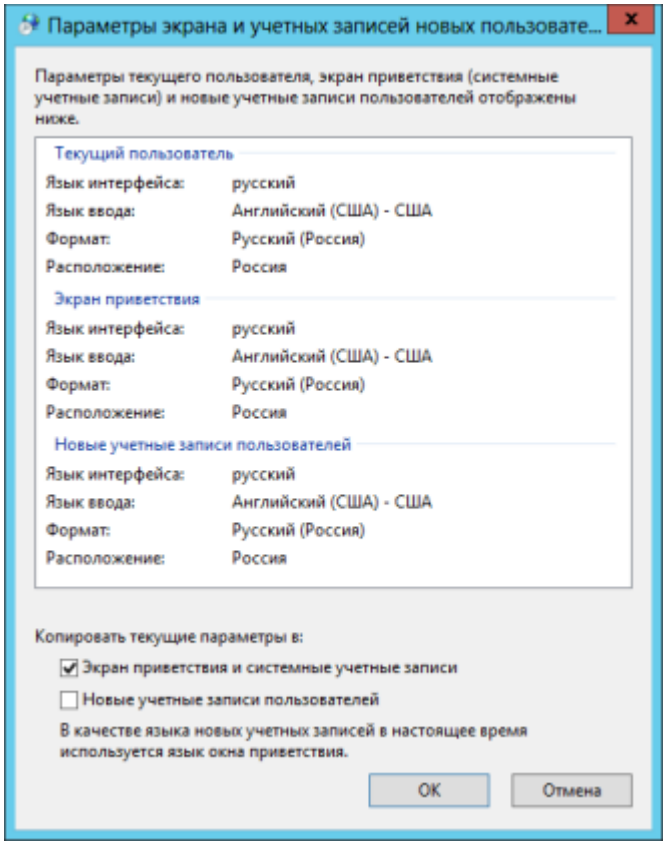


Рисунок 199: Копирование параметров

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

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

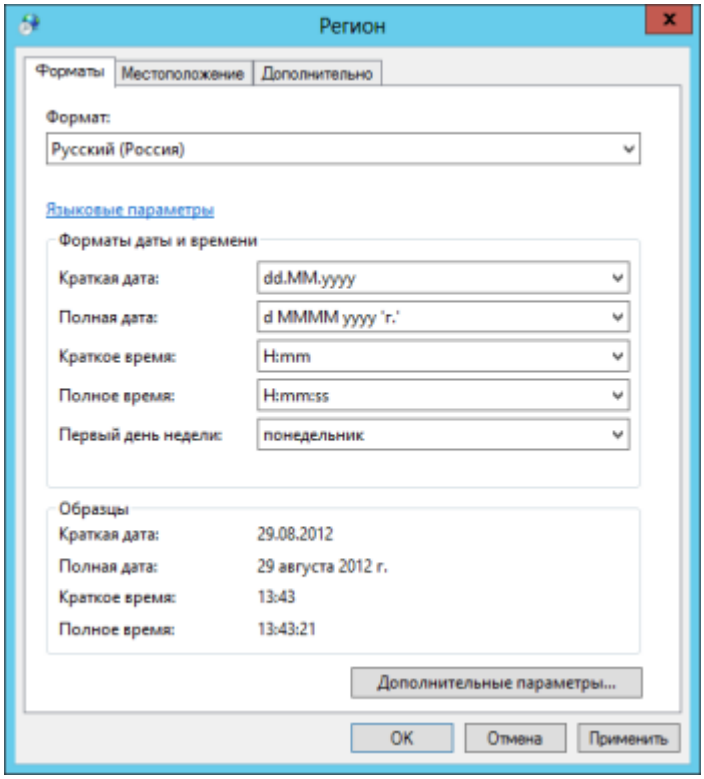


Рисунок 200: Настройка форматов

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

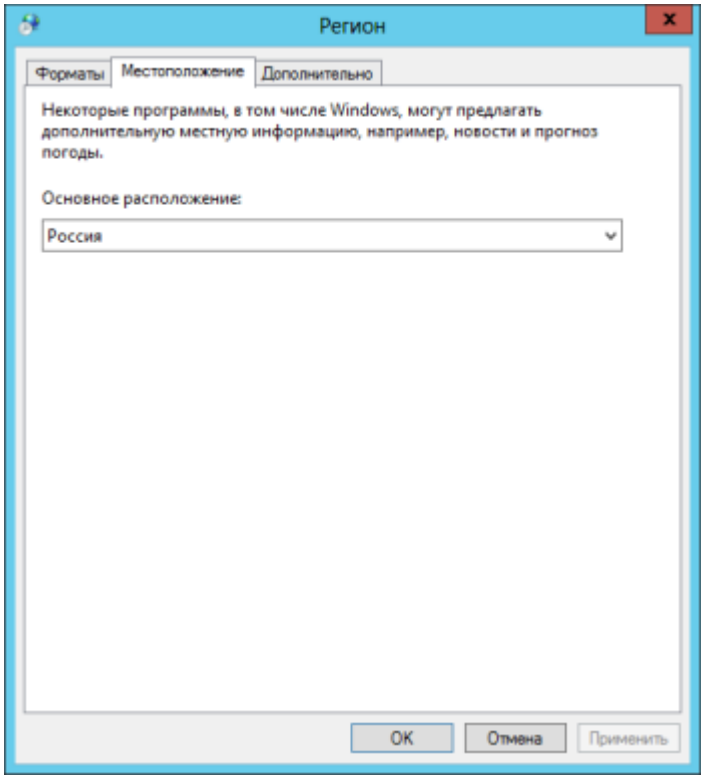


Рисунок 201: Выбор текущего расположения

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей (см. «Контейнер ключей» на стр. 485), которые вы можете использовать для аутентификации, формирования электронной подписи (см. «Электронная подпись» на стр. 494) или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объема памяти устройства.

Программное обеспечение ViPNet Монитор поддерживает два способа аутентификации с помощью внешнего устройства (см. «Способы аутентификации пользователя» на стр. 80):

- По персональному ключу пользователя ViPNet, который хранится на устройстве. Этот способ аутентификации имеет следующие ограничения:
  - Одно внешнее устройство невозможно использовать для аутентификации нескольких пользователей ViPNet.
  - Одно внешнее устройство невозможно использовать для аутентификации одного пользователя на нескольких узлах ViPNet.

- Если используется этот способ аутентификации, тогда ключи электронной подписи пользователя, изданные в удостоверяющем центре на базе ПО ViPNet, должны храниться на одном устройстве с персональным ключом.

- По сертификату, который хранится на устройстве вместе с соответствующим закрытым ключом.

  Сертификат для аутентификации можно запросить в домене Windows, сохранив контейнер ключей на внешнем устройстве, которое поддерживает стандарт PKCS#11.

Примечание. Если требуется выполнять аутентификацию по сертификату, изданному в соответствии с ГОСТ 34.10-2001, следует использовать устройство ruToken ECP.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP (см. «Настройка параметров криптопровайдера ViPNet CSP» на стр. 325). Чтобы использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

В следующей таблице перечислены внешние устройства, которые могут быть использованы в программном обеспечении ViPNet. Для каждого внешнего устройства в таблице приведено описание, условия и особенности работы с устройством, информация о поддержке стандарта PKCS#11.

Примечание. Стандарт PKCS#11 (также известный как Cryptoki) — один из стандартов семейства PKCS (Public Key Cryptography Standards — криптографические стандарты открытого ключа), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 20. Поддерживаемые внешние устройства

Название устройства в программе ViPNet CSP	Полное название и тип устройства	Необходимые условия работы с устройством	Поддержка стандарта PKCS#11
UEC	**Универсальная электронная карта**	На компьютере необходимо указать расположение сертификатов и контейнера ключей, полученных в пункте выдачи карт.	Да
ESMART CryptoToken 64K	Смарт-карты **ESMART CryptoToken 64K**	На компьютере должно быть установлено программное обеспечение ESMART PKI Client.	Да
Infotecs Software Token	**Infotecs Software Token** — программная реализация стандарта PKCS#11	Входит в поставку программы ViPNet CSP.	Да
A-Key S1000	Смарт-карта **AkToken** производства компании Ak Kamal Security	На компьютере должны быть установлены драйверы, предоставленные компанией Ak Kamal Security. Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — `12345678`. Перенос ключей подписи на данный тип устройств невозможен.	Да
Magistra	Смарт-карты **Магистра** производства компании «СмартПарк»	Устройство не поддерживает ГОСТ 34.10-2012; создание ключей по этому алгоритму невозможно, перенос ключей, созданных по этому алгоритму, на данный тип устройств невозможен.	Да
ViPNet HSM	Виртуальный токен **ViPNet HSM** производства компании «ИнфоТеКС»	Необходимо установить клиентское приложение ViPNet HSM и проинициализировать виртуальный токен.	Да

KAZTOKEN	**KAZTOKEN**, электронный идентификатор производства компании «Цифровой поток»	На компьютере должны быть установлены драйверы ktDrivers.x64.v.2.73.00.04.08 (для 64-разрядной ОС) или ktDrivers.x86.v.2.73.00.04.08. Перенос ключей подписи на данный тип устройств невозможен.	Да
JaCarta	Персональные электронные ключи **JaCarta Laser** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено программное обеспечение JC-Client компании «Аладдин Р.Д.».	Да
JCDS	Смарт-карты **Gemalto Optelio Contactless D72**, **KONA 131 72K** с апплетом от компании «Аладдин Р.Д.»	На карту должен быть загружен апплет, позволяющий модулю jcpkcs11ds.dll компании «Аладдин Р.Д.» работать с картой.	Да
Mifare Standard4K	Смарт-карты **MIFARE Classic 4K** для считывателей ACR128	Для работы с устройством используется интерфейс подключения USB 2.0 (совместимый с USB 1.1). Карта MIFARE Classic 4K поддерживается только через считыватель ACR128.	Нет
SmartCard RIK	**Российская интеллектуальная карта (РИК)** производства компании «Атлас-Телеком»	Работа с картой ПО ViPNet может производиться через любой PC/SC-совместимый считыватель.	Нет
Rosan Mifare	Смарт-карты **MIFARE** для считывателей компании «Розан»	Необходимо наличие COM-порта и считывателя от компании «Розан».	Нет

Siemens CardOS	Смарт-карты **CardOS/M4.01a**, **CardOS V4.3B**, **CardOS V4.2B**, **CardOS V4.2B DI**, **CardOS V4.2C**, **CardOS V4.4** производства компании Atos (Siemens)	На компьютере должно быть установлено ПО Siemens CardOS API V5.0 или более поздних версий.	Да
eToken GOST	Персональные электронные ключи **eToken ГОСТ** и **JaCarta ГОСТ** производства компании «Аладдин Р.Д.»	Создание ключей подписи возможно только по ГОСТ 34.10-2001, ГОСТ 34.10-2012 не поддерживается; перенос ключей подписи на данный тип устройств невозможен.	Да
Rutoken ECP/Rutoken Lite	**Рутокен ЭЦП**, **Рутокен Lite** — электронные идентификаторы производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken версии 2.89.00.0491. В программе ViPNet CSP настоятельно рекомендуется отключить поддержку устройств Рутокен. Создание ключей подписи возможно только по ГОСТ 34.10-2001, ГОСТ 34.10-2012 не поддерживается; перенос ключей подписи на данный тип устройств невозможен.	Да
Rutoken/ Rutoken S	**Рутокен**, **Рутокен S** — электронные идентификаторы производства компании «Актив»	На компьютере должны быть установлены драйверы Rutoken версии 2.89.00.0491. Постоянная корректная работа ПО ViPNet при использовании устройств Рутокен с драйверами указанной версии не гарантирована. Для гарантированной корректной работы ПО ViPNet рекомендуется использовать устройства другого типа.	Да
Shipka	ПСКЗИ **ШИПКА** (любой версии) производства компании «ОКБ САПР»	На компьютере должно быть установлено программное обеспечение ACShipka Environment версии не ниже 3.3.2.7. Проведите инициализацию устройства с помощью утилиты производителя «Параметры авторизации».	Да

eToken Aladdin	Персональные электронные ключи **eToken PRO (Java)**, **eToken PRO**, смарт-карты **eToken PRO (Java)**, **eToken PRO** производства компании «Аладдин Р.Д.»	На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше. Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт.	Да
Smartcard Athena	Смарт-карты с памятью типа I2C (ASE M4), синхронные смарт-карты с шиной 2/3 и защищенной памятью, удовлетворяющие стандарту ISO7816-3 (ASE MP42)	Чтение и запись на смарт-карту осуществляется через считыватель ASEDrive III PRO-S компании Athena. На компьютере должны быть установлены драйверы версии 2.5.0.0.	Нет
iButton Accord	Электронные ключи **iButton** типа **DS1993**, **DS1994**, **DS1995** и **DS1996** для использования с платой Аккорд-5MX производства компании «ОКБ САПР»	Необходимо использование платы Аккорд-5MX На компьютере должен быть установлен драйвер версии не ниже 3.18.0.0.	Нет
iButton Aladdin	Электронные ключи **Dallas, iButton** типа **DS1993**, **DS1994**, **DS1995** и **DS1996**	К компьютеру должно быть подключено устройство считывания. На компьютере должно быть установлено программное обеспечение для обмена информации с iButton — 1-Wire Drivers версии 3.20 либо версии 4.0.3. На ОС Windows XP и Server 2003 совместно с ПО ViPNet может использоваться только ПО 1-Wire Drivers версии 3.20.	Нет

Примечание. Список поддерживаемых операционных систем для каждого из приведенных устройств вы найдете на официальном веб-сайте производителя этого устройства.

Рекомендации по обеспечению совместной работы ПО ViPNet Coordinator с другими приложениями

Совместное использование программы ViPNet Монитор и технологии Hyper-V

Hyper-V — это система виртуализации, реализованная в 64-разрядной версии операционной системы Microsoft Windows Server 2008.

Особенностью Hyper-V является то, что для обеспечения доступа виртуальных машин к внешней сети требуется выделить один из физических сетевых интерфейсов компьютера. Этот интерфейс будет подключен к виртуальному коммутатору Hyper-V, а вместо него в хостовой операционной системе будет создан виртуальный интерфейс с такими же настройками.

Для правильного подключения виртуальных сетевых интерфейсов (в том числе в хостовой операционной системе) к внешней сети на физическом интерфейсе, который используется для этого подключения, должны быть отключены все службы и протоколы, кроме протокола коммутации виртуальных сетей (Virtual Network Switching Protocol).

При установке программы ViPNet Монитор на компьютер с 64-разрядной операционной системой на всех сетевых интерфейсах компьютера включается служба Iplir lightweight Filter (x64 edition), то есть сетевой ViPNet-драйвер (на стр. 17). Этот драйвер осуществляет шифрование, расшифрование и фильтрацию IP-пакетов, проходящих через сетевой интерфейс, и может нарушить работоспособность виртуальной сети Hyper-V.

Чтобы обеспечить нормальное функционирование виртуальной сети и программного обеспечения ViPNet в хостовой операционной системе, в настройках физического сетевого интерфейса, подключенного к виртуальной сети Hyper-V, требуется отключить службу Iplir lightweight Filter (x64 edition).

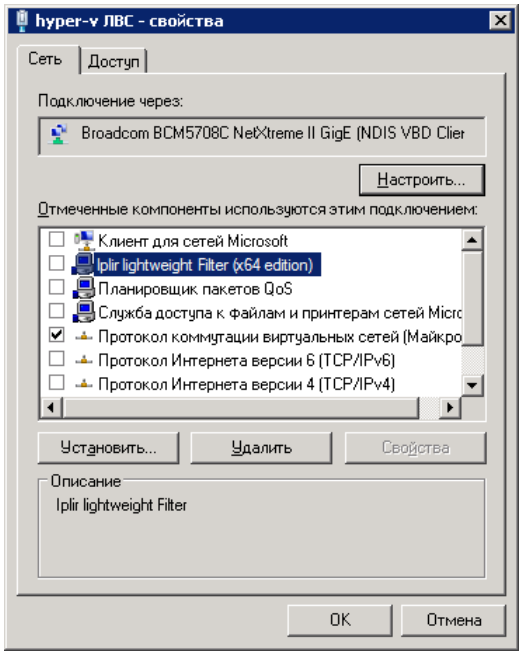


Рисунок 202: Настройки физического интерфейса, подключенного к виртуальной сети Hyper-V

Совместное использование ViPNet Монитор и ПО Dallas Lock

Внимание! Рекомендации, приведенные в данном разделе, относятся к программному обеспечению Dallas Lock версии 7.7. Прежде чем приступать к настройке Dallas Lock 7.7, ознакомьтесь с руководством по эксплуатации программы.

Чтобы обеспечить на компьютере совместную работу программы ViPNet Монитор и системы защиты от несанкционированного доступа Dallas Lock, выполните следующие действия:

1. В программе ViPNet Монитор в разделе **Фильтры защищенной сети** для всех защищенных узлов создайте широковещательный фильтр (см. «Создание фильтров для защищенной сети» на стр. 180), разрешающий входящие и исходящие соединения по следующим портам TCP: 17484, 17485, 17486, 17487.

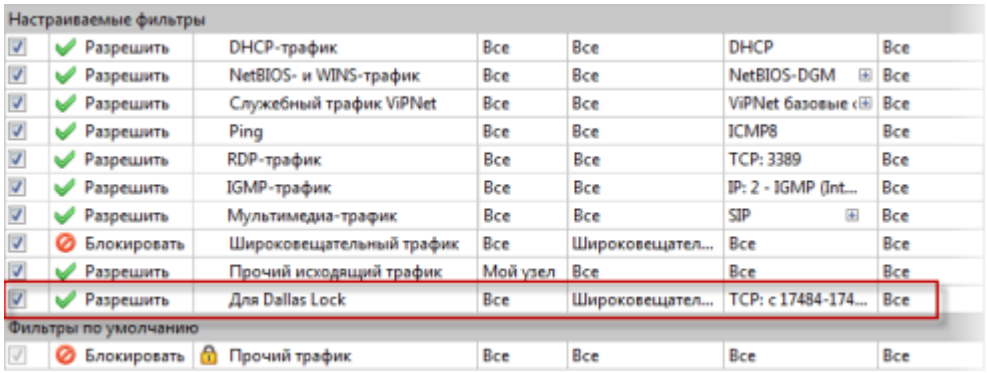


Рисунок 203: Широковещательный фильтр защищенной сети

2. В оболочке администратора Dallas Lock зарегистрируйте пользователя с именем «__ViPNet__User__» и задайте для него следующие параметры:
   - В группе **Пароль** установите флажок **Пароль проверяется только в Windows**.
   - В группе **Учетная запись** установите флажок **Системный пользователь**.

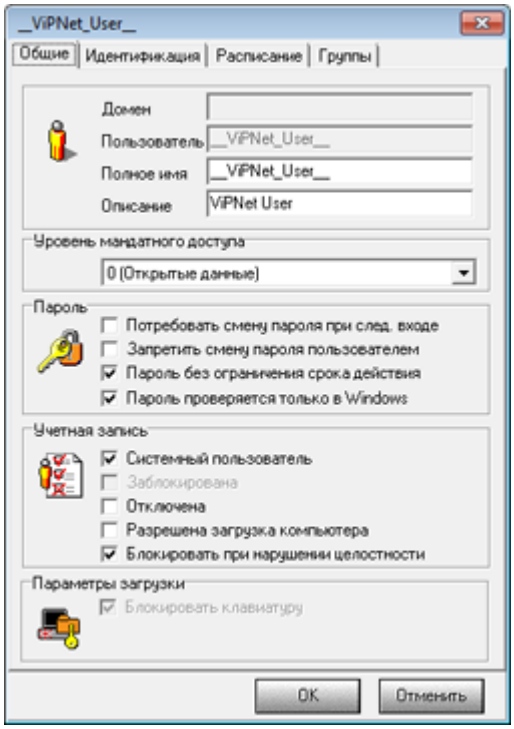


Рисунок 204: Свойства пользователя Dallas Lock

После регистрации пользователя его значок должен смениться на желтый.

3 В оболочке администратора Dallas Lock в разделе **Параметры безопасности > Политика входа в систему** отключить политику **Автоматический вход в ОС**.

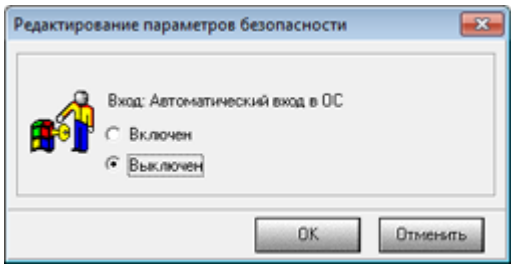


Рисунок 205: Политика «Автоматический вход в систему»

4 Настройте мандатный доступ с мандатом 0 на папку установки программы ViPNet Coordinator. В список **Программы имеющие доступ на запись** добавьте следующие исполняемые файлы:

- Все исполняемые файлы из папки установки программы ViPNet Coordinator.
- `c:\windows\explorer.exe`.
- `c:\windows\system32\dllhost.exe`.
- `c:\windows\system32\svchost.exe`.

- `c:\windows\system32\wbem\wmiprvse.exe`.

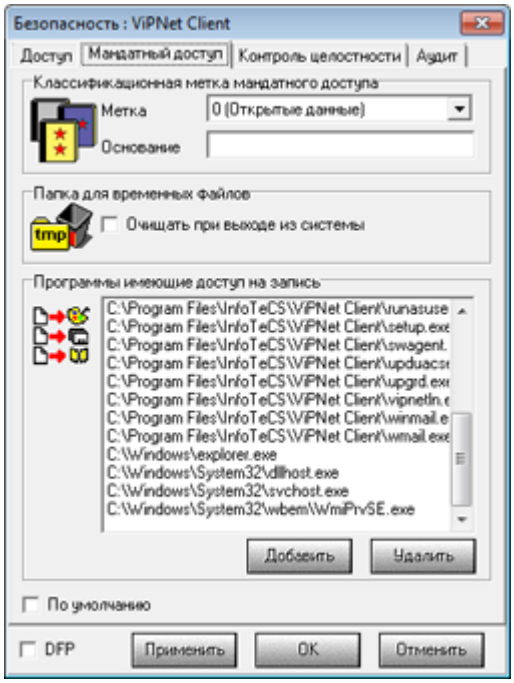


Рисунок 206: Настройка мандатного доступа

5 Настройте мандатный доступ с мандатом 0 на папку пользователя Windows, от имени которого будет запускаться ПО ViPNet:

- При использовании Windows XP `C:\Documents and Settings\<имя пользователя>\`.
- При использовании Windows Vista или Windows 7 `C:\Users\<имя пользователя>\`.

В список **Программы имеющие доступ на запись** добавьте следующие исполняемые файлы:

- `C:\Windows\explorer.exe`.
- `C:\Program Files\InfoTeCS\ViPNet Coordinator\Monitor.exe`.

6 Настройте мандатный доступ с мандатом 0 на папку временных файлов пользователя. По умолчанию:

- При использовании Windows XP `C:\Documents and Settings\<имя пользователя>\Local Settings\Temp\`.
- При использовании Windows Vista или Windows 7 `C:\Users\<имя пользователя>\AppData\Local\Temp\`.

Для этой папки установить флажок **Очищать при выходе из системы**.

7 Настройте мандатный доступ с мандатом 0 на папку `C:\ProgramData\Infotecs\`.

В список **Программы имеющие доступ на запись** добавьте следующие исполняемые файлы:

- `C:\Program Files\InfoTeCS\ViPNet Coordinator\Monitor.exe`.
- `C:\Windows\System32\rundll.exe`.

8 После выполнения указанных настроек программы ViPNet Монитор и Dallas Lock готовы к совместной работе.

G

История версий

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

Что нового в версии 4.1

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.1.

- **Отключение сетевого экрана Windows при первом запуске программы**

  При установке программы ViPNet Coordinator версии 4.1 стандартный сетевой экран Windows остается включенным и выключается автоматически только при первом запуске программы. Такая логика позволяет обеспечить непрерывную защиту вашего компьютера при развертывании сети. Сообщение об отключении сетевого экрана не выводится. В версиях 3.2.x сетевой экран выключается при установке программного обеспечения.

- **Новые алгоритмы подписи**

  В программе ViPNet Монитор версии 4.1 реализована поддержка ключей электронной подписи, созданных по алгоритму ГОСТ 34.10.2012.

- **Возможность использования экранной клавиатуры для аутентификации**

  В версии 4.1 во время загрузки Windows для аутентификации в программе ViPNet Монитор вы можете использовать экранную клавиатуру. Для этого нажмите кнопку  и в меню выберите пункт **Экранная клавиатура.**

- **Упрощена настройка подключения координатора к внешней сети через межсетевой экран с трансляцией адресов**

  В программе ViPNet Coordinator Монитор версии 3.2.x при настройке подключения ViPNet-координатора к внешней сети через межсетевой экран со статической или динамической трансляцией адресов требуется указать сетевой интерфейс, через который будет осуществляться подключение (список **Адаптер, со стороны которого установлен межсетевой экран**).

  В программе ViPNet Coordinator Монитор версии 4.1 вам нужно указывать интерфейс, только если вы хотите, чтобы все ответные пакеты от узлов из внешней сети направлялись на определенный адрес межсетевого экрана (флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран**). Для сетевого экрана с динамической трансляцией адресов и для сетевого экрана со статической трансляцией без фиксирования IP-адреса данная настройка больше не требуется.

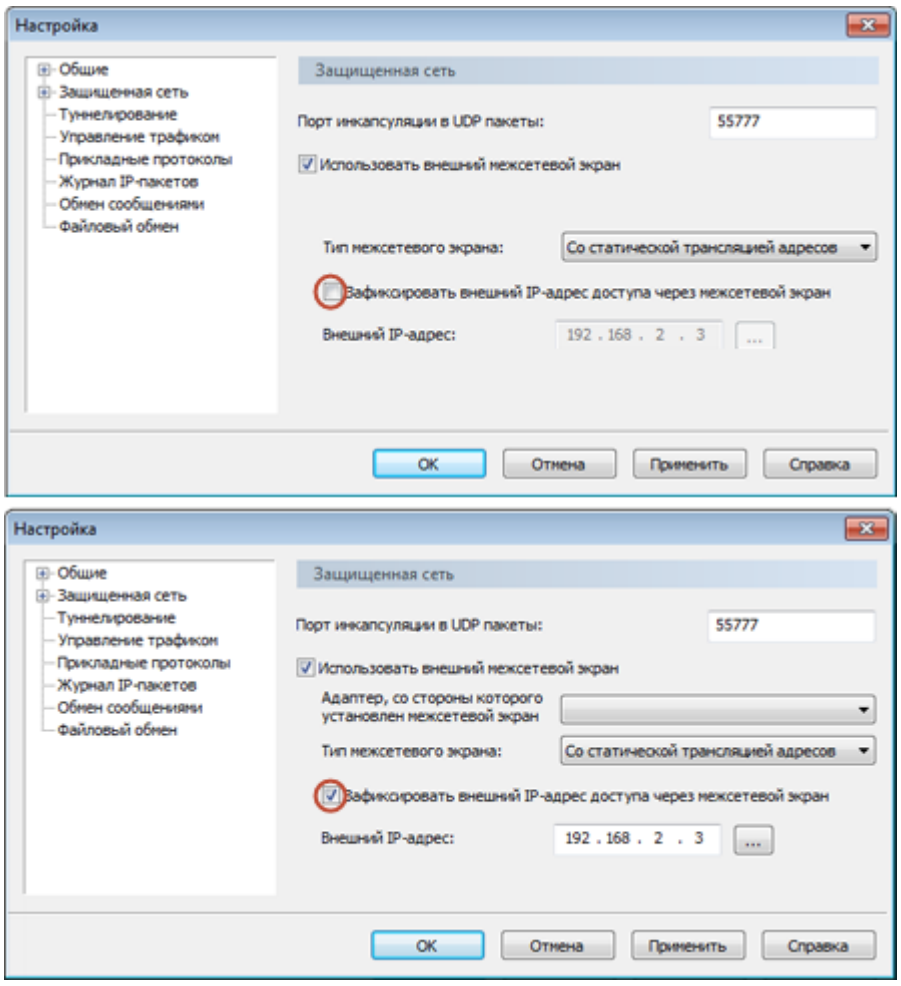


Рисунок 207: Указание интерфейса межсетевого экрана в версии 4.x

Что нового в версии 4.0

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

- **Поддержка централизованного управления политиками безопасности**

  В программе ViPNet Монитор реализована возможность применять сетевые фильтры и правила трансляции IP-адресов, созданные в программе ViPNet Policy Manager.

- **Новый формат сетевых фильтров и правил трансляции IP-адресов**

  В версии 4.0 используется новый формат сетевых фильтров и правил трансляции IP-адресов (см. «Интегрированный сетевой экран» на стр. 155), который позволяет применять политики безопасности, созданные в программе ViPNet Policy Manager. При переходе на новую версию фильтры и правила конвертируются без каких-либо потерь. Таким образом, никаких действий со стороны пользователя не требуется.

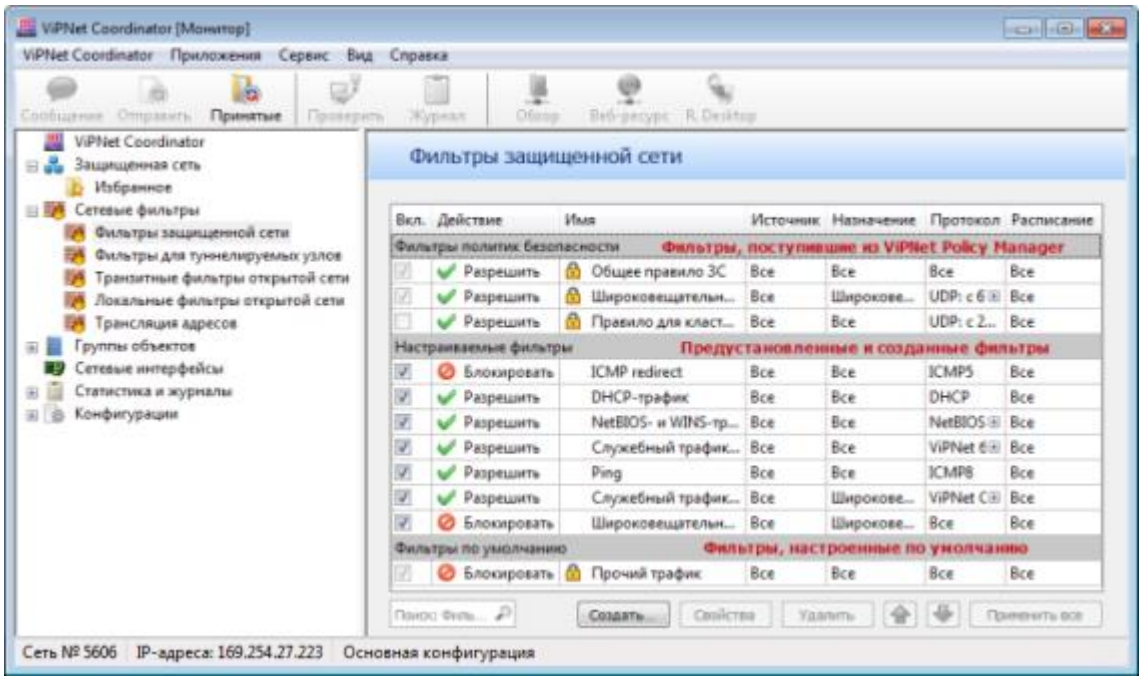


Рисунок 208: Отображение сетевых фильтров в программе ViPNet Монитор

- **Отказ от режимов безопасности**

  В версии 4.0 режимы безопасности не используются. Необходимый уровень безопасности можно настроить, создав сетевые фильтры или назначив соответствующий уровень полномочий пользователя.

- **Использование технологии MSI для установки ПО ViPNet**

Для программы ViPNet Монитор версии 4.0 разработан установочный пакет MSI, который позволяет устанавливать программу с использованием Microsoft System Center, а также с помощью программ, обращающихся к командной строке Windows для запуска автоматической установки ViPNet Монитор (см. «Установка в неинтерактивном режиме» на стр. 45).

- **Установка и настройка ViPNet CSP**

  Программа ViPNet CSP может быть установлена как из отдельного установочного файла, так и вместе с программами ViPNet Client и ViPNet Coordinator версии 4.0. При любом из способов установки ViPNet CSP устанавливается как отдельная программа, что обеспечивает удобство обновления ViPNet CSP независимо от программ ViPNet Client и ViPNet Coordinator.

  Настройка криптопровайдера теперь выполняется только в программе ViPNet CSP. На вкладке **Криптопровайдер** программы ViPNet Монитор можно осуществить только переход к окну настройки.

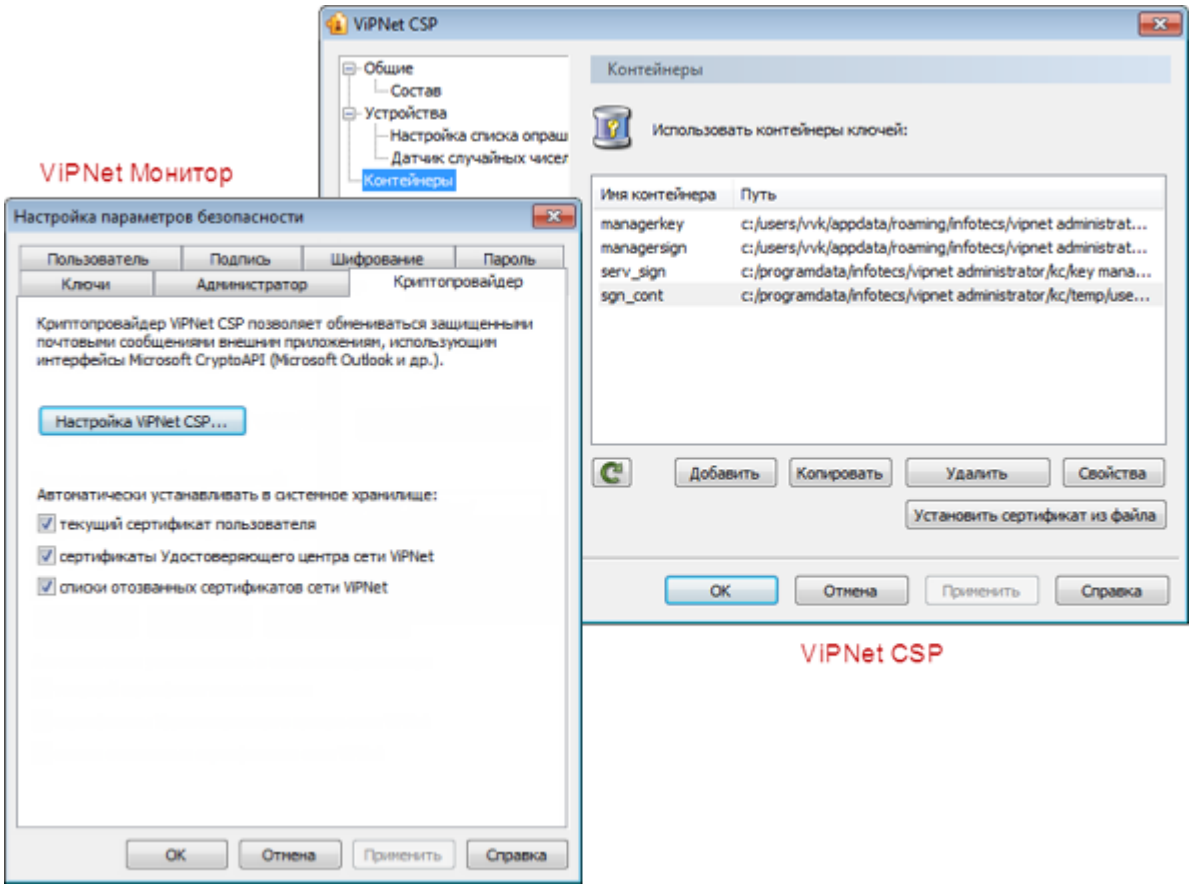


Рисунок 209: Настройка параметров криптопровайдера

- **Мастер установки ключей ViPNet**

В версии 4.0 мастер первичной инициализации больше не используется. Мастер установки ключей ViPNet позволяет выполнять все сценарии, связанные с установкой и обновлением ключей на сетевом узле ViPNet (см. «Установка справочников и ключей» на стр. 59).

- **Способы аутентификации пользователя**

  В программе ViPNet Монитор версии 4.0 при использовании устройства аутентификации (способ **Устройство**) для входа в программу реализована возможность выполнять аутентификацию пользователя не только с помощью персонального ключа (как в версии 3.2.x), но и с помощью сертификата (см. «Способы аутентификации пользователя» на стр. 80).

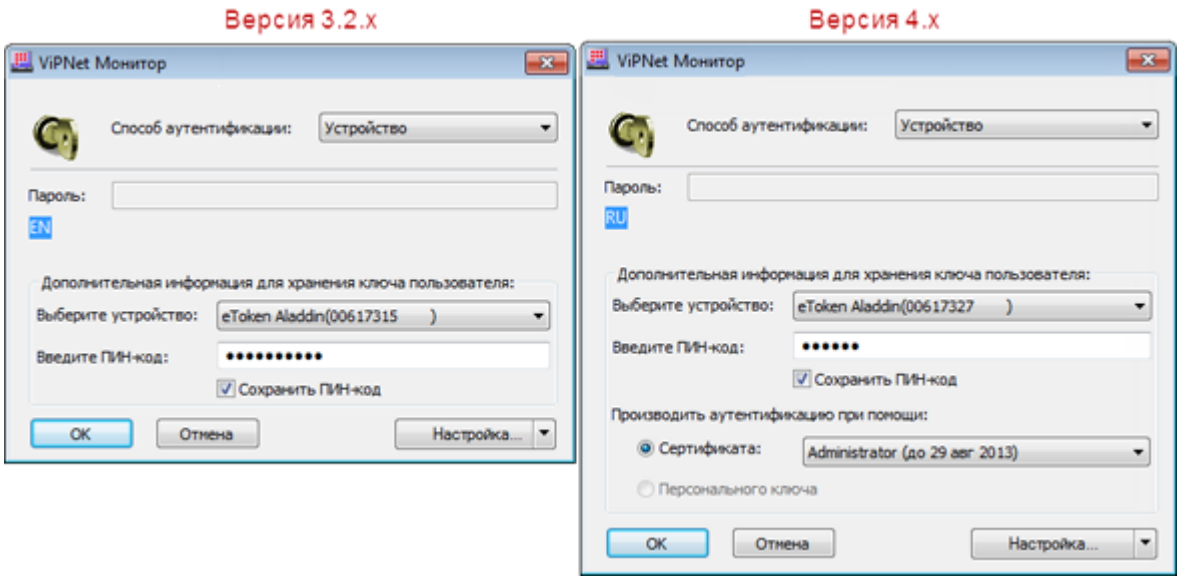


Рисунок 210: Использование устройства для аутентификации пользователя

Способ аутентификации **Пароль на устройстве** в дальнейшем поддерживаться не будет, поэтому в версии 4.0 рекомендуется перейти на другие способы аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 312).

Если для входа в программу используется пароль, то при смене пользователя достаточно выбрать в соответствующем списке учетную запись. При этом не требуется указывать папку ключей пользователя.

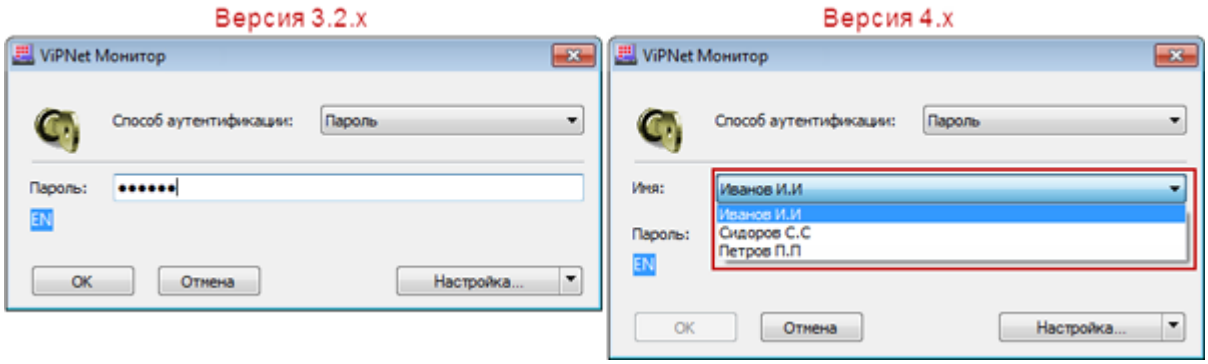


Рисунок 211: Аутентификация пользователя с помощью пароля

- **Система обновления ViPNet**

  В ViPNet Монитор версии 4.0 реализована новая система обновления, позволяющая принимать и устанавливать обновления программного обеспечения, справочников и ключей, а также политик безопасности, созданных в ViPNet Policy Manager. Система обновления продуктов ViPNet предоставляет удобный графический интерфейс для работы с поступившими файлами обновления.

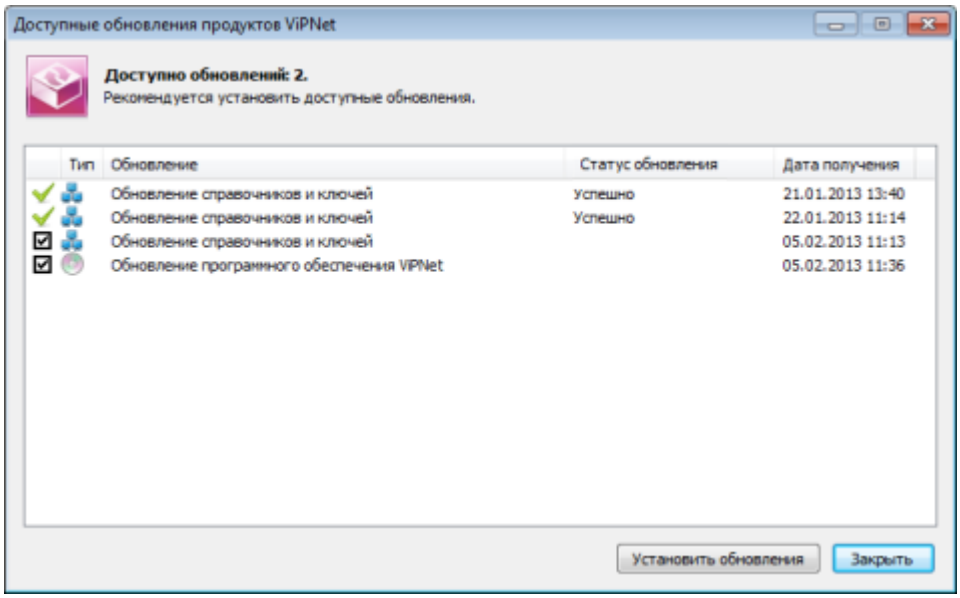


Рисунок 212: Список полученных обновлений

При поступлении файлов обновления вы получите уведомление.

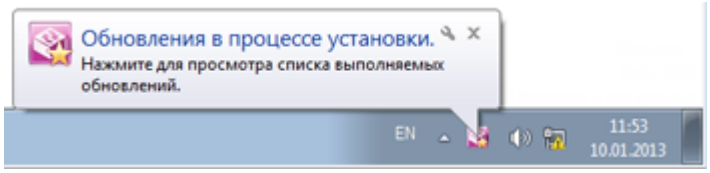


Рисунок 213: Уведомление о получении и установке файлов обновления

- **Создание фильтров для IP-пакетов**

  В программе ViPNet Монитор версии 4.0 реализована возможность использовать журнал IP-пакетов для создания фильтров (как разрешающих, так и блокирующих). В связи с этим удален раздел **Блокированные IP-пакеты** и все действия над IP-пакетами выполняются в разделе **Журнал IP-пакетов**.

- **Смена конфигураций программы**

  В программе ViPNet Монитор версии 4.x реализована возможность автоматической смены конфигураций. Если вы работаете с несколькими конфигурациями программы, каждую из которых нужно устанавливать в определенное время, вы можете настроить расписание смены этих конфигураций.

- **Ограниченный интерфейс пользователя**

  В версии 4.0 возможность ограничивать интерфейс пользователя (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 305) приравнена к назначению уровня полномочий 3. Таким образом, если узлу назначен уровень полномочий 3, то флажок ограничения интерфейса пользователя будет недоступен.

- **Блокировка компьютера и IP-трафика**

  В программе ViPNet Монитор версии 4.0 блокировка компьютера осуществляется стандартными средствами операционной системы. Реализована возможность блокировки всего IP-трафика (любые соединения с защищенными и открытыми узлами будут запрещены) и отключения защиты трафика (прекращение обработки трафика и ведения журнала регистрации IP-пакетов, отключение системы обнаружения атак).

- **Антиспуфинг**

  Для обеспечения высокого уровня безопасности сети в программе ViPNet Coordinator версии 3.2.x требуется выполнять настройку антиспуфинга. В версии 4.0 настройка антиспуфинга (см. «Антиспуфинг» на стр. 192) не требуется. При включении антиспуфинга соответствующие фильтры формируются автоматически на основе таблицы маршрутизации данного сетевого узла.

- **Задание фильтров для туннелируемых узлов**

В программе ViPNet Монитор 3.2.x для задания IP-адресов туннелируемых узлов в соответствующем разделе нужно нажать кнопку **IP-адреса** и добавить адреса. В версии 4.x IP-адреса туннелируемых узлов можно добавлять в окне настройки туннелирующего координатора в разделе **Туннелирование**. В этом разделе также отображается разрешенное количество одновременно туннелируемых узлов.

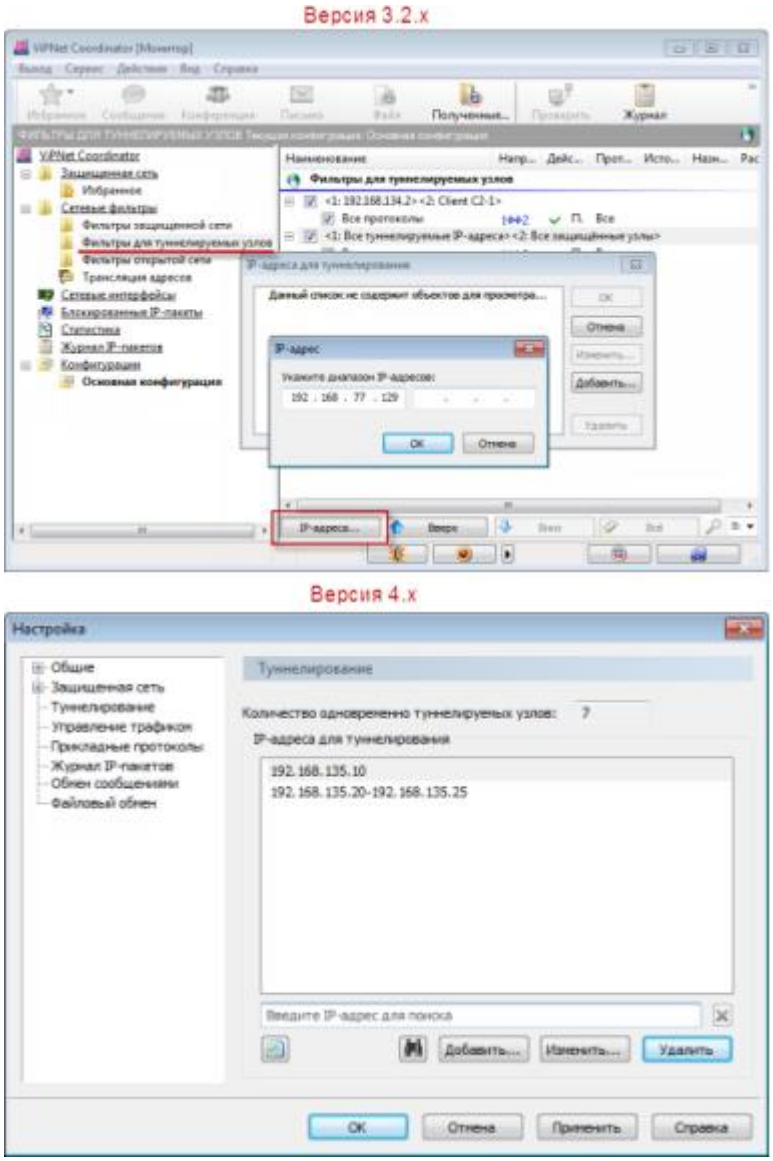


Рисунок 214: Задание адресов туннелируемых узлов

- **Настройка параметров сетевых интерфейсов**

  В ViPNet Монитор версии 4.0 в разделе **Сетевые интерфейсы** вы можете только просмотреть список сетевых интерфейсов на данном компьютере. Для настройки необходимого уровня безопасности нужно создать соответствующие фильтры и

указать в них нужные интерфейсы. Настройка антиспуфинга в версии 4.0 не требуется.

- **Возможность работы с программой SafeDisk-V**

  Программа ViPNet Coordinator 4.0 совместима с программой ViPNet SafeDisk-V версии 4.2. При запуске ViPNet SafeDisk-V 4.2 программа ViPNet Монитор перезапускается, и большинство настроек становятся недоступными для редактирования, в том числе в целях безопасности невозможно сменить пользователя или выйти из программы ViPNet Монитор.

- **Изменения в интерфейсе и терминологии**

  Таблица 21. Основные изменения в терминологии и интерфейсе

Что изменено	Версия 3.2.x	Версия 4.0
Термины	Абонентский пункт	Клиент
	Прикладная задача	Роль
	Правила фильтрация трафика	Сетевые фильтры
	Экспорт настроек	Сохранение настроек
	Импорт настроек	Восстановление настроек
Главное меню		Полностью переработано
Запуск компонентов Деловая почта, Контроль приложений, Файловый обмен, MFTP	Запускаются по нажатию соответствующих кнопок в главном окне программы ViPNet Монитор	Запускаются из меню **Приложения**
Сетевые фильтры		Представление фильтров в программах ViPNet Монитор и ViPNet Policy Manager было приведено к единому виду
Настройка управления трафиком	Окно **Настройка** разделы **Общие** и **Обнаружение атак**	Настройка вынесена в новый раздел, а именно окно **Настройка** раздел **Управление трафиком**
Блокировка компьютера	Кнопка в главном окне программы	Кнопка блокировки удалена

- **Обновление документации и справки**

  Документация и справка, поставляемые вместе с ПО ViPNet Coordinator, были существенно обновлены, для того чтобы отразить произошедшие изменения в функциональности программы.

Что нового в версии 3.2.11

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.11.

- **Исправление ошибок в программе ViPNet Coordinator**

  В программе ViPNet Coordinator исправлены следующие ошибки:

  - Невозможность регистрировать DNS-серверы в файле `DNS.TXT` на компьютере, имя которого содержит русские символы.
  - Невозможность удаленного подключения с помощью программы Remote Desktop Connection.

Что нового в версии 3.2.10

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.10.

- **Предупреждение о блокировании IP-пакетов**

  В программе ViPNet Монитор появилась возможность уведомления о блокировании IP-пакетов встроенным сетевым экраном. Чтобы включить уведомление, в окне **Настройка** в разделе **Общие > Предупреждения** установите флажок **Выдавать предупреждение о блокированных IP-пакетах**.

- **Исправление ошибок в ПО ViPNet Coordinator:**
  - Исправлена ошибка, вызывавшая критический системный сбой в операционной системе Windows XP SP3.
  - Исправлена ошибка при проверке соединения с узлами, на которых установлено ПО ViPNet более ранних версий.

- **Изменения, касающиеся работы с сертификатами открытого ключа:**
  - Прекращена поддержка алгоритма формирования и проверки электронной подписи ГОСТ Р 34.10-94.
  - Исправлены ошибки при опросе точек распространения списков отозванных сертификатов (COC).
  - Исправлены ошибки при формировании запроса на квалифицированный сертификат.

- **Исправление ошибок в ПО ViPNet Cluster**

Исправлены ошибки, связанные с произвольным переключением ролей кластера. Сокращено количество широковещательных пакетов, отправляемых элементами кластера.

Что нового в версии 3.2.9

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.2.9. Более подробная информация приведена в документе «Новые возможности ViPNet Client и ViPNet Coordinator версии 3.2. Приложение к документации ViPNet».

- **Совместимость с программным обеспечением других производителей**

  Обеспечена совместимость программного обеспечения ViPNet с приложениями Lumension Device Control, Cisco Security Agent, Kaspersky Administration Kit, MSDE 2000.

- **Улучшенная поддержка многоядерных процессоров**

  Оптимизирована параллельная обработка IP-пакетов в многопроцессорных системах. Благодаря своевременной обработке IP-пакетов и отправке полученных данных в нужной последовательности повышается скорость и качество передачи мультимедиа информации.

- **Автоматическая маршрутизация трафика на сетевом узле с несколькими сетевыми интерфейсами, а также при использовании нескольких каналов связи**

  Реализована маршрутизация IP-трафика, не зависящая от адресов видимости узлов. В результате маршрут IP-пакета на сетевом узле с несколькими сетевыми интерфейсами, а также канал передачи IP-пакета (в случае использования нескольких каналов) вычисляются автоматически, без дополнительно настройки.

- **Увеличение количества обрабатываемых программой прикладных протоколов**

  Расширен список прикладных протоколов, для которых в программе ViPNet Монитор реализована специальная обработка IP-пакетов.

- **Новый способ представления информации о блокированных IP-пакетах**

  В разделе **Блокированные IP-пакеты** главного окна представлены IP-пакеты, заблокированные с момента запуска программы ViPNet Монитор или с момента последней очистки списка.

- **Изменение отображения фильтров защищенной сети и задания правил фильтрации защищенного трафика**

  Информация обо всех фильтрах объединена в разделе **Сетевые фильтры** главного окна.

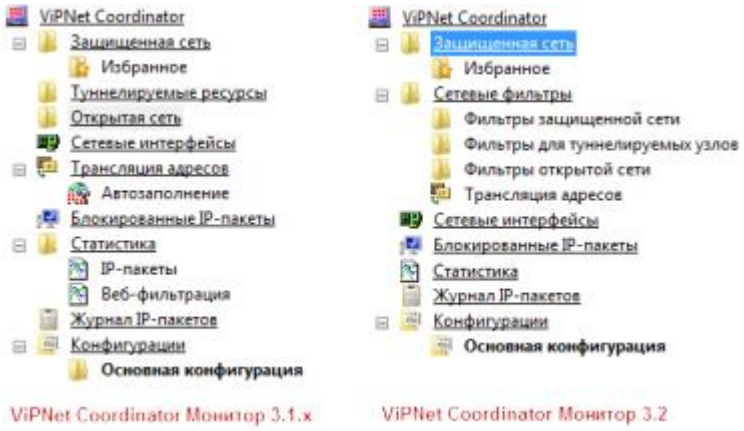


Рисунок 215: Список разделов в программе ViPNet Coordinator Монитор версий 3.1.x и 3.2

Приведена к единому виду структура фильтров защищенной и открытой сети, а также набор возможных действий с фильтрами.

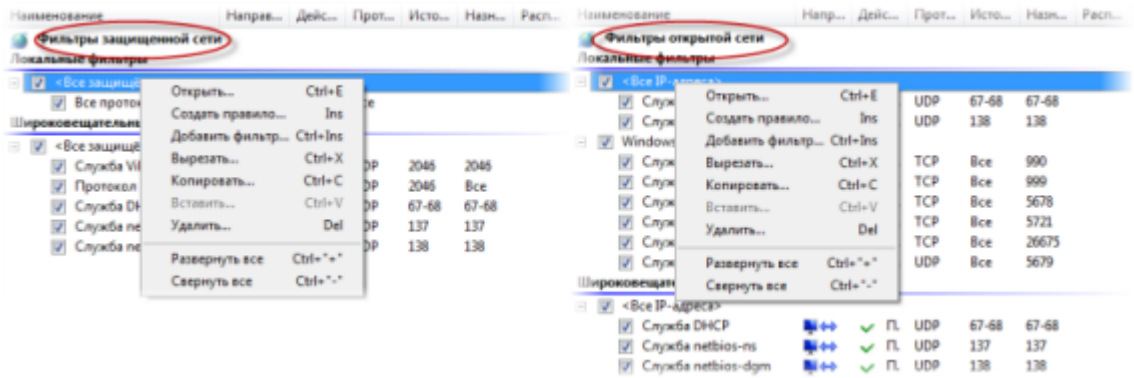


Рисунок 216: Отображение фильтров защищенной и открытой сетей в ПО ViPNet Монитор 3.2 и возможные действия с этими фильтрами

- **Автоматический вход в ПО ViPNet Coordinator**

  Реализована возможность входа в программу без необходимости подтверждения пароля пользователя ViPNet в окне входа в программу. Управление данной функцией возможно только в режиме администратора в окне **Настройка параметров безопасности** на вкладке **Администратор**. Если флажок **Автоматически входить в ViPNet** установлен, при запуске программы на текущем сетевом узле окно входа в программу не появляется и вход в ПО ViPNet Coordinator выполняется автоматически.

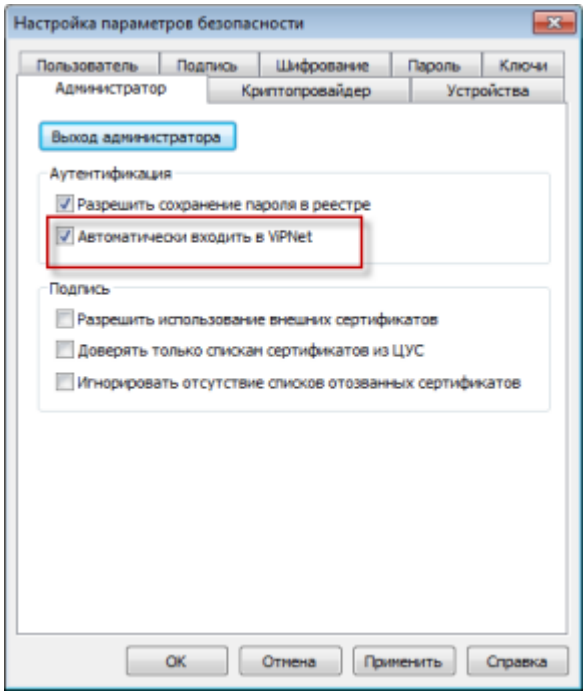


Рисунок 217: Настройка автоматического входа в ПО ViPNet Coordinator

- **Автоматическое получение и ввод в действие сертификатов, изданных по инициативе администратора без запроса со стороны пользователя**

  Реализована возможность автоматически получать и вводить в действие сертификаты, изданные администратором в программе ViPNet Удостоверяющий и ключевой центр по собственной инициативе. Если функция включена, получение таких сертификатов и ввод их в действие не требуют никаких дополнительных действий со стороны пользователя. После того как сертификат будет введен в действие, появится окно **Предупреждение сервиса безопасности** с соответствующим сообщением (см. «Сертификат, изданный по инициативе администратора, введен в действие» на стр. 388).

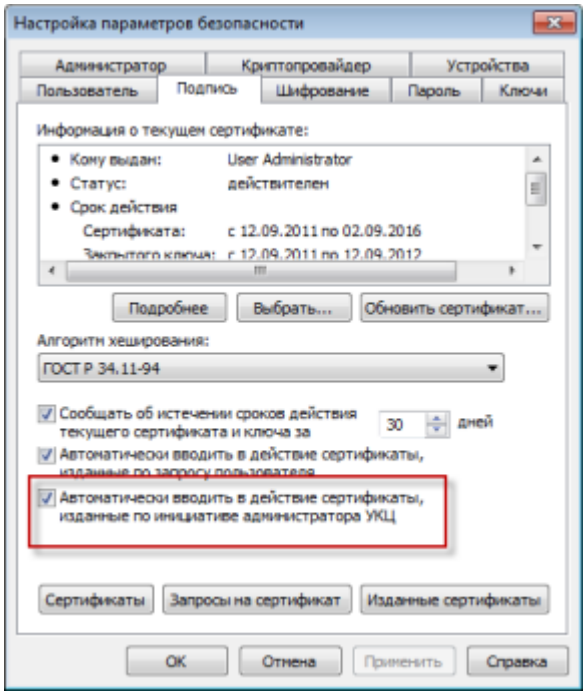


Рисунок 218: Новый элемент вкладки «Подпись» окна «Настройка параметров безопасности»

- **Разработан новый мастер установки ключей ViPNet**

  Новый мастер установки ключей поддерживает работу с дистрибутивами ключей, созданными в программе ViPNet Удостоверяющий и ключевой центр версий 2.8 и 3.x и в программе ViPNet Network Manager версий 2.x и 3.0. Кроме того, новый мастер обладает более богатыми функциональными возможностями и удобным пользовательским интерфейсом.

Внимание! В сетях ViPNet CUSTOM не рекомендуется использовать мастер **Установка ключей сети ViPNet** на сетевых узлах, на которых зарегистрировано несколько пользователей ViPNet или установлено несколько программ, использующих ключи ViPNet.

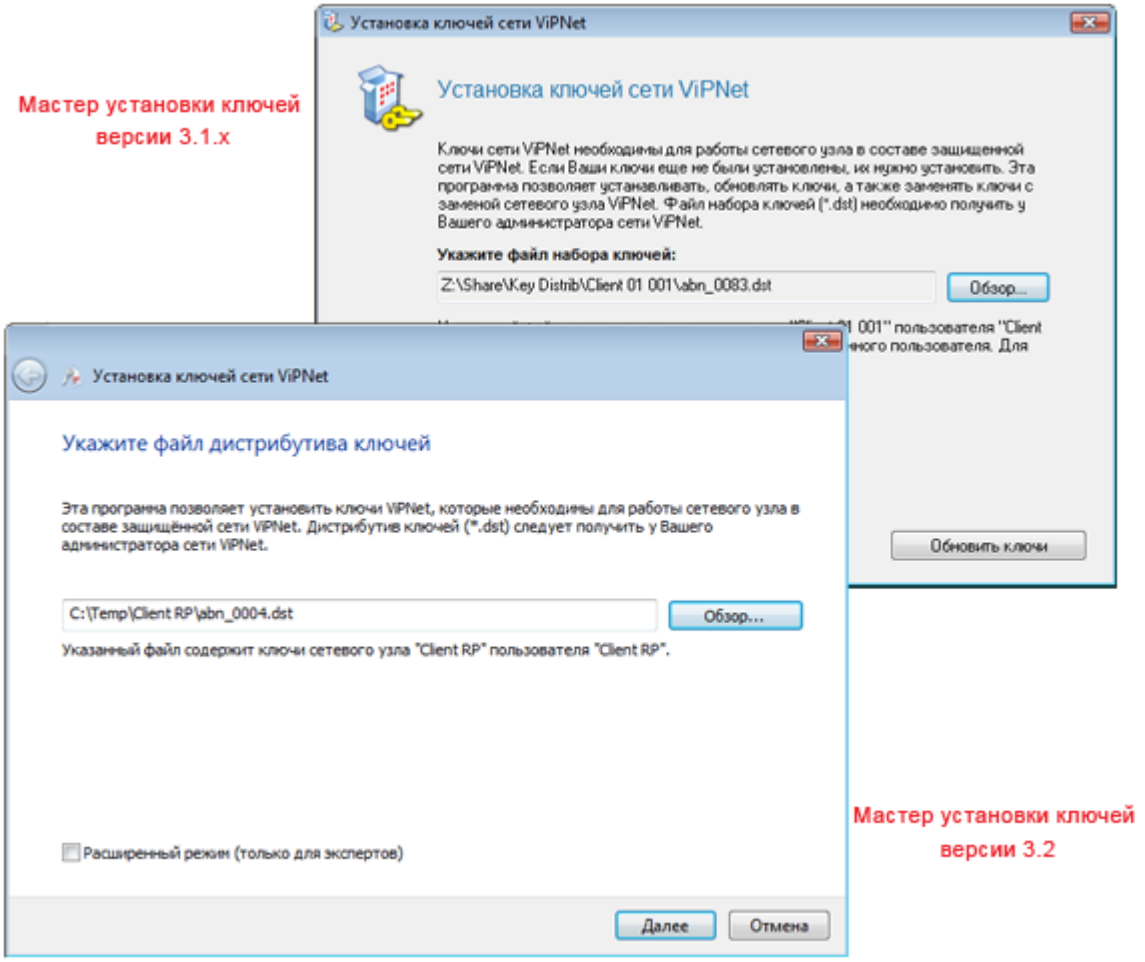


Рисунок 219: Новый мастер установки ключей ViPNet

- **Доработка Криптопровайдера ViPNet**

  Реализована следующая функциональность для компонента Криптопровайдер ViPNet:

  - поддержка TLS-протокола в ОС Windows 7;
  - совместимость с 64-разрядными операционными системами;
  - шифрование и электронная подпись в Microsoft Office 2010.

  Появилась возможность установки сертификата в контейнер ключей.

- **Доработка программы ViPNet Контроль приложений**

  Реализована следующая функциональность для программы ViPNet Контроль приложений:

  - совместимость с 64-разрядными операционными системами;

- работа в нескольких сессиях.

- **Расширен список поддерживаемых устройств аутентификации**

- Реализована поддержка следующих устройств аутентификации: Mifare, Mifare Standard 4K, eToken ГОСТ, JaCarta, устройства компании Gemalto с апплетом «Аладдин Р.Д.», устройство Kaztoken с поддержкой казахстанского стандарта электронной подписи. Теперь эти устройства можно применять для записи и считывания персональной информации.

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины**

  Для соответствия Федеральному закону 06.04.2011 N 63-ФЗ «Об электронной подписи» (текст закона http://www.rg.ru/2011/04/08/podpis-dok.html) термин «электронная цифровая подпись» («цифровая подпись») в интерфейсе программы изменен на термин «электронная подпись».

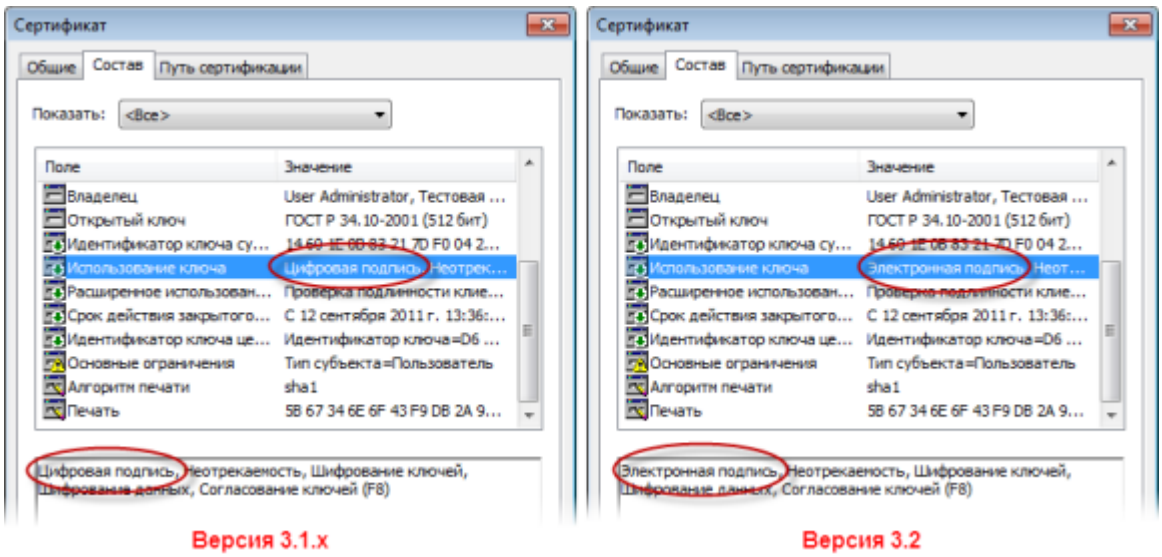


Рисунок 220: Изменение термина «цифровая подпись» на примере окна «Сертификат»

Прочие изменения терминологии приведены в таблице ниже:

Что изменено	До изменения, в версиях 3.1.x	В результате изменения, в версии 3.2
Название раздела в главном окне ПО ViPNet Coordinator Монитор	**Туннелируемые ресурсы**	**Фильтры для туннелируемых узлов**

Что изменено	До изменения, в версиях 3.1.x	В результате изменения, в версии 3.2
Раздел в главном окне ПО ViPNet Coordinator Монитор	**Автозаполнение**	Раздел отсутствует
Названия окон	**Туннелируемое правило**	**Туннельное правило**
	Туннелируемый фильтр	**Туннельный фильтр**
	Правило доступа (окно, вызываемое из раздела **Защищенная сеть**)	**Свойства узла**
Термины	**Правило доступа**	**Правило**
	Фильтр протоколов	**Фильтр**
Пункт меню **Сервис**	**Настройка прикладных протоколов**	Пункт отсутствует
Раздел окна **Настройка**	**Блокированные IP-пакеты**	Раздел отсутствует
Интерфейс для настройки параметров работы прикладных протоколов	Окно **Настройка прикладных протоколов**	Раздел **Настройка прикладных протоколов** в окне **Настройка**
Контекстное меню элементов раздела **Блокированные IP-пакеты** главного окна	Совпадает с контекстным меню элементов разделов **Открытая сеть** и **Защищенная сеть**	Индивидуальное контекстное меню

- **Доработка программы ViPNet Cluster**

  Изменилась логика синхронизации времени на элементах ViPNet-кластера. Теперь все элементы кластера синхронизируют системное время с элементом в роли представителя, а не с мастером. В связи с этим при необходимости можно настроить синхронизацию времени ViPNet-кластера как узла сети с внешним источником, например, NTP-сервером.

- **Обновление документации и справки**

  Документация и справка, поставляемые вместе с ПО ViPNet Coordinator, были существенно обновлены, для того чтобы отразить произошедшие изменения в функционале программы.

Что нового в версии 3.1.5

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.5.

- **Контроль работоспособности приложений, установленных на ViPNet-кластере**

  Реализована возможность организовать постоянное слежение за работоспособностью приложений, установленных на ViPNet-кластере и специально адаптированных для работы на нем. Это позволяет обеспечить высокий уровень отказоустойчивости и доступности данных приложений в процессе их работы. Настройка параметров контроля работоспособности приложений и мониторинг их состояния осуществляется с помощью программы ViPNet Cluster Монитор. Подробную информацию см. в документе «ViPNet Cluster. Руководство администратора».

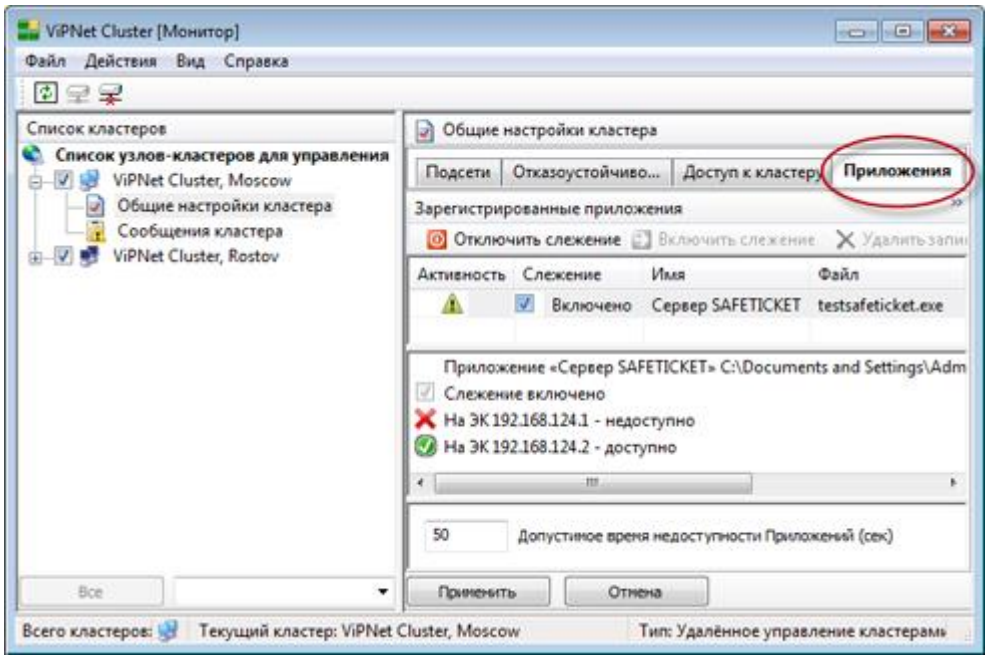


Рисунок 221: Настройка параметров контроля приложений в ViPNet Cluster Монитор

- **Изменены некоторые термины и названия элементов интерфейса, содержащие эти термины**

Старый термин	Новый термин
Режим авторизации	Способ аутентификации
Контейнер ключей подписи, ключевой контейнер, контейнер закрытого ключа, контейнер с закрытым ключом, контейнер с открытым ключом	Контейнер ключей
Дистрибутив справочно-ключевой информации	Дистрибутив ключей
Ключевой диск (КД)	Ключи пользователя ViPNet
Ключевой набор (КН)	Ключи узла ViPNet

В связи с изменениями переработан интерфейс программ ViPNet Client и ViPNet Coordinator.

Рисунок 222: Измененный интерфейс окна ввода пароля

В соответствии с заменой терминов обновлена документация и справка по всем продуктам.

- **Дополнена документация ViPNet Coordinator**

  В руководство администратора ViPNet Coordinator Монитор добавлен сценарий резервирования и аварийного восстановления координатора.

- **Документация и справка других локализаций**

  Проведена проверка актуальности документации и справки к продуктам ViPNet CUSTOM на других языках (немецком, испанском и французском) в соответствии с текущей русской версией. Также выполнено обновление английской документации и справки.

Что нового в версии 3.1.4

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.4.

- **Модернизированный механизм блокировки компьютера**

  Изменен механизм блокировки компьютера: теперь для блокировки используется встроенная функциональность ОС Windows.

- **Автоматическая защита узла при отключении устройства аутентификации пользователя**

  Добавлен контроль отключения аппаратных средств аутентификации пользователя. Теперь при отключении устройства аутентификации автоматически блокируется компьютер и IP-трафик. Режим блокировки можно изменить с помощью настроек: задать блокировку только компьютера, только IP-трафика либо не использовать блокировку.

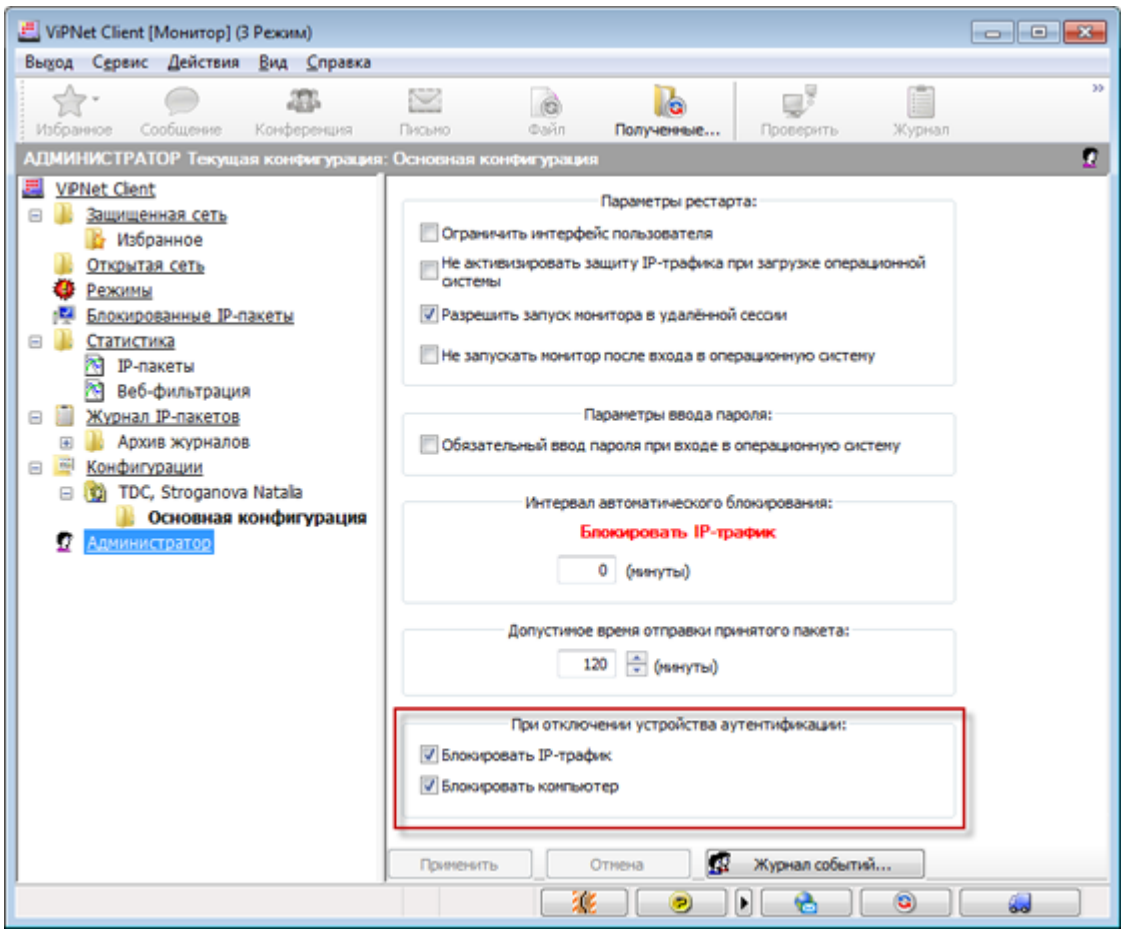


Рисунок 223: Настройка блокировки при отключении устройства аутентификации

- **Ограничение количества записей в разделе блокированных IP-пакетов**

  Реализован контроль числа отображаемых блокированных IP-пакетов. Теперь отображается не более 300 IP-адресов и для каждого адреса не более 30 записей по каждому порту. Информация в разделе блокированных IP-пакетов обновляется при каждом открытии или обновлении раздела. Если при этом указанные ограничения окажутся превышены, то будут удалены самые старые записи и добавлены новые.

- **Более информативный экспортированный журнал IP-пакетов**

  Расширен список параметров IP-пакетов, включаемых в экспортированную версию журнала IP-пакетов. Теперь при просмотре журнала в веб-браузере или в Microsoft Excel отображается полная информация о пакетах.

- **Более информативные сведения о числе элементов в папках программы ViPNet Деловая почта**

  Изменен принцип отображения числа элементов в папках программы ViPNet Деловая почта. Теперь при перемещении по дереву папок отображается общее число элементов, содержащихся в текущей папке и всех ее подпапках. Для папки «Входящие» дополнительно отображается число непрочитанных писем, а для папки «Исходящие» — число недоставленных писем.

- **Корректное отображение последней выделенной позиции в папке при переходе между папками программы ViPNet Деловая почта**

  Реализовано сохранение позиции последнего выбранного элемента при переходе между папками программы ViPNet Деловая почта. Теперь при переходе из одной папки в другую запоминается позиция выбранного элемента, и при возврате в папку этот элемент остается выбранным и находится в той же позиции экрана.

- **Доработка поиска в программе ViPNet Деловая почта**

  Изменена логика при открытии окна поиска в программе ViPNet Деловая почта. Теперь в качестве папки поиска (поле **Искать в**) подставляется текущая папка, а также не перемещается фокус (текущим всегда является поле **Архив**).

- **Более прозрачная логика обработки входящих писем правилами автопроцессинга**

  Изменена логика обработки входящих писем правилами автопроцессинга программы ViPNet Деловая почта. В новой версии:

  - если в правиле задан список отправителей, то под это правило подпадают входящие письма, отправитель которых входит в заданный список;
  - если в правиле задан список пользователей для проверки подписи, то под это правило подпадают входящие письма, вложения которых подписаны одним из заданных пользователей (при условии действительности подписи);

- входящие письма с отсутствующим текстом (телом письма) не копируются на диск в виде файла blank.txt.

- **Более понятное управление включением и отключением криптопровайдера ViPNet CSP**

  Изменен способ включения и отключения криптопровайдера ViPNet CSP в настройках параметров безопасности (на вкладке Криптопровайдер). Теперь вместо флажка используется кнопка, а также отображается понятное сообщение в случае отсутствия прав на изменение этого параметра.

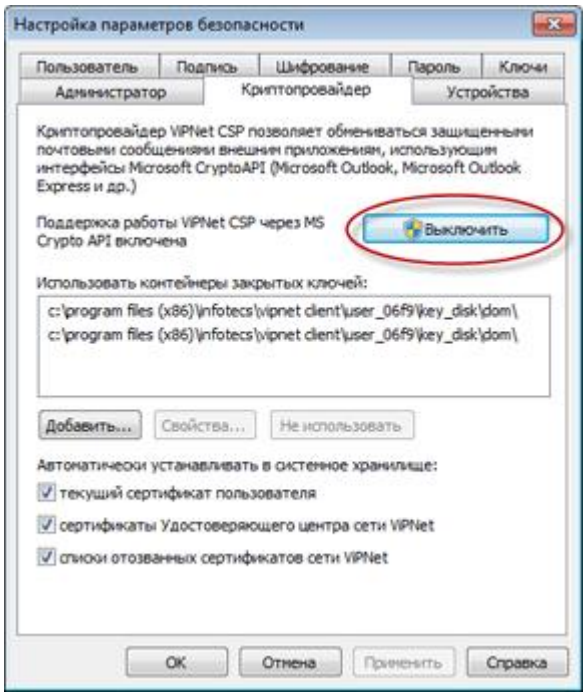


Рисунок 224: Кнопка включения и отключения криптопровайдера

- **Устранена проблема входа в программу ViPNet Монитор при использовании Network Logon 5.1**

  Обеспечена совместимость программы ViPNet Монитор с eToken Network Logon 5.1. Теперь вход в ViPNet Монитор происходит одинаково как при использовании Network Logon 5.1, так и без него.

- **Улучшенная справка**

  Изменен внешний вид справки, улучшена наглядность предоставляемой справочной информации.

- **Документация и справка других локализаций**

Выпущена документация и справка к продуктам ViPNet CUSTOM на испанском языке. Документация и справка на немецком и французском языках обновлены в соответствии с русской версией. Также выполнено обновление английской документации и справки.

Что нового в версии 3.1.3

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.3.

- **Сняты ограничения на удаленный запуск ПО ViPNet**

  Изменено значение параметра «Разрешить запуск монитора в удаленной сессии», используемое по умолчанию. Теперь удаленным пользователям запуск ViPNet Монитор по умолчанию разрешен.

- **Оптимизирована межузловая рассылка**

  Существенно сокращено число служебных рассылок между сетевыми узлами. Теперь информация о состоянии и параметрах узлов отправляется только тем узлам сети, которым эта информация действительно необходима. Для снижения числа рассылок дополнительно используется агрегирование сообщений в течение определенного периода времени.

- **Поддержка DHCP-протокола при работе в конфигурации «Открытый Интернет»**

  Изменена технология выхода защищенных узлов в открытый Интернет. Теперь при работе в конфигурации «Открытый Интернет» узлы могут получать IP-адреса от защищенного DHCP-сервера.

- **Поддержка кластера на 64-разрядных ОС**

  Реализована поддержка функционирования ПО ViPNet Cluster на координаторах, работающих под управлением 64-разрядных операционных систем.

- **Расширенная поддержка системы централизованного мониторинга ViPNet StateWatcher**

  Реализован агент мониторинга, расширяющий сбор информации о состоянии узлов сети ViPNet. Теперь можно анализировать работоспособность транспортного модуля MFTP и программы ViPNet Деловая почта, количество конвертов в очереди и их суммарный размер, список туннелируемых координатором адресов, суммарный трафик на каждом сетевом интерфейсе (отдельно исходящий и входящий), загрузку процессора, использование памяти и дискового пространства, записи о событиях из системного журнала и журнала приложений ОС Windows.

- **Усилена защита от некорректной установки или обновления ключей на сетевых узлах**

  Реализован контроль соответствия дистрибутива ключей (файла *.dst) типу сетевого узла (клиент или координатор). Теперь установка или обновление выполняются, только если дистрибутив создан для того же приложения (ViPNet Client или ViPNet Coordinator), которое установлено на узле.

- **Документация и справка других локализаций**

  Появилась документация и справка к продуктам ViPNet CUSTOM на немецком и французском языках.

Что нового в версии 3.1.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 3.1.2.

- **Более понятные названия способов аутентификации.**

  Названия режимов, используемых для авторизации пользователей, переименованы следующим образом:

  - **Пароль.**
  - **Пароль на устройстве.**
  - **Устройство.**

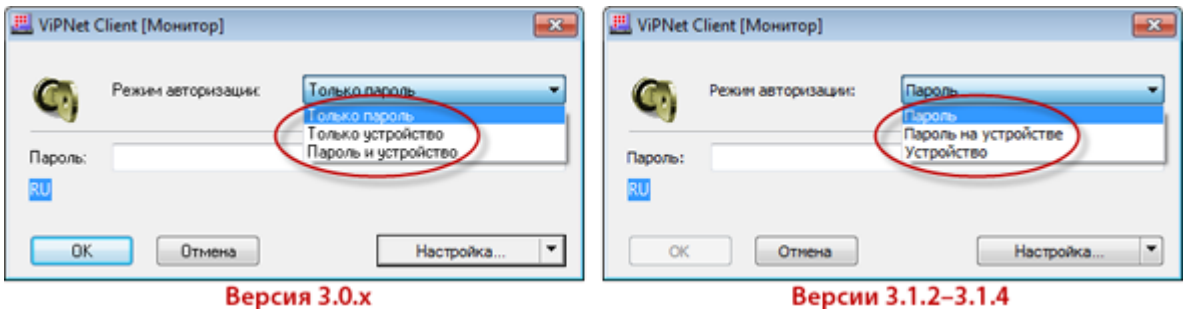


Рисунок 225: Изменение типов авторизации

- **Оптимальное расположение различных настроек**

  Настройки, находившиеся на панели навигации, удалены с неё и объединены с другими настройками.

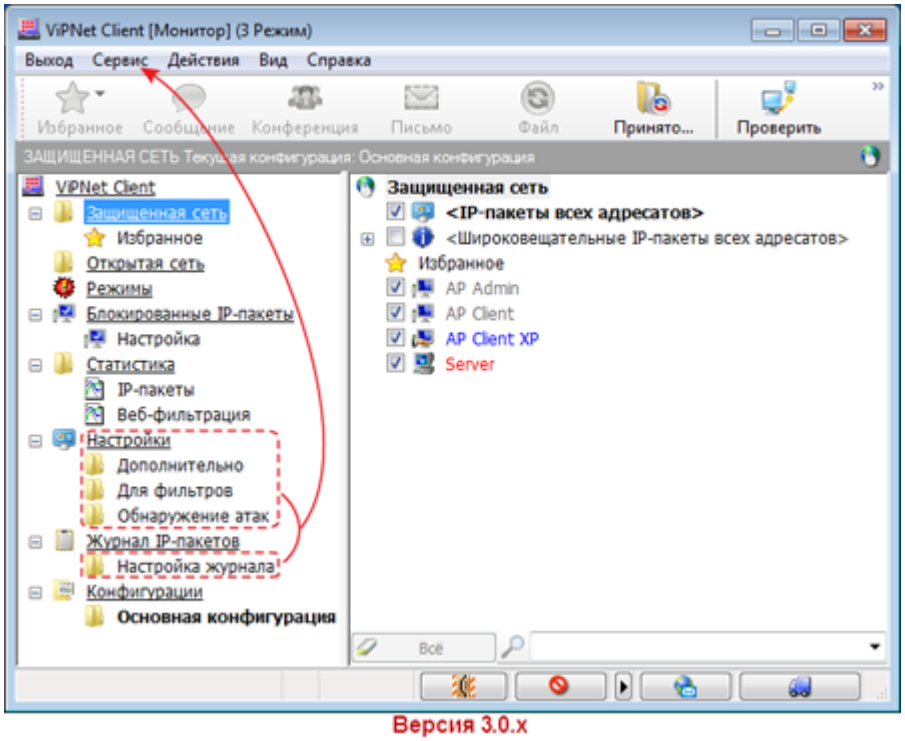


Рисунок 226: Изменение местоположения настроек защищенной сети

Теперь все настройки содержатся в одном окне, которое вызывается по команде **Сервис > Настройки**.

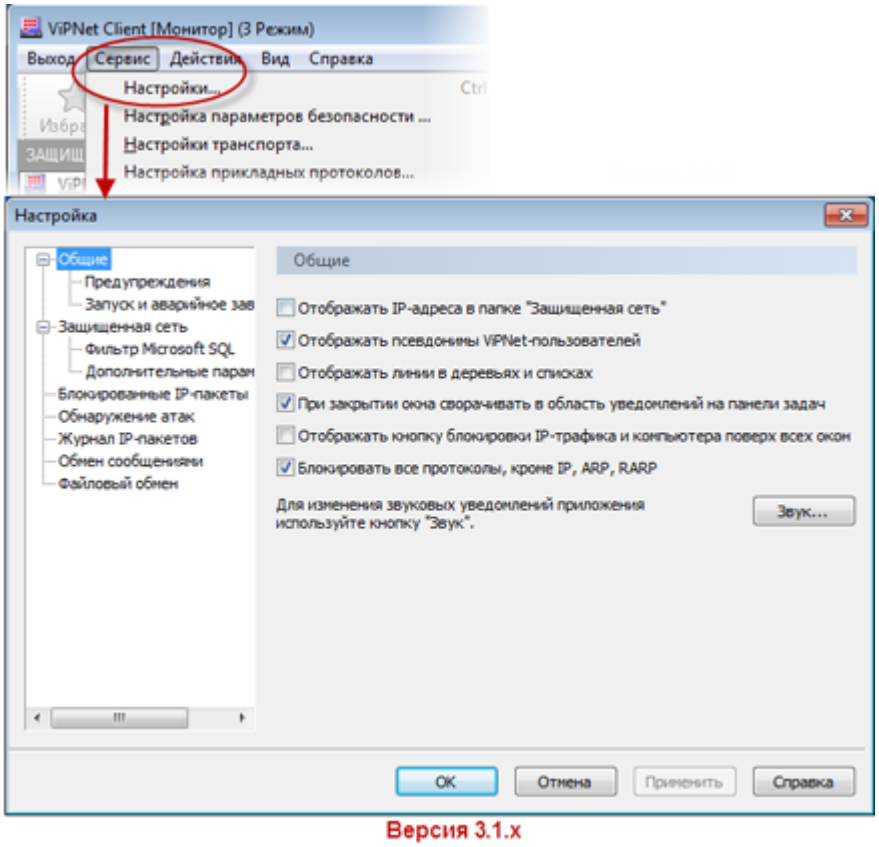


Рисунок 227: Настройки защищенной сети в новой версии

- **Дополнительный способ проверки соединения с узлом**

  Появилась возможность проверить соединение с узлом в течение сеанса обмена защищенными сообщениями с этим узлом. Для этого достаточно щелкнуть узел правой кнопкой мыши и в контекстном меню выбрать команду **Проверить соединение**.

- **Более удобный способ просмотра информации о статусе нескольких узлов**

  При проверке соединения сразу с несколькими сетевыми узлами информация о статусе этих узлов отображается не в отдельных окнах, а в одном окне.

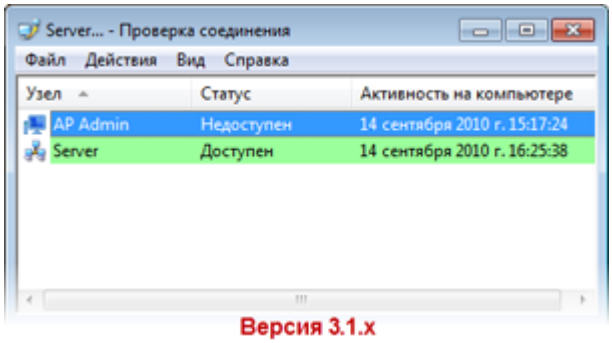


Рисунок 228: Проверка соединения с несколькими узлами сети

- **Детализация информации о доступности узла**

  К сообщениям, выводимым при проверке соединения с узлом, добавлено специальное сообщение для ситуации, когда узел доступен по сети, но ПО ViPNet на нем неактивно.

- **Более простая процедура отправки файлов**

  Сократилось количество действий, необходимых для отправки файлов получателям.

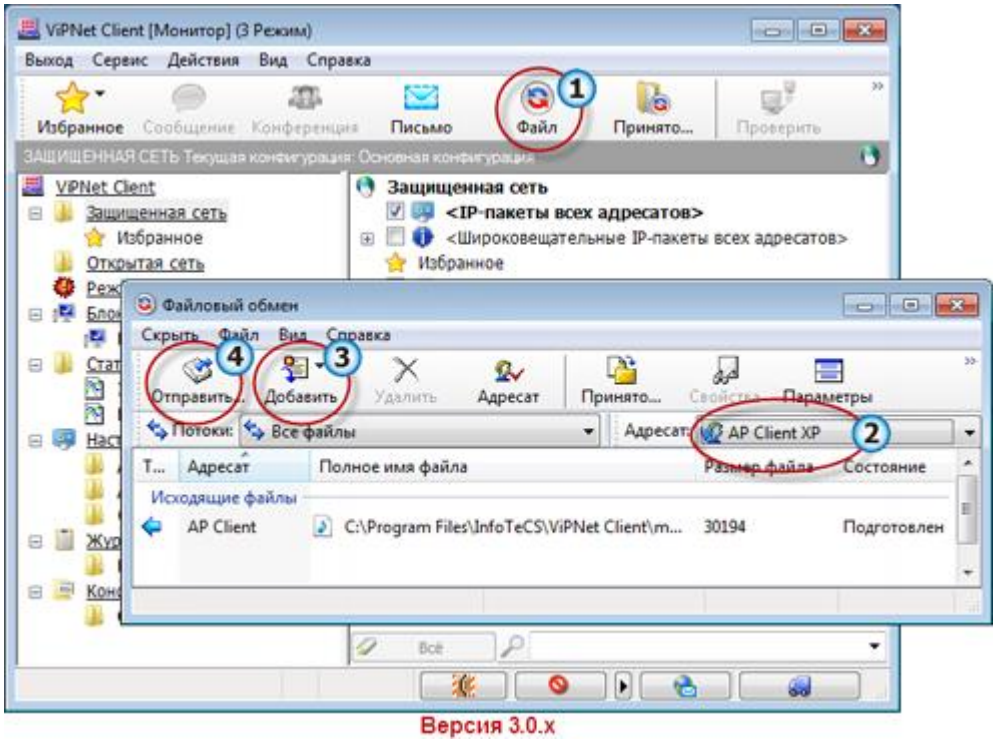


Рисунок 229: Процесс файлового обмена

Теперь отправка файлов осуществляется сразу после выбора получателя (сетевого узла).

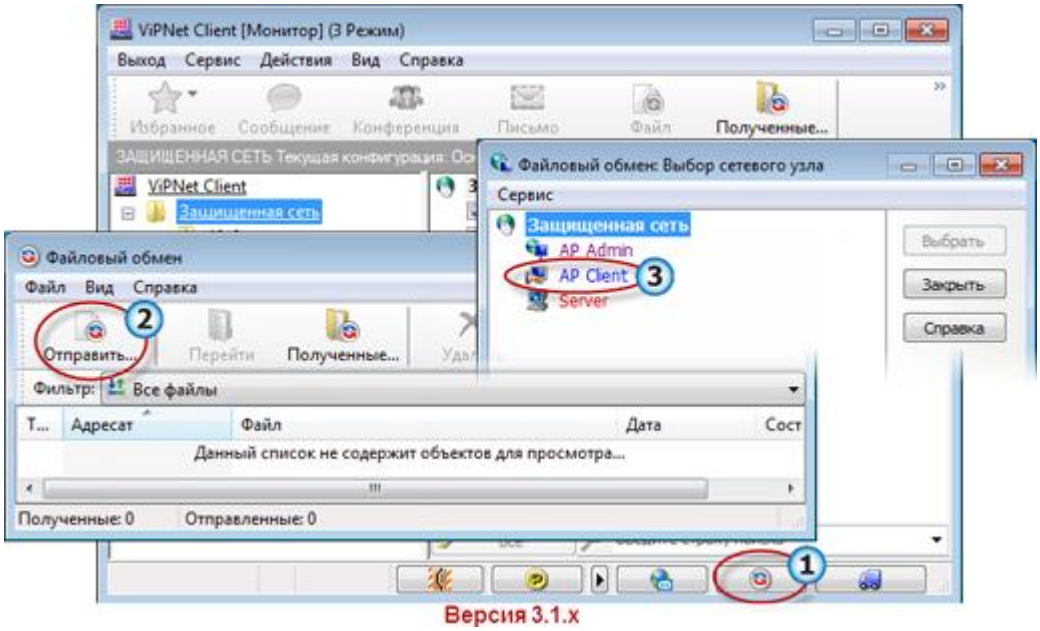


Рисунок 230: Измененный процесс файлового обмена

- **Возможность добавления правил фильтрации при просмотре блокированных IP-пакетов**

  Появилась возможность добавлять правила фильтрации для открытой сети и туннелируемых узлов из окна блокированных IP-пакетов.

- **Расширенные возможности поиска**

  Расширен список параметров, по которым выполняется поиск сетевых узлов. Теперь узлы можно искать по имени или идентификатору узла, имени компьютера, псевдониму, DNS-имени, по виртуальным и реальным IP-адресам.

- **Дополнительные способы входа в режим администратора**

  Появилась возможность быстро войти в режим администратора одним из следующих способов: из области уведомлений Windows или по команде **Сервис > Вход администратора**.

- **Унификация логики доступа к журналу IP-пакетов**

  Переход к просмотру журнала IP-пакетов, выполняемый из разных точек интерфейса, теперь происходит одинаковым образом: сначала открывается окно поиска для задания параметров отбора записей из журнала, затем — окно просмотра отобранных записей.

- **Возможность настройки некоторых параметров при входе в программу**

Появилась возможность указать транспортный каталог и каталог ключей пользователя при входе в программу.

- **Новый механизм включения антиспуфинга на координаторе**

  Изменен механизм включения антиспуфинга на координаторе: теперь антиспуфинг включается отдельно для каждого сетевого интерфейса.

- **Дополнительные полномочия пользователей**

  Добавлена поддержка новых полномочий «h» для прикладной задачи «Защита трафика». При этом уровне полномочий на узле всегда присутствуют две фиксированные конфигурации «Внутренняя сеть» и «Интернет». В конфигурации «Внутренняя сеть» разрешена работа с ресурсами защищенной сети и запрещен доступ в Интернет, в конфигурации «Интернет» разрешена работа в Интернете и запрещен доступ в защищенную сеть.

- **Независимость установки ПО ViPNet от текущей локализации**

  Убраны отличия в регистрации ПО ViPNet различных локализаций. Теперь при обновлении ПО ViPNet можно установить поверх используемой версии версию другой локализации.

- **Расширенная поддержка протокола SIP**

  Реализована поддержка протокола SIP в случае, когда на компьютере установлено несколько сетевых интерфейсов. Теперь в этом случае есть возможность пользоваться IP-телефонией, защищенной технологиями ViPNet.

- **Автоматическая настройка доступа к корпоративным защищенным DNS- и WINS-серверам**

  Реализована регистрация защищенных DNS- и WINS-серверов средствами ПО ViPNet (см. «Создание списка DNS (WINS) серверов вручную» на стр. 150). Теперь достаточно внести информацию о серверах в специальный файл, и их IP-адреса автоматически будут добавлены в настройки сетевых интерфейсов. Автоматическая настройка удобна для мобильных пользователей, а также в случае, если DNS- и WINS-серверы доступны по виртуальным адресам.

- **Усовершенствованная документация и справка**

  Полностью переработаны документация и справка, улучшено их качество. При переработке документации акцент сделан на сценарный подход.

Глоссарий

D

DMZ (демилитаризованная зона)

Физическая или логическая подсеть, предоставляющая доступ к внешним корпоративным службам из большей сети, с которой нет отношений доверия, как правило, из Интернета. При этом серверы, отвечающие на запросы из внешней сети или направляющие туда запросы, находятся в этой подсети и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана. Прямых соединений между внутренней сетью и внешней нет: любые соединения возможны только с серверами в DMZ, которые обрабатывают запросы и формируют свои, возвращая ответ получателю уже от своего имени.

См. также: Внешняя сеть (на стр. 483), Внутренняя сеть (на стр. 484).

V

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

См. также: Сеть ViPNet (на стр. 491), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 481), ViPNet Центр управления сетью (ЦУС) (на стр. 481).

ViPNet Network Manager

Программа, которая входит в состав программного комплекса ViPNet VPN. Предназначена для создания, конфигурирования и управления малыми и средними сетями ViPNet.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками отозванных сертификатов.

См. также: Администратор УКЦ (на стр. 481), ViPNet Administrator (на стр. 480).

ViPNet Центр управления сетью (ЦУС)

В сети ViPNet CUSTOM ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

В сети ViPNet VPN Центр управления сетью — это рабочее место администратора сети ViPNet. В ЦУСе создается структура сети ViPNet, формируются и отправляются на сетевые узлы обновления наборов ключей и программного обеспечения ViPNet.

См. также: Клиент (ViPNet-клиент) (на стр. 485), Ключи узла ViPNet (на стр. 485), Полномочия пользователя (на стр. 488), Справочники (на стр. 491), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 481), ViPNet Administrator (на стр. 480), ViPNet Network Manager (на стр. 480).

А

Администратор УКЦ

Лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

См. также: Сетевой узел ViPNet (на стр. 491), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 481).

Администратор ЦУСа

Лицо, обладающее правом доступа к программе ViPNet Центр управления сетью (ЦУС) и отвечающее за создание и настройку сети ViPNet, создание и рассылку адресных справочников, обновление ключей, обновление программного обеспечения ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

См. также: Сеть ViPNet (на стр. 491), ViPNet Центр управления сетью (ЦУС) (на стр. 481).

Адрес источника

Адрес сетевого устройства, отправившего IP-пакет.

См. также: Адрес назначения (на стр. 482).

Адрес назначения

Адрес сетевого устройства, на которое отправлен IP-пакет.

См. также: Адрес источника (на стр. 482).

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

См. также: Виртуальный IP-адрес (на стр. 483), Реальный IP-адрес (на стр. 489).

Антиспуфинг

Защита от спуфинг-атак, при которых злоумышленник подделывает адрес источника для обхода межсетевых экранов и организации DoS-атак (от англ. Denial of Service, отказ в обслуживании).

Аутентификация

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

В

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

См. также: Аутентификация (на стр. 482), Внешняя сеть (на стр. 483).

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet Б назначаются непосредственно на узле А. На других узлах узлу ViPNet Б могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

См. также: Реальный IP-адрес (на стр. 489).

Внешние IP-адреса

Адреса внешней сети.

См. также: Внешняя сеть (на стр. 483).

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

См. также: Внутренняя сеть (на стр. 484).

Внутренняя сеть

Локальная сеть, где находятся рассматриваемые узлы, которая отделена от внешней сети межсетевым экраном.

См. также: Внешняя сеть (на стр. 483).

Д

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

См. также: Сетевой узел ViPNet (на стр. 491), Справочники (на стр. 491), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 481).

З

Закрытый ключ

Закрытая (секретная) часть пары асимметричных ключей. Служит для создания электронных подписей, которые можно проверять с помощью парного ему открытого ключа, или для расшифрования сообщений, которые были зашифрованы парным ему открытым ключом.

Ключ электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является закрытым ключом.

См. также: Открытый ключ (на стр. 487), Электронная подпись (на стр. 494).

Защищенное соединение

Соединение между узлами, зашифрованное с помощью программного обеспечения ViPNet.

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

К

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

См. также: Координатор (ViPNet-координатор) (на стр. 485), Маршрутизация (на стр. 486), Сетевой узел ViPNet (на стр. 491).

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

См. также: Сетевой узел ViPNet (на стр. 491), Электронная подпись (на стр. 494).

Контейнер ключей

Файл, в котором хранятся закрытый ключ и соответствующий ему сертификат открытого ключа.

См. также: Закрытый ключ (на стр. 484), Сертификат открытого ключа подписи пользователя (на стр. 490).

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator или ViPNet Coordinator Linux) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

См. также: Маршрутизация (на стр. 486), Сеть ViPNet (на стр. 491).

Координатор соединений

Координатор, с помощью которого клиенты организуют соединения друг с другом в том случае, если находятся в разных подсетях и не могут установить соединение напрямую. Для каждого клиента можно выбрать свой координатор соединений. По умолчанию координатором соединений для клиента назначен сервер IP-адресов.

См. также: Клиент (ViPNet-клиент) (на стр. 485), Координатор (ViPNet-координатор) (на стр. 485), Сервер IP-адресов (на стр. 490).

Корневой сертификат

Самоподписанный сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

См. также: Сертификат издателя (на стр. 490), Сертификат открытого ключа подписи пользователя (на стр. 490).

Л

Лицензия на сеть ViPNet CUSTOM

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet CUSTOM. В частности, лицензия на сеть ViPNet CUSTOM определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешенную версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

См. также: Клиент (ViPNet-клиент) (на стр. 485), Координатор (ViPNet-координатор) (на стр. 485), Роль (на стр. 489), Сеть ViPNet (на стр. 491).

М

Маршрутизация

Процесс выбора пути для передачи информации.

О

Обновление справочников и ключей

Файлы, формируемые администратором сети ViPNet в управляющем приложении (ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр, ViPNet Network Manager) при изменении справочников и ключей для сетевых узлов ViPNet, то есть, в случае добавления, удаления сетевого узла ViPNet, добавления пользователя, издания нового сертификата и так далее. Администратор сети ViPNet централизованно высылает на сетевой узел сформированные новые ключи и справочники из ЦУСа или ViPNet Network Manager.

См. также: Сетевой узел ViPNet (на стр. 491), Сеть ViPNet (на стр. 491), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 481), ViPNet Центр управления сетью (ЦУС) (на стр. 481), ViPNet Network Manager (на стр. 480).

Открытый Интернет

Технология, реализованная в программном обеспечении ViPNet. При подключении к Интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от Интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

См. также: Сеть ViPNet (на стр. 491).

Открытый ключ

Последовательность символов, связанная с закрытым ключом определенным математическим соотношением. Открытый ключ доступен любым пользователям информационной системы и предназначен для подтверждения подлинности электронной подписи (или шифрования).

Ключ проверки электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является открытым ключом.

См. также: Закрытый ключ (на стр. 484), Электронная подпись (на стр. 494).

Открытый узел

Узел, с которым обмен информацией происходит в незашифрованном виде.

См. также: Туннелируемый узел (на стр. 492).

П

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

Папка ключей сетевого узла

Папка, в которой находятся ключи сетевого узла ViPNet и справочники.

См. также: Ключи узла ViPNet (на стр. 485), Справочники (на стр. 491).

Пароль администратора сетевого узла ViPNet

Пароль для включения на сетевом узле ViPNet режима администратора, в рамках которого появляются дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан в УКЦ или ViPNet Network Manager администратором сети ViPNet.

См. также: Сетевой узел ViPNet (на стр. 491), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 481), ViPNet Network Manager (на стр. 480).

Политика безопасности

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

См. также: Сетевой узел ViPNet (на стр. 491).

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

См. также: Администратор ЦУСа (на стр. 482), Пароль администратора сетевого узла ViPNet (на стр. 488), Роль (на стр. 489), Сетевой узел ViPNet (на стр. 491).

Порт источника

TCP- или UDP-порт, используемый отправителем пакета при его отправке.

Порт назначения

TCP- или UDP-порт, на который посылается пакет.

Протокол Диффи — Хеллмана

Протокол открытого распределения ключей, позволяющий двум пользователям вырабатывать общий секретный ключ путем динамического взаимодействия на основе обмена открытыми сообщениями без какой-либо общей секретной информации, распределяемой заранее.

Публичный адрес

IP-адрес, который может применяться в Интернете.

См. также: Частный адрес (на стр. 493).

Р

Реальный IP-адрес

IP-адрес, назначенный сетевому интерфейсу компьютера в локальной сети или Интернете.

См. также: Виртуальный IP-адрес (на стр. 483), Сетевой интерфейс (на стр. 490).

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ или ViPNet Network Manager создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

См. также: Администратор УКЦ (на стр. 481), Дистрибутив ключей (на стр. 484).

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла `infotecs.reg` и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

См. также: Полномочия пользователя (на стр. 488), Сеть ViPNet (на стр. 491).

С

Сеансовый ключ

Случайный или производный ключ, предназначенный для шифрования одного сообщения.

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

См. также: Защищенный узел (на стр. 484), Координатор (ViPNet-координатор) (на стр. 485).

Сертификат издателя

Сертификат уполномоченного лица удостоверяющего центра, которым заверяются издаваемые сертификаты.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 490).

Сертификат открытого ключа подписи пользователя

Электронный документ определенного формата, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, открытый ключ, сведения о его назначении и области применения, информацию о выпустившем сертификат удостоверяющем центре, период действия сертификата, а также некоторые дополнительные параметры. В программе ViPNet Удостоверяющий и ключевой центр сертификат создается в соответствии со стандартом X.509 v3 и заверяется электронной подписью администратора УКЦ.

В терминологии Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» сертификат открытого ключа подписи пользователя называют «сертификатом ключа проверки электронной подписи».

См. также: Администратор УКЦ (на стр. 481), Открытый ключ (на стр. 487), Электронная подпись (на стр. 494), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 481).

Сетевой интерфейс

Устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. Сетевым интерфейсом может служить сетевая плата, модем и другие подобные устройства.

Сетевой порт

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

Сетевой узел ViPNet

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

См. также: ViPNet Центр управления сетью (ЦУС) (на стр. 481), ViPNet Network Manager (на стр. 480).

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

См. также: Сетевой узел ViPNet (на стр. 491).

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в управляющих приложениях ViPNet, предназначенных для создания структуры и конфигурирования сети ViPNet (ViPNet Центр управления сетью, ViPNet Network Manager).

См. также: ViPNet Центр управления сетью (ЦУС) (на стр. 481), ViPNet Network Manager (на стр. 480).

Статический адрес

Постоянный IP-адрес, присвоенный сетевому интерфейсу вручную.

Структура сети ViPNet

Упорядоченная совокупность связей между компонентами сети ViPNet, такими как:

- рабочее место администратора сети ViPNet;
- координаторы;
- клиенты.

Каждый клиент должен быть зарегистрирован на координаторе. Связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

См. также: Клиент (ViPNet-клиент) (на стр. 485), Координатор (ViPNet-координатор) (на стр. 485), Сеть ViPNet (на стр. 491).

Т

Трансляция сетевых адресов (NAT)

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

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на сетевые узлы ViPNet транспортным модулем ViPNet MFTP.

См. также: Транспортный модуль (MFTP) (на стр. 492).

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

См. также: Клиент (ViPNet-клиент) (на стр. 485), Координатор (ViPNet-координатор) (на стр. 485).

Туннель

Канал связи между конечными точками сети или взаимодействующих сетей, созданный с помощью технологии туннелирования.

Ц

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

См. также: Корневой сертификат (на стр. 486), Сертификат открытого ключа подписи пользователя (на стр. 490).

Ч

Частный адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к Интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в Интернете. Чтобы выйти в Интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

См. также: Публичный адрес (на стр. 489), Трансляция сетевых адресов (NAT) (на стр. 492).

Ш

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие.

Шлюзовые координаторы назначаются в ЦУСе каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

См. также: Координатор (ViPNet-координатор) (на стр. 485), Межсетевое взаимодействие, Сеть ViPNet (на стр. 491), Транспортный конверт (на стр. 492), ViPNet Центр управления сетью (ЦУС) (на стр. 481).

Э

Электронная подпись

Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата открытого ключа подписи пользователя, а также установить отсутствие искажения информации в электронном документе.

См. также: Закрытый ключ (на стр. 484), Сертификат открытого ключа подписи пользователя (на стр. 490).

Указатель

Т

У

Ф