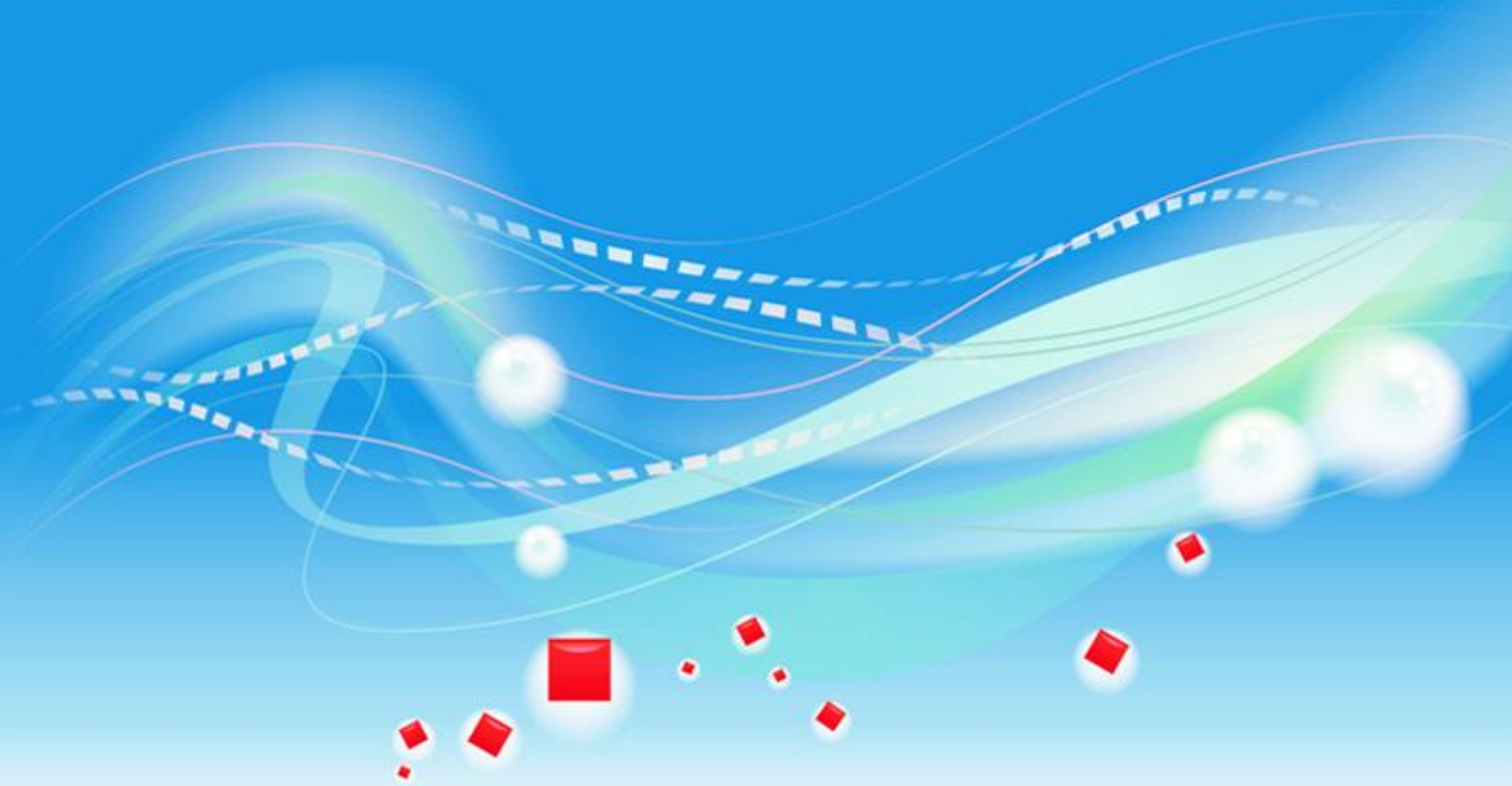


ViPNet Client Монитор 3.2

Руководство пользователя

ViPNet
Virtual Private Network
infotecs

ФРКЕ.00004-05 34 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

Для кого предназначен документ

Данное руководство предназначено для пользователей программного обеспечения ViPNet Client. В нем содержится информация о назначении и составе ПО ViPNet Client, а также рекомендации по настройке и использованию возможностей программы ViPNet Монитор.

Предполагается, что читатель данного руководства имеет общее представление о сетевых технологиях, IP-протоколах, межсетевых экранах и информационной безопасности.

Соглашения документа

Соглашения данного документа представлены в таблице ниже.

Таблица 1. Условные обозначения

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

О программе

Назначение ПО ViPNet Client

Программное обеспечение ViPNet Client входит в состав пакетов ViPNet CUSTOM и ViPNet OFFICE. ViPNet Client выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях.

Программное обеспечение ViPNet Client может быть установлено для защиты трафика на любом компьютере с ОС Windows, будь то стационарный, удаленный, мобильный компьютер или сервер.

Состав ПО ViPNet Client

Программное обеспечение ViPNet Client состоит из следующих компонентов:

- Низкоуровневый драйвер сетевой защиты ViPNet-драйвер.
- Программа ViPNet Монитор.
- Транспортный модуль ViPNet MFTP.
- Программа ViPNet Контроль приложений.
- Программа ViPNet Деловая почта.

ViPNet-драйвер

ViPNet-драйвер (см. «Принцип работы ViPNet-драйвера» на стр. 15) взаимодействует непосредственно с драйверами сетевых интерфейсов компьютера (реальных или их эмулирующих), что обеспечивает независимость программы от операционной системы и недокументированных возможностей в ней. ViPNet-драйвер перехватывает и контролирует весь IP-трафик, поступающий и исходящий из 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 адаптеров 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

Программа ViPNet Монитор предназначена для настройки различных параметров ViPNet-драйвера (см. «Принцип работы ViPNet-драйвера» на стр. 15) и записи событий, возникающих в процессе работы драйвера, в журнал регистрации IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 210). 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:

- Выполняет функции персонального сетевого экрана (см. «Интегрированный сетевой экран» на стр. 122).
- Шифрует IP-трафик компьютера.
- Позволяет управлять параметрами обработки прикладных протоколов.
- Предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена и так далее.

ViPNet MFTP

На абонентском пункте (см. «Абонентский пункт (АП)») транспортный модуль ViPNet MFTP обеспечивает обмен управляющими конвертами, конвертами программы «Деловая почта» и файлами с другими сетевыми узлами ViPNet. Подробнее о программе см. документ «ViPNet MFTP. Руководство администратора».

ViPNet Контроль приложений

Программа «Контроль приложений» является необязательным модулем программного обеспечения ViPNet Client. Чтобы иметь возможность контролировать сетевую

активность приложений на каждом компьютере, необходима специальная лицензионная запись в регистрационном файле на ПО ViPNet.

Программа «Контроль приложений» позволяет:

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

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

ViPNet Деловая почта

«Деловая почта» — это программа в составе ПО ViPNet Client, предназначенная для обмена электронной почтой между пользователями сети ViPNet. С помощью программы «Деловая почта» можно отправлять и получать сообщения с вложенными файлами, шифровать сообщения и вложения, подписывать сообщения и вложения электронной подписью. В программе предусмотрена система автоматической обработки входящих сообщений и файлов в соответствии с заданными правилами (автопроцессинг).

Подробная информация о программе «Деловая почта» содержится в документе «ViPNet Деловая почта. Руководство пользователя».

Принцип работы ViPNet-драйвера

Ядром программного обеспечения ViPNet является так называемый ViPNet-драйвер, основной функцией которого является фильтрация и шифрование/дешифрование входящих и исходящих IP-пакетов.

Каждый исходящий пакет обрабатывается ViPNet-драйвером в соответствии с одним из следующих правил:

- переадресуется или отправляется в исходном виде (без шифрования);
- блокируется;
- шифруется и отправляется;
- шифруется и переадресуется.

Каждый входящий пакет обрабатывается следующим образом:

- пропускается (если он не зашифрован и это разрешено правилами фильтрации для нешифрованного трафика);
- блокируется (в соответствии с установленными правилами фильтрации);
- расшифровывается (если пакет был зашифрован) и перенаправляется для дальнейшей обработки соответствующим приложением.

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 1: 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.

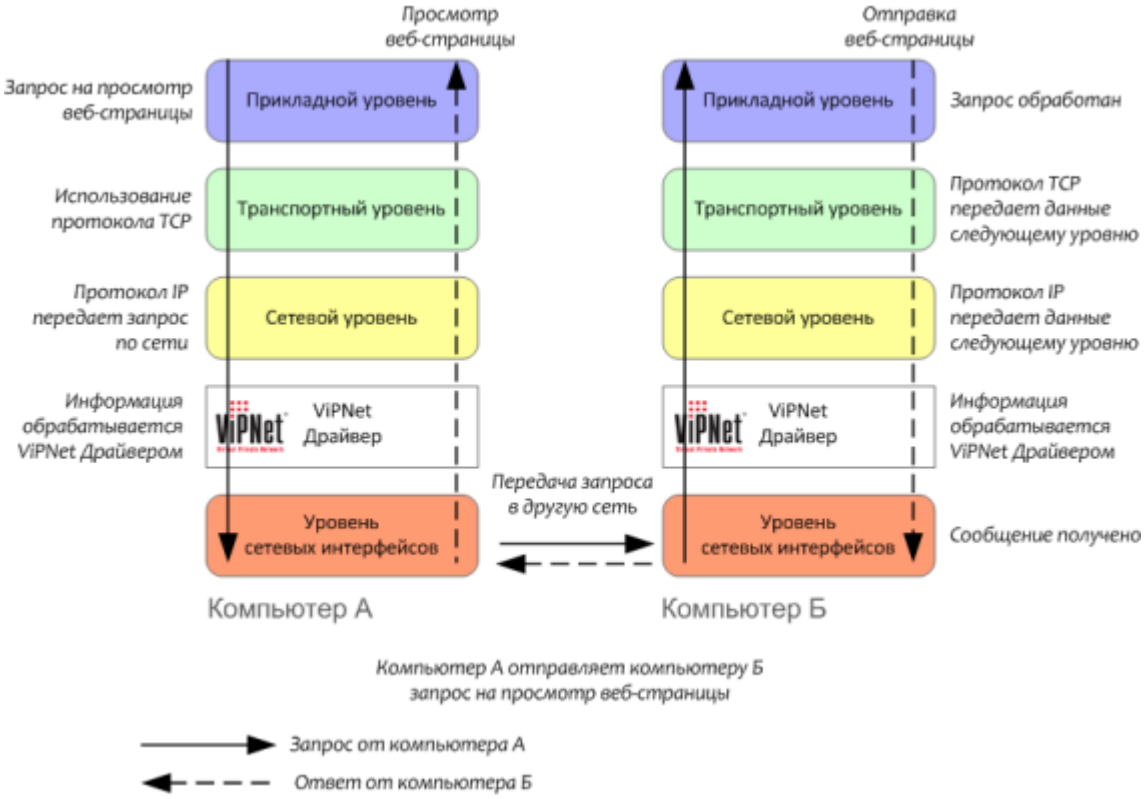


Рисунок 2: Схема работы сети TCP/IP, защищенной ПО ViPNet

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.

Новые возможности

Данный раздел описывает новые функциональные возможности программного обеспечения ViPNet Client.

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.

- **Увеличение количества обрабатываемых программой прикладных протоколов**

  Расширен список прикладных протоколов, для которых в программе ViPNet Монитор реализована специальная обработка IP-пакетов.

- **Интеграция ПО ViPNet Client с ПО ViPNet SafeDisk-V**

  Благодаря интеграции обеспечена дополнительная защита конфиденциальной информации, хранящейся в контейнерах ViPNet SafeDisk-V. Теперь доступ к контейнерам в программе ViPNet SafeDisk-V определяется текущей конфигурацией ViPNet Монитор — защищенной или незащищенной.

- **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.

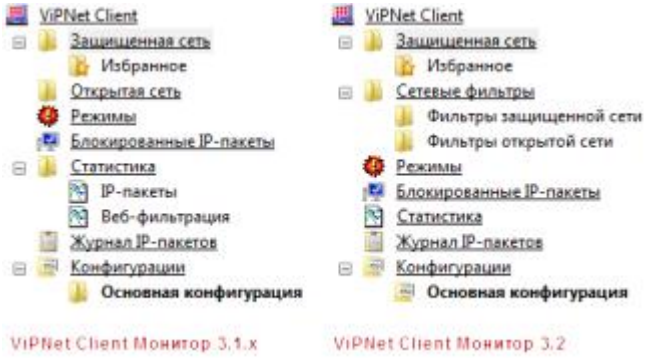


Рисунок 3: Отображение фильтров на панели навигации главного окна в ПО ViPNet Client Монитор версий 3.1.x и 3.2

Приведена к единому виду структура фильтров защищенной и открытой сети, а также набор возможных действий с фильтрами.

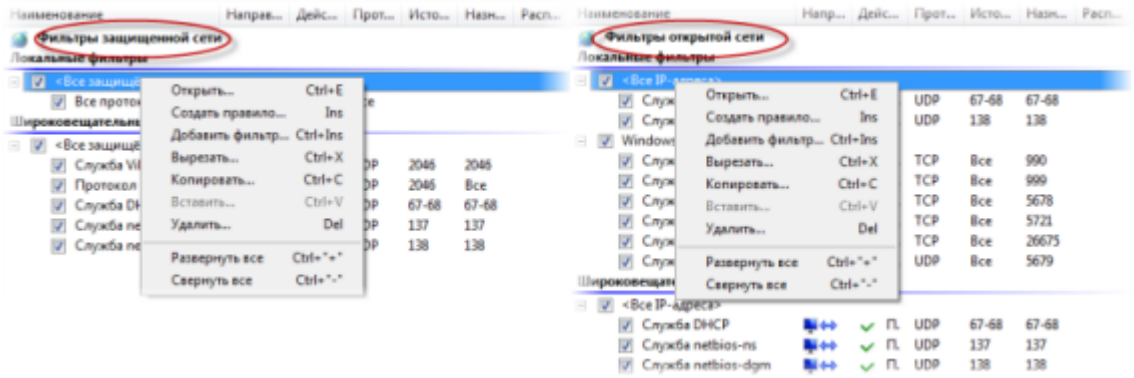


Рисунок 4: Отображение фильтров защищенной и открытой сетей в ПО ViPNet Монитор 3.2 и возможные действия с этими фильтрами

- **Автоматический вход в ПО ViPNet Client**

  Реализована возможность входа в программу без необходимости подтверждения пароля пользователя ViPNet в окне входа в программу (см. Рисунок 33 на стр. 71). Управление данной функцией возможно только в режиме администратора в окне **Настройка параметров безопасности** на вкладке **Администратор** (см. «Дополнительные настройки параметров безопасности» на стр. 256). 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 Client выполняется автоматически.

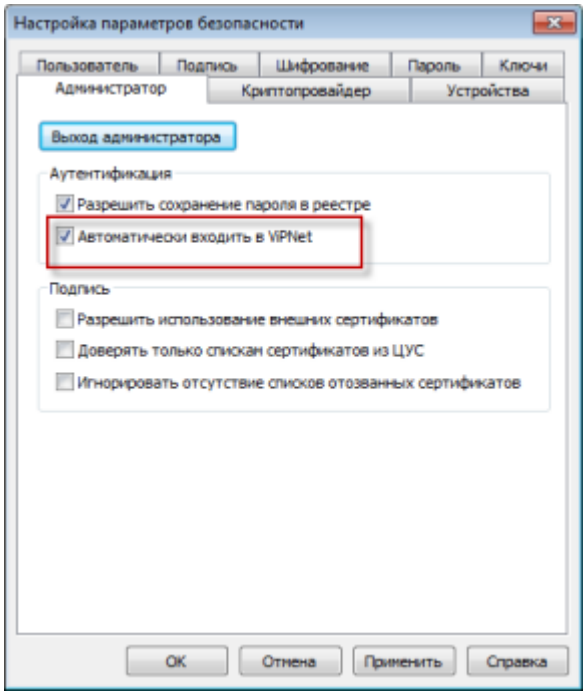


Рисунок 5: Настройка автоматического входа в ПО ViPNet Client

- **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. 356).

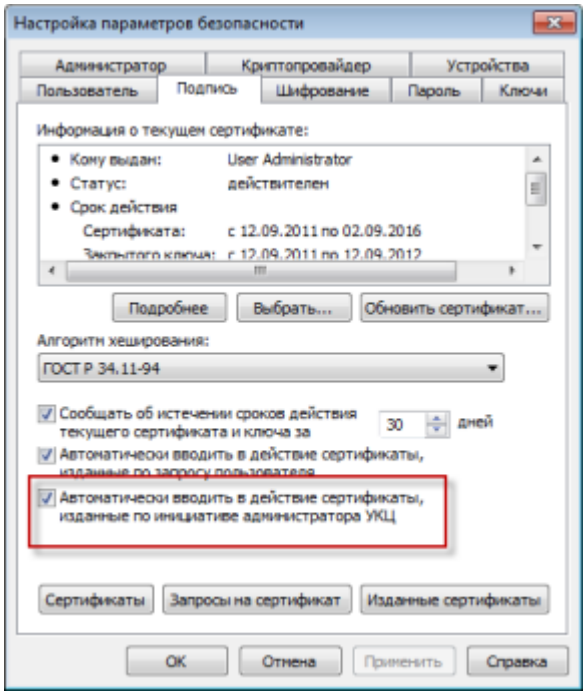


Рисунок 6: Новый элемент вкладки «Подпись» окна «Настройка параметров безопасности»

- **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 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.

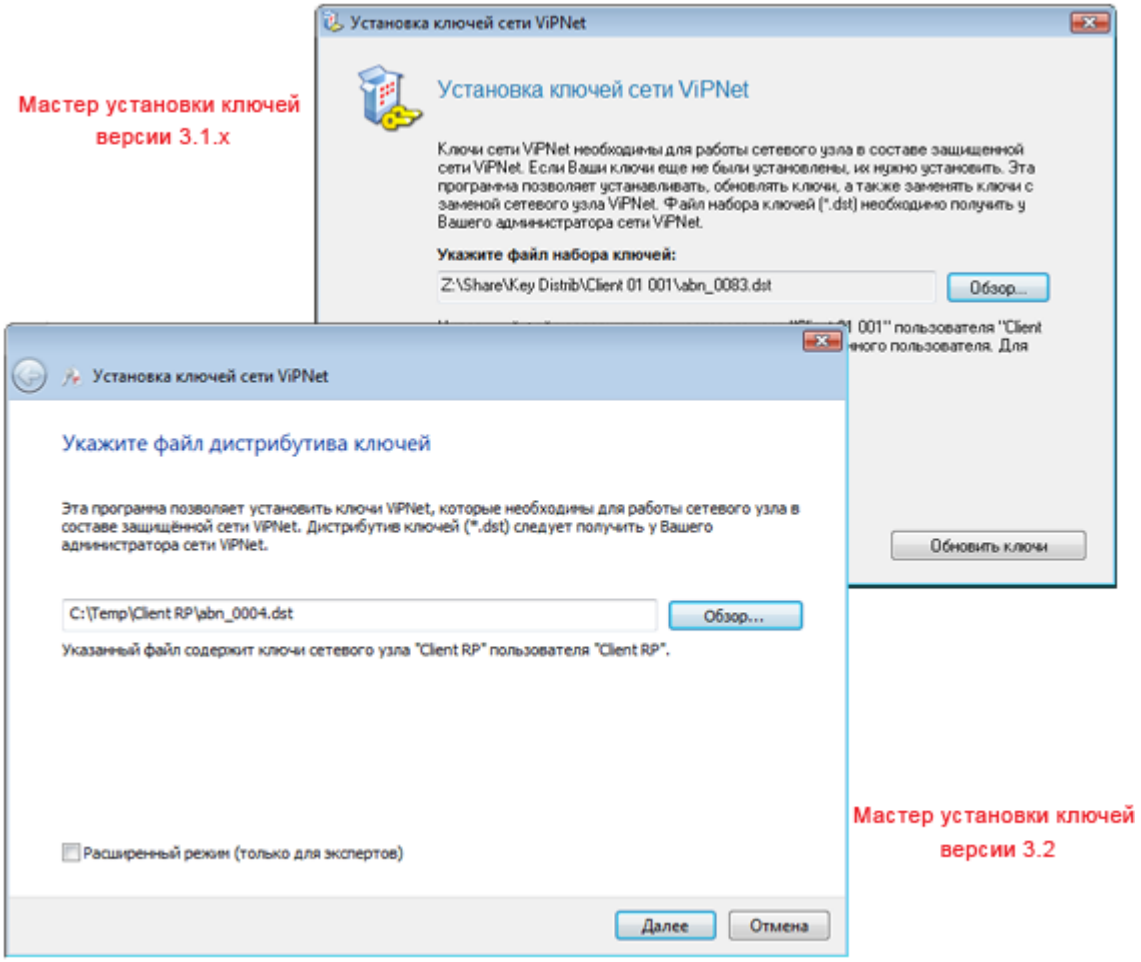


Рисунок 7: Новый мастер установки ключей ViPNet

- **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 MS 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».

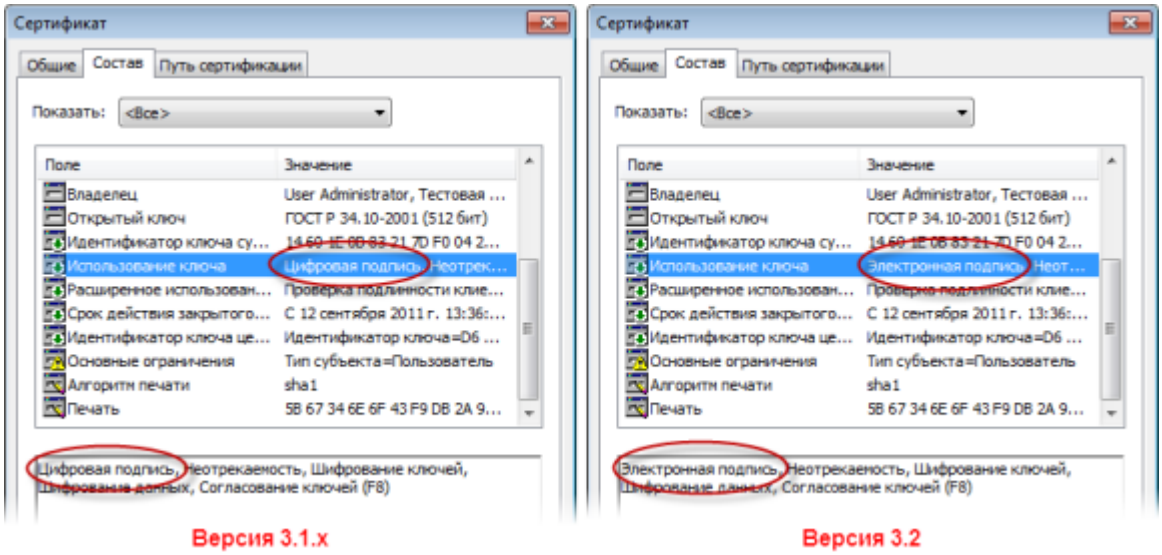


Рисунок 8: Изменение термина «цифровая подпись» на примере окна «Сертификат»

Прочие изменения терминологии приведены в таблице ниже:

Что изменено	До изменения, в версиях 3.1.x	В результате изменения, в версии 3.2
Название окна	**Правило доступа** (окно, вызываемое из раздела **Защищенная сеть**)	**Свойства узла**

Что изменено	До изменения, в версиях 3.1.x	В результате изменения, в версии 3.2
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

- **Обновление документации и справки**

  Документация и справка, поставляемые вместе с ПО ViPNet Client, были существенно обновлены, для того чтобы отразить 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».

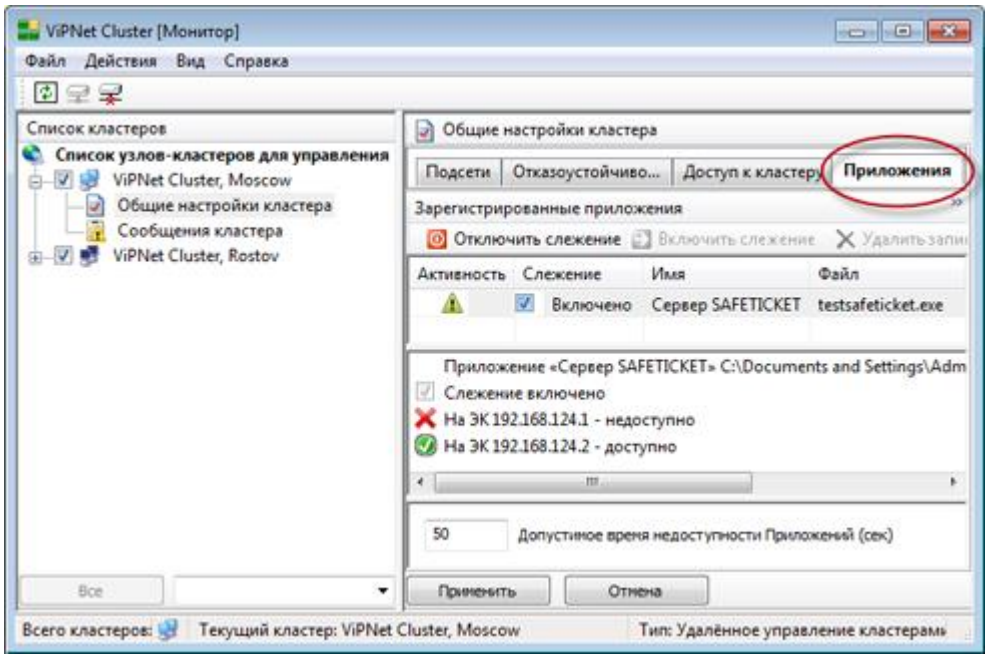


Рисунок 9: Настройка параметров контроля приложений в ViPNet Cluster Монитор

- **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.

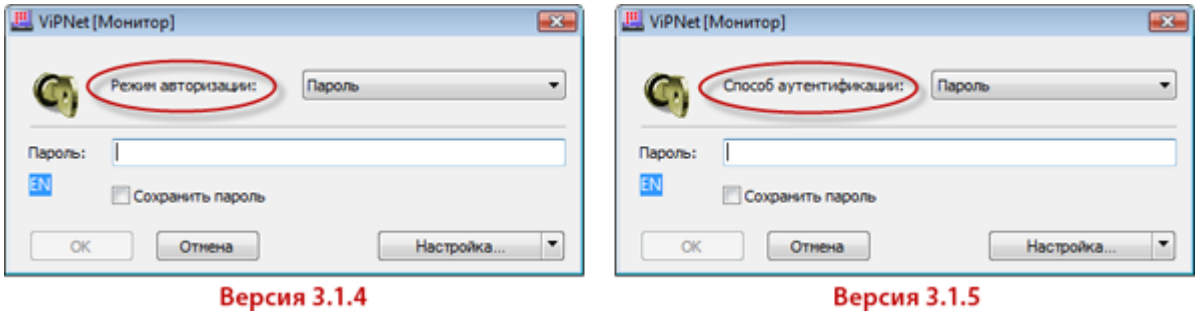


Рисунок 10: Измененный интерфейс окна ввода пароля

В соответствии с заменой терминов обновлена документация и справка по всем продуктам.

- **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 (см. «Особенности блокировки компьютера при использовании внешнего устройства для аутентификации пользователя» на стр. 208).

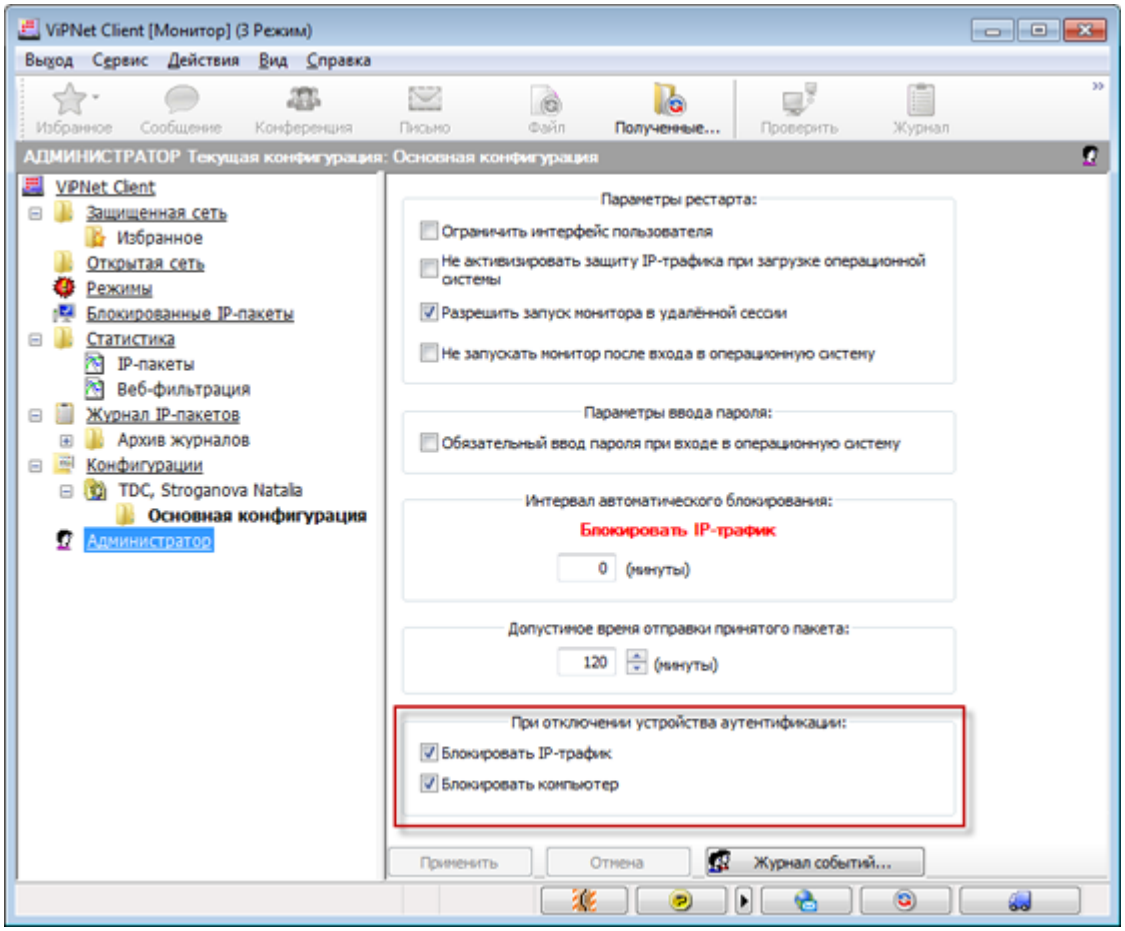


Рисунок 11: Настройка блокировки при отключении устройства аутентификации

- **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 «Деловая почта»**

Изменен принцип отображения числа элементов в папках программы «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 «Деловая почта»**

  Реализовано сохранение позиции последнего выбранного элемента при переходе между папками программы «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 «Деловая почта»**

  Изменена логика при открытии окна поиска в программе «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 «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.

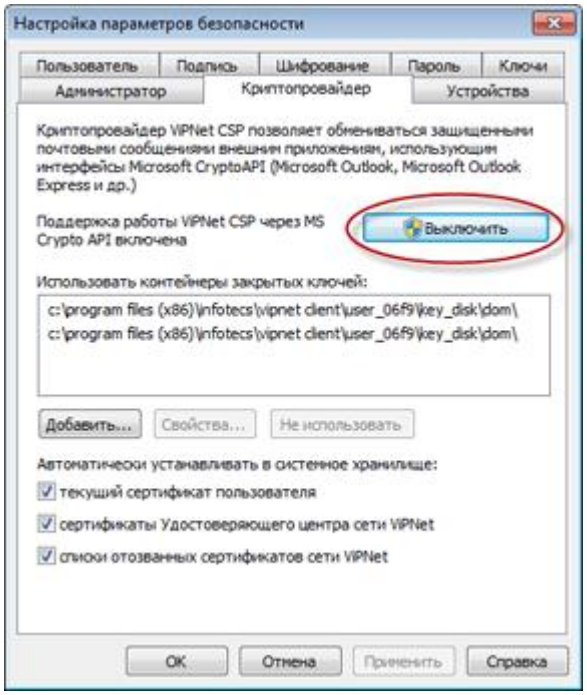


Рисунок 12: Кнопка включения и отключения криптопровайдера

- **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 «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**.

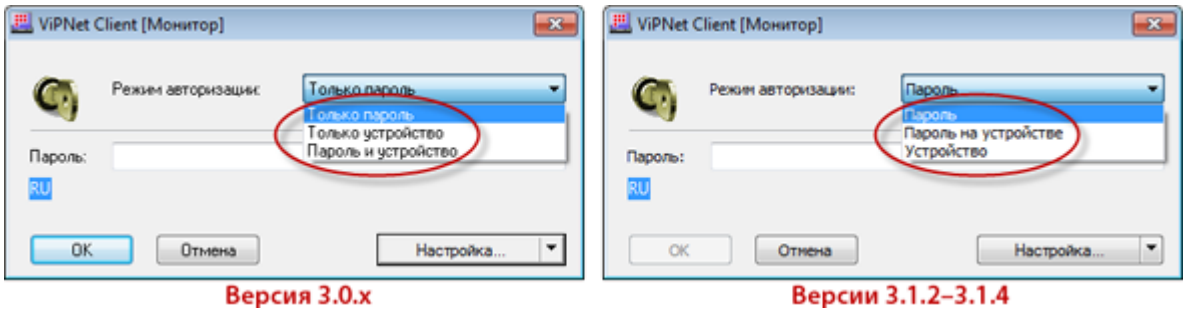


Рисунок 13: Изменение типов авторизации

- **Оптимальное расположение различных настроек**

  Настройки, находившиеся на панели навигации, удалены с неё и объединены с другими настройками.

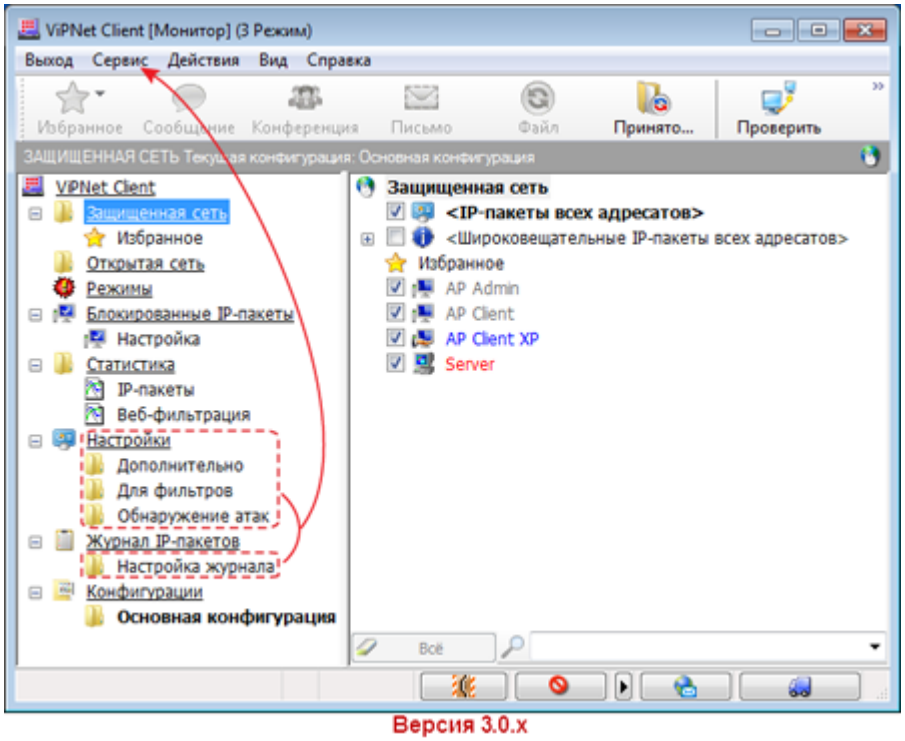


Рисунок 14: Изменение местоположения настроек защищенной сети

Теперь все настройки содержатся в одном окне, которое вызывается по команде **Сервис > Настройки**.

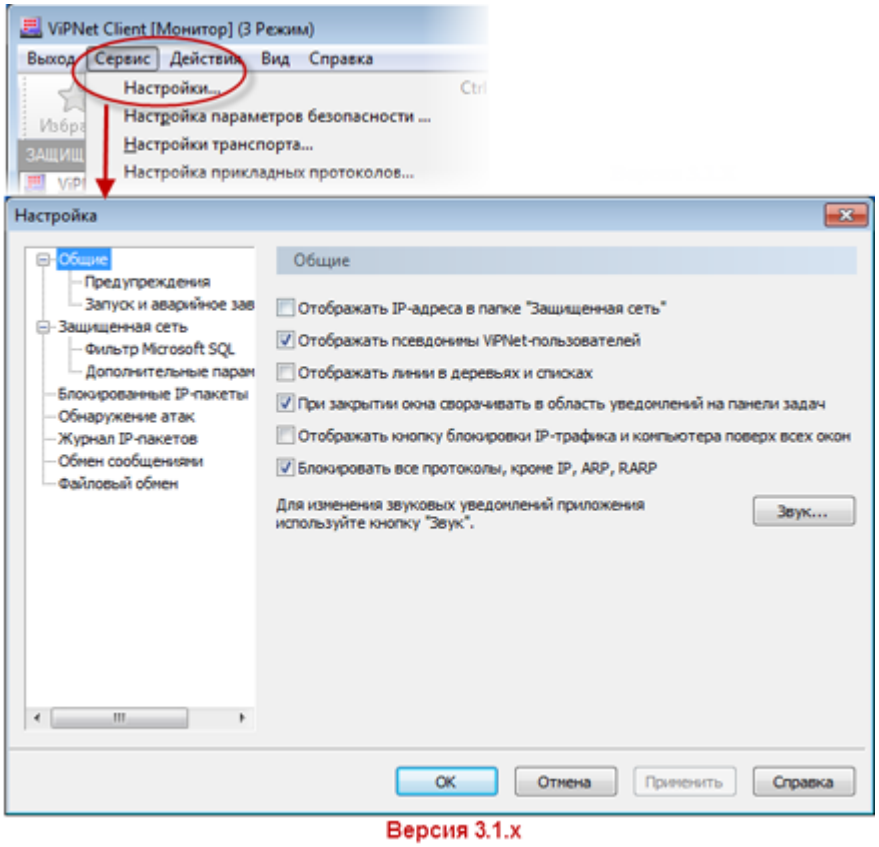


Рисунок 15: Настройки защищенной сети в новой версии

- **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.

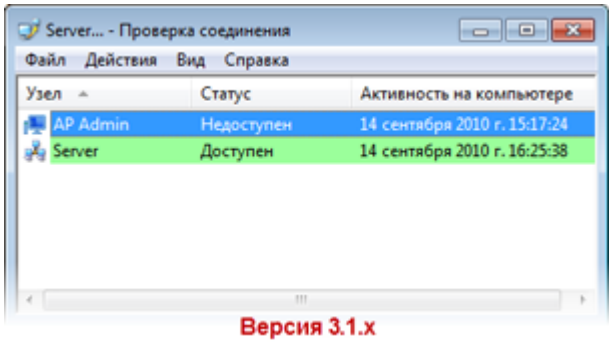


Рисунок 16: Проверка соединения с несколькими узлами сети

- **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 17: Процесс файлового обмена

Теперь отправка файлов осуществляется сразу после выбора получателя (сетевого узла).

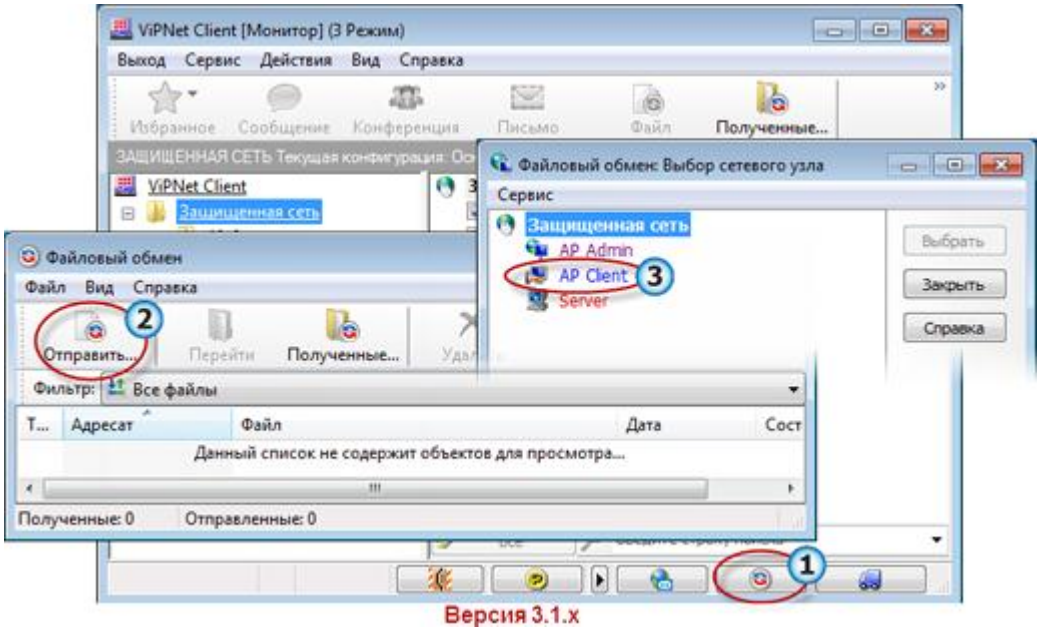


Рисунок 18: Измененный процесс файлового обмена

- **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 адаптеров. 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. «Регистрация защищенного DNS-сервера средствами ПО ViPNet» на стр. 173). Теперь достаточно внести информацию о серверах в специальный файл, и их IP-адреса автоматически будут добавлены в настройки сетевых адаптеров. 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.

Системные требования

Требования к компьютеру для установки программы ViPNet Client:

- Процессор — Pentium IV. Рекомендуется Intel Core 2 Duo E6400 или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 512 Мбайт (рекомендуется 1 Гбайт).
- Свободное место на жестком диске — не менее 150 Мбайт (рекомендуется 250 Мбайт).
- Сетевой адаптер или модем.
- Операционная система — Windows XP SP3 (32-разрядная)/Server 2003 (32-разрядная)/ Vista SP2 (32/64-разрядная)/Server 2008 (32/64-разрядная)/Windows 7 (32/64-разрядная)/Server 2008 R2 (64-разрядная).
- При использовании Internet Explorer — версия 6.0 или выше.

Примечание. На компьютере не должны быть установлены другие сетевые экраны (также называемые брандмауэрами).

Совместимость приложений ViPNet с другими приложениями

Приложения, совместимые с ПО ViPNet

Обеспечена совместимость программного обеспечения ViPNet со следующими приложениями:

- Lumension Device Control (ранее Sanctuary Device Control).
- Cisco Security Agent.
- Kaspersky Administration Kit.
- Microsoft SQL Server 2000 Desktop Engine (MSDE 2000).

Совместное использование ПО ViPNet и КриптоПро CSP

Обеспечение совместимости ПО ViPNet и КриптоПро CSP

В состав программного обеспечения ViPNet Client входит криптопровайдер ViPNet CSP, предназначенный для выполнения криптографических операций.

При установке на один компьютер криптопровайдеров ViPNet и КриптоПро CSP (независимо от порядка установки) сохранится следующая работоспособность:

- Функциональность ПО ViPNet в рамках VPN.
- Криптопровайдер КриптоПро CSP.

Примечание. При установке программ ViPNet и ПО КриптоПро CSP будет работать только криптопровайдер КриптоПро CSP, но сохранится функциональность клиентского ПО ViPNet (Монитор, шифрование трафика), в котором операции шифрования выполняет драйвер ViPNet. Отсутствие конфликтов обусловлено тем, что драйвер ViPNet шифрует информацию на сетевом уровне, а КриптоПро CSP на прикладном.

Замена криптопровайдера ViPNet на КриптоПро CSP

Поскольку ПО ViPNet, установленное на одном компьютере с КриптоПро CSP, не нарушает его структуру и работоспособность, то возможна прозрачная замена криптопровайдера ViPNet на КриптоПро CSP простой установкой последнего.

Системные ограничения не позволяют одновременную работу двух и более криптопровайдеров, даже если они установлены на одном компьютере. Поэтому, чтобы использовать ПО ViPNet совместно с КриптоПро CSP, следует отключить криптопровайдер ViPNet. Для этого в главном окне программы ViPNet Monitor, в меню **Сервис**, выберите **Настройка параметров безопасности**, перейдите на вкладку **Криптопровайдер** и нажмите кнопку **Выключить.**

Чтобы восстановить функциональность криптопровайдера ViPNet, удалите программное обеспечение КриптоПро CSP и нажмите кнопку **Включить.**

Использование сертификатов ViPNet в ПО КриптоПро CSP и сертификатов КриптоПро в ПО ViPNet

Сертификаты пользователей, сформированные в удостоверяющем центре (УЦ) КриптоПро по запросу из ПО ViPNet CSP, могут использоваться для подписи в ПО ViPNet. Аналогично сертификаты, сформированные в ViPNet Administrator УКЦ по запросу из ПО КриптоПро CSP, могут использоваться в ПО КриптоПро CSP.

Примечание. Ключи, сформированные в ПО ViPNet Administrator УКЦ по запросу из ПО ViPNet, не могут преобразовываться и использоваться ПО КриптоПро CSP.

В программе ViPNet Manager обработка внешних запросов на сертификаты невозможна.

Совместное использование 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 Iplirim Driver, то есть сетевой ViPNet-драйвер. 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 драйвер Iplirim.

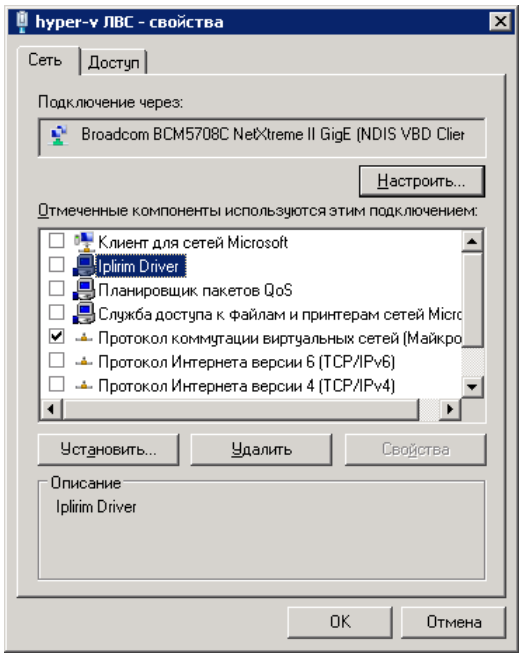


Рисунок 19: Настройки физического интерфейса, подключенного к виртуальной сети Hyper-V

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» на стр. 140), разрешающий входящие и исходящие соединения по следующим портам TCP: 17484, 17485, 17486, 17487.

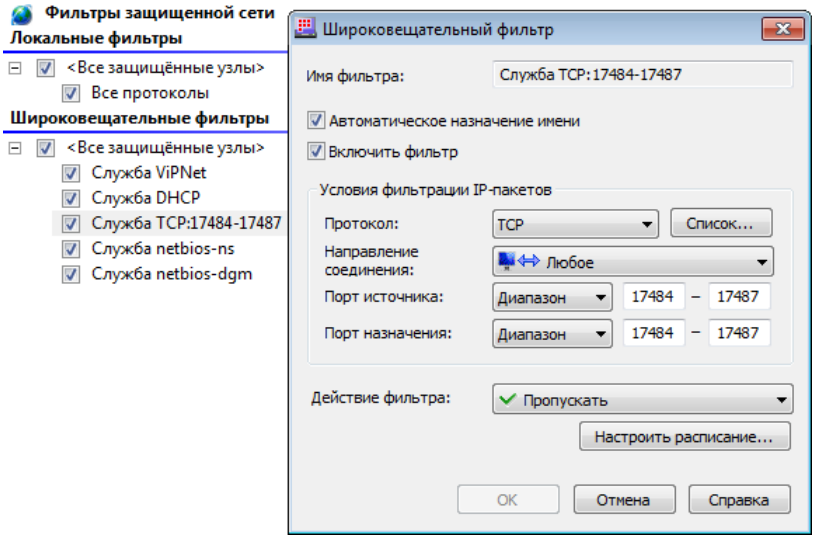


Рисунок 20: Широковещательный фильтр защищенной сети

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**.

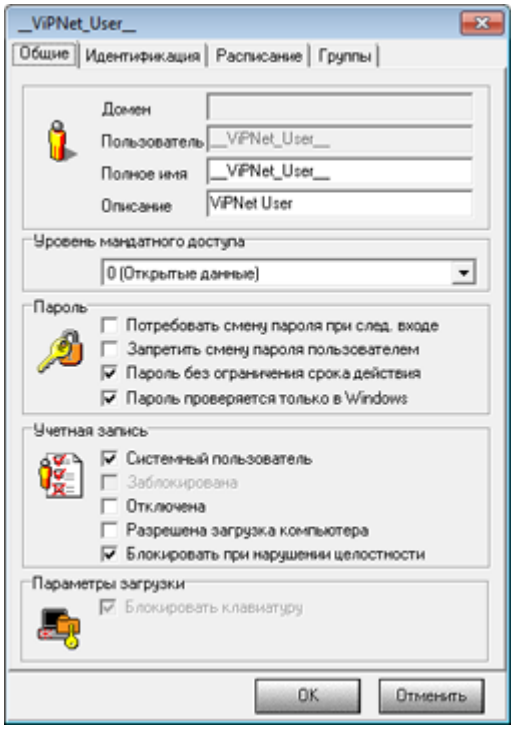


Рисунок 21: Свойства пользователя Dallas Lock

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**.

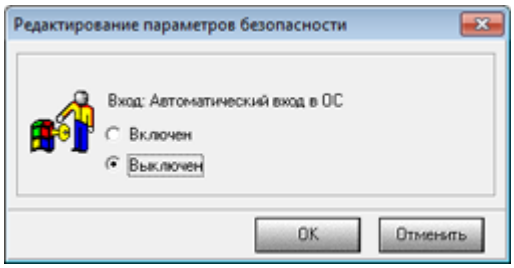


Рисунок 22: Политика «Автоматический вход в систему»

4 Настройте мандатный доступ с мандатом 0 на папку установки программы ViPNet Client. В список **Программы имеющие доступ на запись** добавьте следующие исполняемые файлы:

- Все исполняемые файлы из папки установки программы ViPNet Client.
- `c:\windows\explorer.exe`.
- `c:\windows\system32\dllhost.exe`.
- `c:\windows\system32\svchost.exe`.

- c:\windows\system32\wbem\wmiprvse.exe.

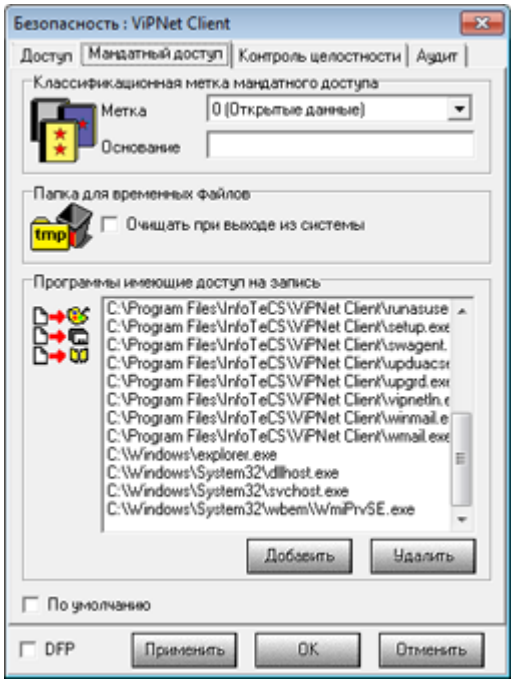


Рисунок 23: Настройка мандатного доступа

5 Настройте мандатный доступ с мандатом 0 на папку пользователя Windows, от имени которого будет запускаться ПО ViPNet: `C:\Documents and Settings\<имя пользователя>\`.

В список **Программы имеющие доступ на запись** добавьте следующие исполняемые файлы:

- `C:\Windows\explorer.exe`.
- `C:\Program Files\InfoTeCS\ViPNet Client\Monitor.exe`.
- `C:\Program Files\InfoTeCS\ViPNet Client\wmail.exe`.

6 Настройте мандатный доступ с мандатом 0 на папку временных файлов пользователя: по умолчанию `C:\Documents and Settings\<имя пользователя>\Local Settings\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 Client\Monitor.exe`.
- `C:\Program Files\InfoTeCS\ViPNet Client\wmail.exe`.

- C:\Windows\System32\rundll.exe.

8 После выполнения указанных настроек программы ViPNet Монитор и Dallas Lock готовы к совместной работе.

Информация о внешних устройствах хранения данных

В ПО ViPNet для записи и считывания персональной информации (паролей, ключей и так далее) имеется возможность использовать различные внешние устройства хранения данных.

Внимание! Хранение ключей нескольких пользователей на одном устройстве невозможно. Однако возможно хранение ключей подписи нескольких пользователей на одном устройстве.

Перед записью ключей на устройство убедитесь, что устройство отформатировано.

Ниже в таблице перечислены устройства и ключи, с которыми может работать ПО ViPNet. Приведенная таблица содержит следующие данные:

- в столбце **Тип устройства** представлены все типы устройств считывания, доступные для выбора в ПО ViPNet;
- в столбце **Тип ключа** представлены типы ключей, используемые для данных устройств;
- в столбце **Необходимые условия работы с ключом** описаны необходимые условия и важные моменты для использования каждого ключа;
- в последнем столбце содержится 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 2. Поддерживаемые внешние устройства

Тип устройства	Тип ключа	Необходимые условия работы с ключом	Поддержка стандарта PKCS#11
eToken Aladdin	**eToken PRO** (персональные электронные ключи, eToken PRO (Java), eToken PRO, смарт-карты eToken PRO (Java), eToken PRO компании «Аладдин Р.Д.»)	• На компьютере должно быть установлено программное обеспечение PKI Client версии 5.1 и выше. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2. • **Замечание:** Смарт-карта eToken PRO может использоваться с любым стандартным PC/SC совместимым USB-устройством считывания с карт.	Да
iButton	**iButton (Dallas)** (электронные ключи iButton типа DS1993, DS1994, DS1995 и DS1996)	• К компьютеру должно быть подключено устройство считывания. • На компьютере должно быть установлено программное обеспечение обмена информации с iButton, 1-Wire Drivers версии 3.6.2. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32-разрядная), Server 2008 (32-разрядная), Windows 7 (32-разрядная).	Нет
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. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная).	Нет
SmartCard RIK	**Российская интеллектуальная**	• Работа с картой ПО ViPNet может производиться через любой PS\CS-	Нет

Тип устройства	Тип ключа	Необходимые условия работы с ключом	Поддержка стандарта PKCS#11
	карта компании «Атлас-Телеком»	совместимый считыватель.	
Shipka	**ПСКЗИ ШИПКА** компании ОКБ САПР	• Перед началом работы с устройством ШИПКА убедитесь, что на АП установлено программное обеспечение ACShipka Environment версии не ниже 3.3.2.6. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная). Проведите инициализацию устройства при помощи утилиты производителя «Параметры авторизации».	Да
ruToken	**Rutoken S**, электронный идентификатор компании «Актив»	• На компьютере должны быть установлены драйверы Rutoken версий не ниже используемых в установочном комплекте версии 2.81.00.0424. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная).	Да
ruTokenECP	**Rutoken ЭЦП**, электронный идентификатор компании «Актив»	• На компьютере должны быть установлены драйверы версии не ниже 2.81.00.0424. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная).	Да
Аккорд-5MX	iButton типа DS1993, DS1994, DS1995 и DS1996	• На компьютере должен быть установлен драйвер версии не ниже 3.18.0.0. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32-разрядная),	Нет

Тип устройства	Тип ключа	Необходимые условия работы с ключом	Поддержка стандарта PKCS#11
		Server 2008 (32-разрядная).	
Siemens CardOS	**Смарт-карты Siemens** (CardOS/M4.01a, CardOS V4.3B, CardOS V4.2B, CardOS V4.2B DI, CardOS V4.2C, CardOS V4.4)	• Для работы на компьютере должно быть установлено ПО Siemens CardOS API V5.0 или выше • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 EE SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 SP2 (32/64-разрядная), Windows 7 (32/64-разрядная).	Да
Mifare	**Rosan Mifare**	• Для работы с устройством необходимо наличие COM-порта. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная).	Нет
Mifare Standard4K	**Mifare 4K**	• Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная). • Для работы с устройством используется интерфейс подключения USB 2.0 (совместимый с USB 1.1). • Карта Mifare 4K поддерживается только через считыватель ACR128.	Нет
eToken ГОСТ (не поддерживается ПО ViPNet Удостоверяющий и ключевой центр)	**eToken ГОСТ Aladdin**	• Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista (32-разрядная), Windows 7 (32/64-разрядная). • **Примечание**: устройство поддерживает ГОСТ 34.10-2001.	Да

Тип устройства	Тип ключа	Необходимые условия работы с ключом	Поддержка стандарта PKCS#11
JCDS	Смарт-карты Gemalto Optelio Contactless D72, KONA 131 72K	• На карту должен быть загружен апплет, позволяющий модулю jcpkcs11ds.dll компании «Аладдин Р.Д.» работать с картой. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2.	Да
JaCarta	Персональные электронные ключи JaCarta компании «Аладдин Р.Д.»	• На компьютере должно быть установлено программное обеспечение JC-Client компании «Аладдин Р.Д.». • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 SP2 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная), Server 2008 R2.	Да
Kaztoken	Персональные электронные ключи Kaztoken	• На компьютере должны быть установлены драйверы Kaztoken версии не ниже 2.53.00.0365. • Поддерживаемые ОС: Windows XP SP3 (32-разрядная), Server 2003 (32-разрядная), Vista SP2 (32/64-разрядная), Server 2008 (32/64-разрядная), Windows 7 (32/64-разрядная).	Да

Комплект поставки

Комплект поставки ViPNet Client включает:

- Установочный файл setup.exe.
- При поставке в составе программного комплекса ViPNet CUSTOM включена документация в формате PDF, в том числе:
  - «ViPNet Client Монитор. Руководство пользователя».
  - «ViPNet Деловая почта. Руководство пользователя».
  - «ViPNet MFTP. Руководство администратора».
  - «ViPNet Контроль приложений. Руководство пользователя».
  - «Классификация полномочий. Приложение к документации ViPNet CUSTOM».
  - «Основные термины и определения. Приложение к документации ViPNet CUSTOM».
  - «Развертывание сети ViPNet. Руководство администратора».
  - «Новые возможности ViPNet Client и ViPNet Coordinator версии 3.2. Приложение к документации ViPNet».

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте компании «ИнфоТеКС». По предложенным ссылкам можно найти ответы на многие вопросы, возникающие в процессе эксплуатации продуктов ViPNet.

- 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 компании «ИнфоТеКС». Для решения возникающих проблем обратитесь в службу технической поддержки.

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

Начало работы с программой ViPNet Client

Установка и удаление программы

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

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

Внимание! Если ViPNet Client устанавливается на компьютер с операционной системой Windows, локализация которой отличается от русской, для правильного отображения кириллицы в интерфейсе ViPNet Client нужно изменить региональные настройки Windows (см. «Региональные настройки» на стр. 59).

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

Для установки ViPNet Client требуются:

- Файл установки `setup.exe`.
- Дистрибутив ключей для сетевого узла (файл *`.dst`).
- Пароль пользователя сетевого узла или внешнее устройство аутентификации (см. «Информация о внешних устройствах хранения данных» на стр. 45).

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

Для установки ПО ViPNet Client выполните следующие действия:

1. Двойным щелчком запустите программу установки setup.exe  , будет запущен мастер установки ViPNet Client.
2. Следуйте указаниям мастера установки.

3 По завершении установки перезагрузите компьютер.

Примечание. ViPNet Client можно установить в неинтерактивном режиме (см. «Неинтерактивный режим установки» на стр. 55). В этом случае процесс установки не будет отображаться на экране.

Если на компьютере установлено несколько программ ViPNet, и в одной из этих программ уже были установлены ключи данного сетевого узла, в программе ViPNet Client требуется указать путь к транспортному каталогу, содержащему справочно-ключевую информацию (см. «Смена транспортного каталога» на стр. 58).

Внимание! Нельзя производить повторную инициализацию справочно-ключевой информации сетевого узла в другую папку, поскольку это может привести к ошибкам в работе программного обеспечения.

Если справочно-ключевая информация еще не установлена на компьютере, выполните следующие действия:

1 Запустите программу ViPNet Client из меню **Пуск** или дважды щелкните значок  на рабочем столе (этот значок отображается, только если при установке программы была выбрана соответствующая опция).

2 В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и в меню выберите пункт **Первичная Инициализация**.

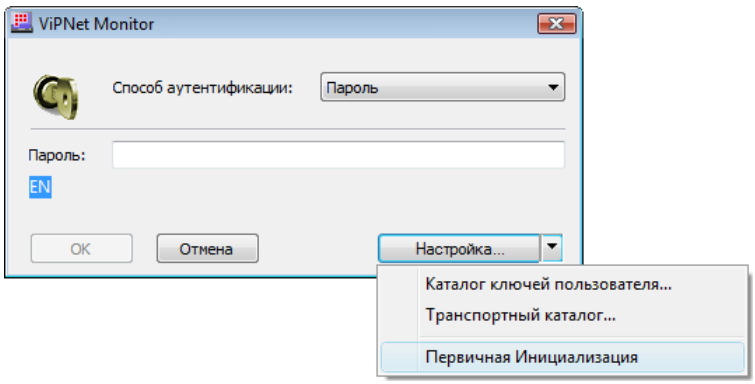


Рисунок 24: Запуск первичной инициализации

3 Следуя указаниям мастера, выполните установку справочников ключей с помощью файла `*.dst`, полученного от администратора сети ViPNet.

Неинтерактивный режим установки

При установке программы ViPNet Client в неинтерактивном режиме процесс установки не отображается на экране компьютера. Параметры установки не запрашиваются у пользователя, а считываются из специального файла `silent.ini`.

В секциях файла `silent.ini` можно указать следующие параметры:

Таблица 3. Параметры файла silent.ini

Секция	Описание
`[version]` `signature="$CHICAGO$"`	Данную секцию необходимо оставить без изменения

`[Components]`
`setup.inf`
`iplir.inf`
`winmail.inf`
`ss.inf`
	В данной секции указываются устанавливаемые компоненты ПО ViPNet Client.
	Для полной установки ПО ViPNet Client нужно указать все четыре параметра.
	Чтобы установить программу ViPNet Монитор, но не устанавливать ViPNet Деловая почта, нужно опустить параметр `winmail.inf`.
	Чтобы установить программу ViPNet Деловая почта, но не устанавливать ViPNet Монитор, нужно опустить параметр `iplir.inf`.

`[Install]` `desktop=1`	Параметр `desktop` указывает, нужно ли создавать ярлык на Рабочем столе. Если `desktop=1`, ярлык создается. Если `desktop=0`, ярлык не создается.

Примечание. По умолчанию используются значения параметров, приведенные в таблице.

Чтобы запустить установку ViPNet Client в неинтерактивном режиме, в командной строке Windows нужно выполнить команду:

```
setup.exe -a silent.ini
```

При запуске установки можно указать дополнительные параметры:

- `/norf` — отказ от установки программы «Контроль приложений».

Примечание. Если лицензия на ПО ViPNet не разрешает установку «Контроля приложений», эта программа не устанавливается в любом случае.

- `/forcereboot` — принудительная перезагрузка компьютера по окончании установки.

  Пример команды с параметрами: `setup.exe /norf -a silent.ini`

В неинтерактивном режиме ПО ViPNet Client устанавливается в папку:

- `C:\Program Files\InfoTeCS\ViPNet Client`, если ПО ViPNet Client устанавливается на данный компьютер впервые.
- Текущую папку установки, если ПО ViPNet Client уже было установлено на компьютере.

Проведение повторной инициализации после сбоя программы

Внимание! Крайне не рекомендуется проводить повторную инициализацию, поскольку в этом случае не гарантируется сохранность пользовательских данных, сформированных в программах ViPNet (письма программы «Деловая почта» и защищенные сообщения, файлы, переданные по файловому обмену, и так далее).

Повторная инициализация возможна, если после программного или системного сбоя пользователь не может войти в программу ViPNet (например, выдается сообщение о том, что введенный пароль неверен), и при этом нет возможности восстановить справочно-ключевую информацию из резервной копии (см. «Резервное копирование и восстановление ключей» на стр. 282).

Разрешение на проведение повторной инициализации следует получить у администратора сети ViPNet.

Потеря пользовательских данных при повторной инициализации возможна, если с момента первичной инициализации до момента сбоя имели место следующие события:

- компрометация ключей пользователя сетевого узла;
- смена мастер-ключа в сети ViPNet.

Если перечисленные события имели место, то повторная инициализация вернет узел пользователя к тому состоянию, которое было после первичной инициализации. Письма программы «Деловая почта», защищенные сообщения и другие пользовательские данные, сформированные в программах ViPNet, будут потеряны. Если перечисленных выше событий не происходило, то повторная инициализация будет выполнена как обновление справочно-ключевой информации (см. «Обновление справочников и ключей» на стр. 276), и пользовательские данные сохранятся.

В ряде случаев при проведении повторной инициализации существующая ключевая информация не может быть обновлена на ту информацию, которая содержится в новом файле дистрибутива. Об этом будет свидетельствовать следующая ошибка:

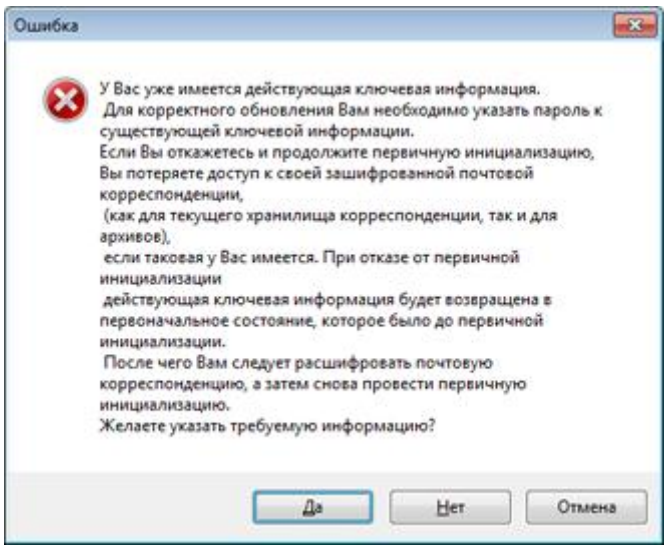


Рисунок 25: Ошибка повторной первичной инициализации

В этом случае можно выбрать один из вариантов действий:

- **Да** — ввести пароль к текущей ключевой информации.

  При этом будет произведена попытка перешифровать существующую ключевую информацию на новом пароле. В случае неудачи полученные ранее зашифрованные письма программы «Деловая почта» будут недоступны для расшифрования и просмотра.

- **Нет** — продолжить процесс первичной инициализации.

  При этом текущая ключевая информация будет заменена на новую, полученные ранее зашифрованные письма программы «Деловая почта» будут недоступны для расшифрования и просмотра.

- **Отмена** (рекомендуется) — отменить текущий процесс инициализации.

Процесс инициализации будет прерван. После этого можно провести расшифрование писем программы «Деловая почта» и снова запустить процесс инициализации.

Смена транспортного каталога

Транспортный каталог — это папка, в которую устанавливается справочно-ключевая информация сетевого узла. Если на компьютере установлено несколько программ ViPNet, для работы которых требуются справочно-ключевая информация сетевого узла и транспортный модуль MFTP, эти программы должны использовать общий транспортный каталог.

Чтобы в программе ViPNet Client изменить транспортный каталог, выполните следующие действия:

1. Запустите программу ViPNet Client из меню **Пуск** или дважды щелкните значок программы на рабочем столе (этот значок отображается, если при установке программы была выбрана соответствующая опция).
2. В окне ввода пароля щелкните значок  справа от кнопки **Настройка** и в меню выберите пункт **Транспортный каталог**.
3. В окне **Просмотр каталогов** укажите путь к транспортному каталогу.

Примечание. По умолчанию транспортным каталогом является папка установки ПО ViPNet.

Работа нескольких пользователей ViPNet на одном сетевом узле

Для того чтобы на одном сетевом узле имели возможность работать несколько пользователей, необходимо для каждого из них провести первичную инициализацию справочно-ключевой информации.

Внимание! Первичную инициализацию всех пользователей, которые будут работать на данном сетевом узле, следует провести до начала работы с программой ViPNet. Крайне не рекомендуется создавать нового пользователя после того, как началась работа с программой ViPNet. В этом случае могут возникнуть проблемы с целостностью и сохранностью пользовательских данных.

Для входа в программу каждому из пользователей необходимо выполнить стандартную процедуру аутентификации — ввести пароль пользователя или авторизоваться с помощью внешнего устройства.

Внимание! При использовании способа аутентификации **Пароль** недопустимо, чтобы у пользователей, работающих на одном сетевом узле, были одинаковые пароли. Поскольку в этом случае разные пользователи будут работать под одной учетной записью.

Региональные настройки

Для корректного отображения русской локализации интерфейса программ ViPNet в русифицированных ОС Microsoft Windows XP/Server 2003/Vista/Server 2008/Windows 7 английской локализации необходимо установить поддержку кириллицы для программ, не поддерживающих Unicode. Эти настройки рекомендуется производить до установки самой программы.

Внимание! 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.

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**).

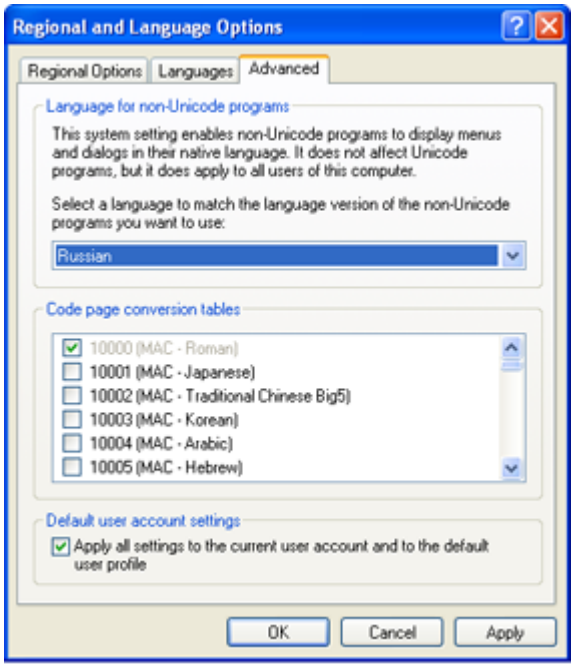


Рисунок 26: Выбор языка для программ, не поддерживающих Юникод, в Windows XP

6 Нажмите кнопку **OK**. Возможно, потребуется перезагрузка.

Для установки поддержки кириллицы на ОС Windows Vista/Server 2008/Windows 7:

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**).

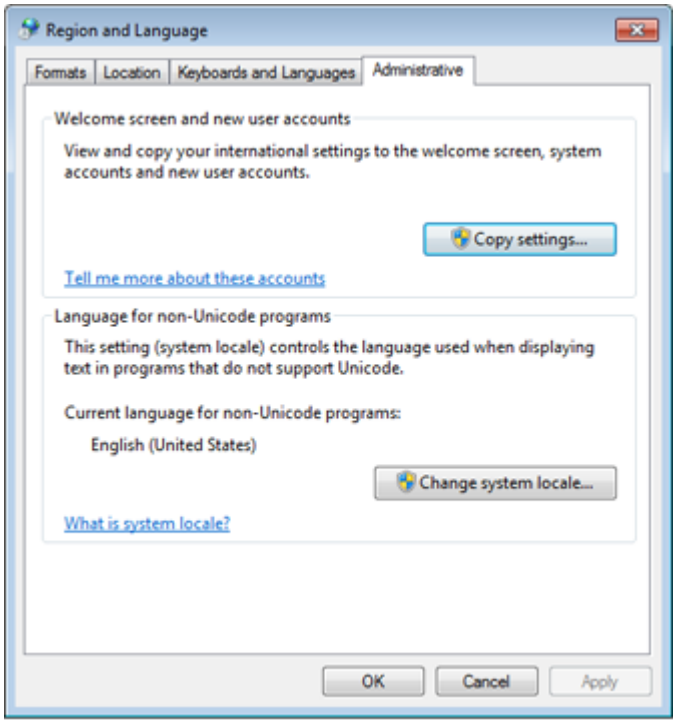


Рисунок 27: Дополнительные языковые параметры

3 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Изменить язык системы** (**Change system locale**).

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**) и нажмите кнопку **OK**.

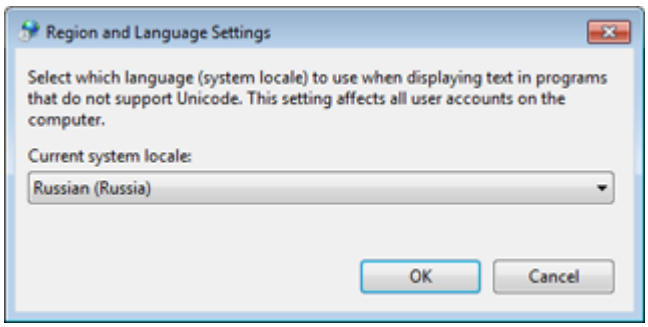


Рисунок 28: Выбор языка системы

5 На вкладке **Дополнительно** (**Administrative**) нажмите кнопку **Копировать параметры** (**Copy settings**).

6 В открывшемся окне установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите кнопку **OK**.

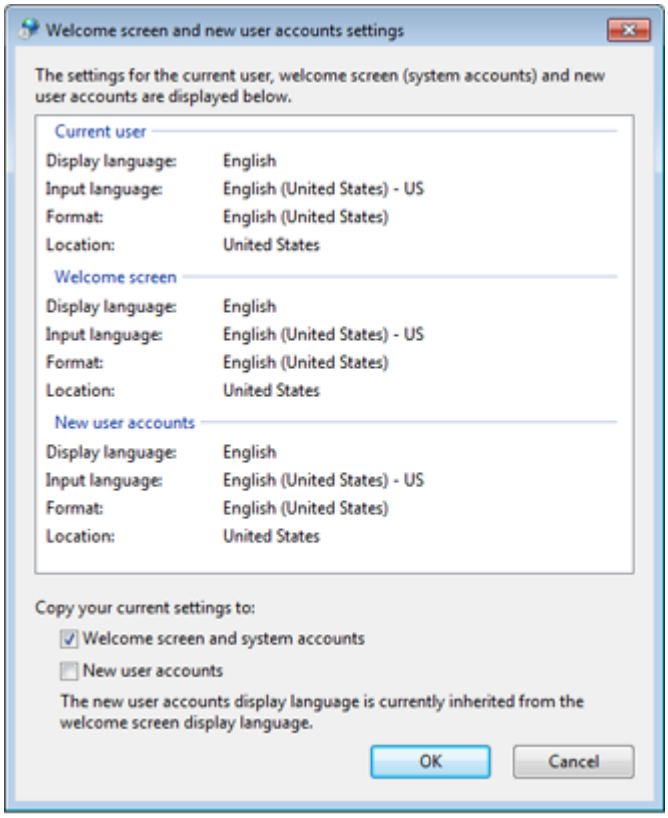


Рисунок 29: Копирование параметров

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)**).

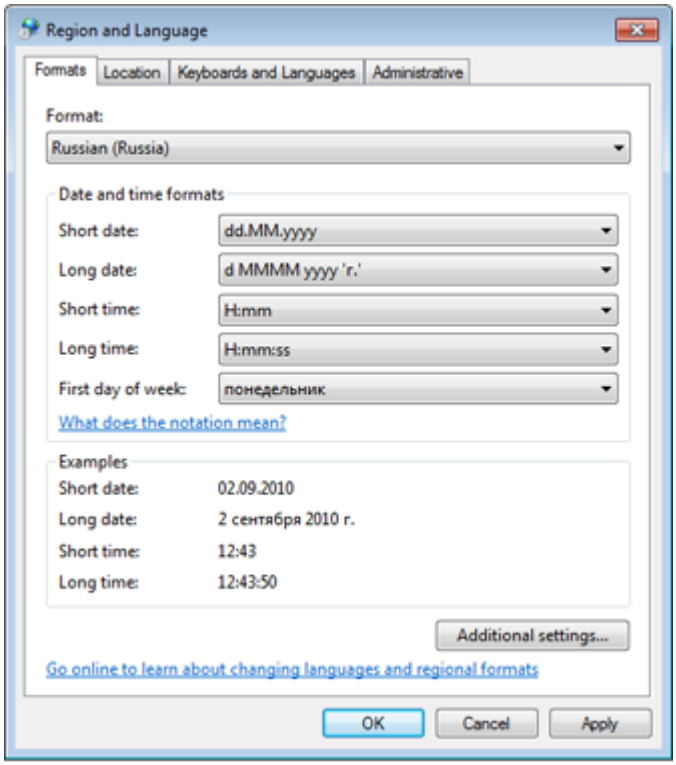


Рисунок 30: Настройка форматов

2 В окне **Язык и региональные стандарты** (**Region and Language**) на вкладке **Расположение** (**Location**) в списке **Текущее расположение** (**Current location**) выберите **Россия**.

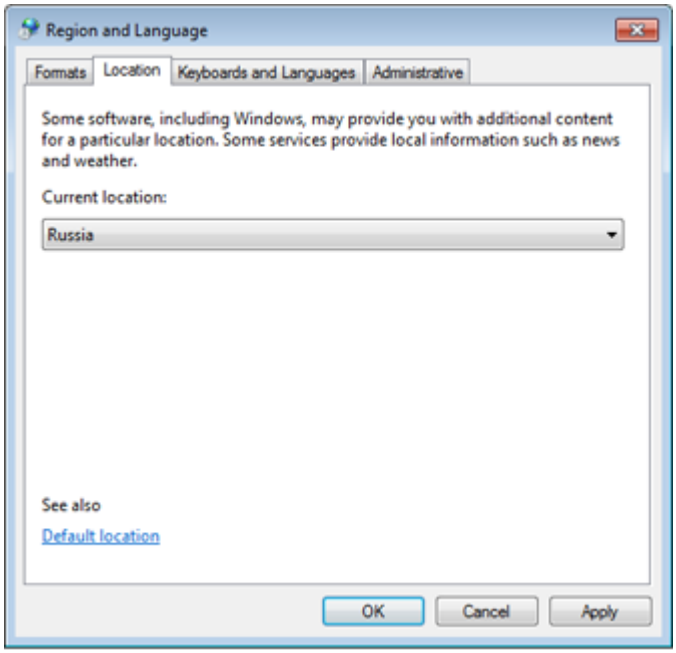


Рисунок 31: Выбор текущего расположения

Перенос абонентского пункта на другой компьютер

Чтобы перенести функционирующий абонентский пункт с одного компьютера на другой (например, в случае замены устаревшего компьютера), сохранив при этом текущие настройки программы ViPNet Монитор и письма «Деловой почты», необходимо скопировать на новый компьютер справочники и ключи, хранилище писем и другие данные из папки программы ViPNet Client.

Внимание! Не следует выполнять перенос абонентского пункта с 32-разрядной версии операционной системы Windows на 64-разрядную версию Windows и наоборот. Если требуется перенести абонентский пункт на компьютер с другой разрядностью Windows, рекомендуется на новом компьютере установить программу ViPNet Client и дистрибутив ключей абонентского пункта (см. «Установка и удаление программы» на стр. 53). В этом случае настройки и данные пользователя не будут сохранены.

С помощью переноса справочников и ключей можно восстановить абонентский пункт после переустановки операционной системы или после изменения папки установки программы ViPNet Client.

После переноса справочников и ключей следует удалить их исходный экземпляр. Недопустима ситуация, когда на разных абонентских пунктах 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 Client:
   - `\d_station`;
   - `\databases`;
   - `\MS`;
   - `\MSArch` (папка хранения архивов «Деловой почты» по умолчанию);
   - `\Protocol` (если требуется скопировать сохраненные протоколы сеансов обмена сообщениями);
   - `\TaskDir` (если требуется сохранить файлы, принятые по файловому обмену);
   - Папка ключей пользователя, 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 Client, тогда следует скопировать папку `\key_disk`.
   - `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);
   - `autoproc.dat` (этот файл присутствует, если настроены правила автопроцессинга);
   - `infotecs.re`;
   - `iplir.cfg, iplirmain.cfg`;
   - `ipliradr.do$`, `ipliradr.doc`;
   - `linkXXXX.txt`, `nodeXXXX.tun` (где XXXX — шестнадцатеричный идентификатор сетевого узла без номера сети);
   - `mftp.ini`;
   - `wmail.ini`.

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

версиях.

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

2 Перед переносом справочно-ключевой информации на новый компьютер установите на этот компьютер программу ViPNet Client (см. «Установка и удаление программы» на стр. 53), но не выполняйте инициализацию справочников и ключей.

   При переносе справочников и ключей на компьютер, на котором уже установлена программа ViPNet Client, убедитесь, что на этом компьютере не установлены справочники и ключи другого сетевого узла. Если эти данные присутствуют, удалите следующие папки и файлы:

   - папку ключей пользователя `\user_BBBB`;
   - файлы `AP*.TXT`, `APNYYYY.CRC`, `APNYYYY.CRG`.

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

4 Если требуется, в файле `wmail.ini` в качестве значений параметров `MSDir` и `MSArchDir` укажите путь к новой папке установки программы ViPNet Client.

5 Если требуется, в файле `mftp.ini` укажите путь к новой папке установки программы ViPNet Client 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 и в окне входа в программу укажите путь к каталогу ключей пользователя, например `C:\Program Files (x86)\InfoTeCS\ViPNet Client\user_AAAA`.

8 Выполните вход в программу ViPNet Монитор (см. «Способы аутентификации пользователя» на стр. 75).

9 В окне **Настройка параметров безопасности** на вкладке **Ключи** установите контейнер ключей электронной подписи. 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 Client\user_AAAA\key_disk\dom`.
   - В списке **Имя контейнера** выберите контейнер (имя контейнера начинается с символов `sgn`).

- Нажмите кнопку **OK**.

После выполнения перечисленных действий программа ViPNet Client готова к работе.

Обновление ПО ViPNet Client

Если выпущена новая версия ПО ViPNet Client, рекомендуется обновить программу, установленную на компьютере. Обновление программного обеспечения на сетевых узлах можно выполнить двумя способами:

- Обновление может быть централизованно отправлено на все сетевые узлы администратором из ЦУС или ViPNet Manager.
- Программу можно обновить на сетевом узле вручную с помощью установочного файла.

Прием централизованного обновления

В зависимости от настроек программы ViPNet Монитор, поступившее обновление ПО ViPNet Client будет принято автоматически либо программа выдаст предупреждение об обновлении. Если в момент поступления обновления активно окно обмена защищенными сообщениями, предупреждение появится в любом случае.

Чтобы получать предупреждения об обновлении, в окне **Настройка** в разделе **Общие** > **Предупреждения** убедитесь, что установлен флажок **Выдавать предупреждения перед ViPNet-обновлениями**. По умолчанию флажок установлен.

Чтобы принять или отложить обновление ПО:

1. В окне сообщения об обновлении выполните одно из действий:
   - Чтобы начать обновление немедленно, нажмите кнопку **OK.**

     Программа ViPNet Монитор будет выгружена из памяти компьютера и начнется процесс обновления. То же самое произойдет, если обновление будет принято автоматически без предупреждения.

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

При обновлении ПО выполняется проверка, позволяет ли лицензия установить данное обновление. Если номер версии обновления превышает лицензионное ограничение, обновление не будет установлено.

- Чтобы отложить обновление, нажмите кнопку **Отмена**.

  В этом случае при следующей загрузке программ ViPNet Монитор или ViPNet Деловая почта снова появится сообщение с предложением провести обновление.

2 Если после обновления требуется перезагрузка компьютера, программа выдаст соответствующее сообщение. Чтобы перезагрузить компьютер немедленно, нажмите кнопку **OK**. Чтобы отложить перезагрузку, нажмите кнопку **Отмена**.

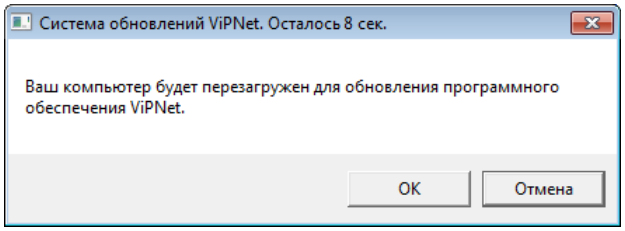


Рисунок 32: Сообщение об автоматической перезагрузке компьютера

Если не нажимать ни одну из кнопок, через некоторое время сообщение автоматически закроется. При этом:

- Если администратор сети ViPNet при отправке обновления ПО установил флажок обязательной перезагрузки компьютера после обновления ПО, компьютер будет автоматически перезагружен.
- Если администратор сети ViPNet при отправке обновления ПО не установил флажок обязательной перезагрузки компьютера после обновления, произойдет запуск программы ViPNet Монитор. Данный сценарий является рискованным, так как в случае отложенного обновления запуск ПО ViPNet может быть неуспешным. В этом случае настоятельно рекомендуется выйти из приложений ViPNet и перезагрузить компьютер вручную.

Обновление вручную

Для обновления ПО ViPNet Client вручную, требуется установочный файл новой версии ПО. Для обновления выполните следующие действия:

1 Выгрузите из памяти компьютера все компоненты ПО ViPNet Client.

2 Двойным щелчком запустите программу установки setup.exe  .

Примечание. Если номер версии устанавливаемого ПО ViPNet Client превышает лицензионное ограничение, установка обновления будет невозможна.

---

3 В окне с сообщением о том, что обнаружена установленная ранее версия ПО ViPNet Client, нажмите кнопку **Да**, чтобы начать обновление (при нажатии на кнопку **Нет** обновление не произойдет и будет запущен мастер для установки ПО в другую папку).

4 Дождитесь завершения процесса обновления.

5 При успешном окончании обновления перезагрузите компьютер.

Запуск программы

По умолчанию программа ViPNet Монитор запускается автоматически после авторизации пользователя ViPNet, которая выполняется во время загрузки операционной системы Windows.

Внимание! Инициализация ViPNet-драйвера выполняется на начальном этапе загрузки Windows, то есть до инициализации остальных служб и драйверов операционной системы. Работа ViPNet-драйвера до авторизации пользователя ViPNet не зависит от настроек фильтров открытой сети, а определяется текущим режимом безопасности и рядом фильтров по умолчанию (см. «Основные принципы фильтрации трафика» на стр. 123).

Если вы вышли из программы или отказались от ввода пароля пользователя при загрузке Windows, то для запуска программы ViPNet Монитор:

1. Выполните одно из действий:
   - В меню **Пуск** выберите пункт **Программы**, затем **ViPNet**, затем **Client** и щелкните **ViPNet Монитор**.

     При установке путь к программе в меню **Пуск** мог быть изменен.
   - Дважды щелкните ярлык программы на рабочем столе (этот ярлык отображается, только если при установке программы была выбрана соответствующая опция).

   Откроется окно входа в программу.

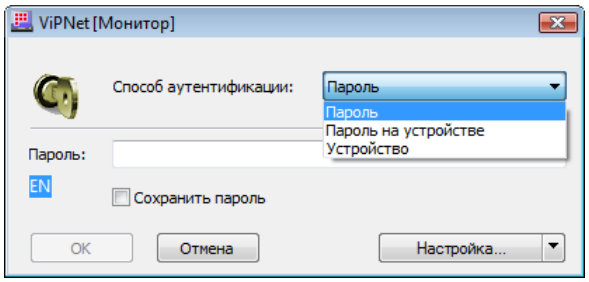


Рисунок 33: Окно входа в программу

2. В зависимости от текущего способа аутентификации (см. «Способы аутентификации пользователя» на стр. 75), для входа в программу введите пароль пользователя либо подключите внешнее устройство хранения данных и введите ПИН-код.

Внимание! Если ПО ViPNet Client было обновлено с версии 3.0.x до текущей версии и до обновления использовался способ аутентификации **Пароль на устройстве** или **Устройство**, то хранящиеся на внешнем устройстве ключи необходимо конвертировать в новый формат. При попытке войти в ViPNet Client с помощью устройства, на котором хранятся ключи старого формата, будет автоматически запущена программа конвертации ключей (см. «Конвертация ключей на внешнем устройстве» на стр. 72).

3 После ввода необходимых для аутентификации данных нажмите кнопку **OK**. Откроется окно программы ViPNet Монитор.

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 окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Смена пользователя**. Откроется окно входа в программу (см. Рисунок 33 на стр. 71).

2 Введите пароль пользователя, от имени которого требуется войти в программу и нажмите **OK**.

Примечание. На сетевом узле должна быть установлена справочно-ключевая информация пользователя, от имени которого выполняется вход в программу.

Конвертация ключей на внешнем устройстве

Конвертер ключей ViPNet запускается автоматически в случае, когда требуется преобразование ключей ViPNet, хранящихся на внешних устройствах в старом формате, в новый формат.

Чтобы преобразовать ключи, хранящиеся на внешних устройствах в старом формате, в новый формат, выполните следующие действия:

1 В окне **Конвертер ключей ViPNet**, в списке **Устройство** выберите внешнее устройство хранения данных, на котором хранятся ключи в старом формате. Если

список пуст, значит устройство не подключено либо для него неправильно установлены драйверы.

2 В поле **Введите ПИН-код** укажите ПИН-код выбранного внешнего устройства хранения данных.

3 Далее в списке **Ключи ViPNet на устройстве** напротив каждого из ключей в старом формате в столбце **Действие** выберите **Конвертировать**.

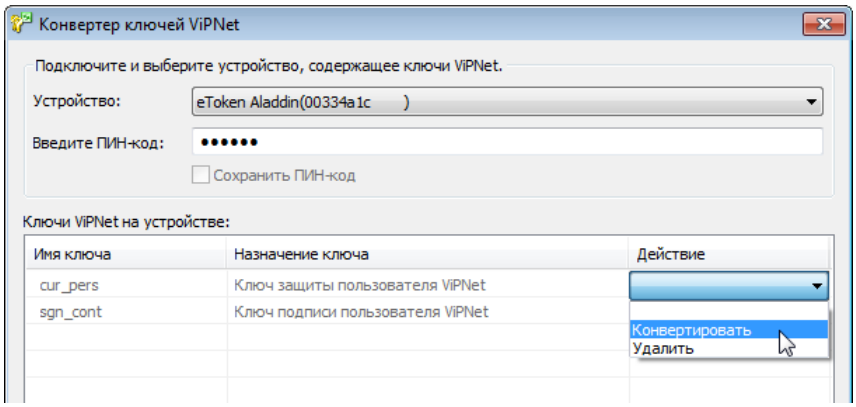


Рисунок 34: Выбор действия Конвертировать для ключей старого формата

4 Введите пароль доступа к ключу.

Внимание! Если вы не знаете пароль к какому-либо ключу, узнайте пароль у администратора или выберите для него действие **Удалить**. Действие должно быть указано для каждого ключа, иначе кнопка **Конвертировать** будет неактивна.

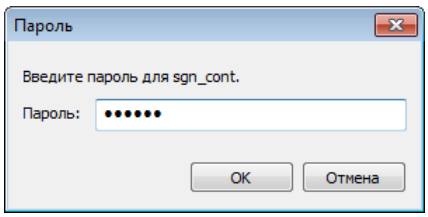


Рисунок 35: Окно ввода пароля

Если на устройстве уже имеется ключ с тем же именем и в новом формате, появится предупреждение об этом.

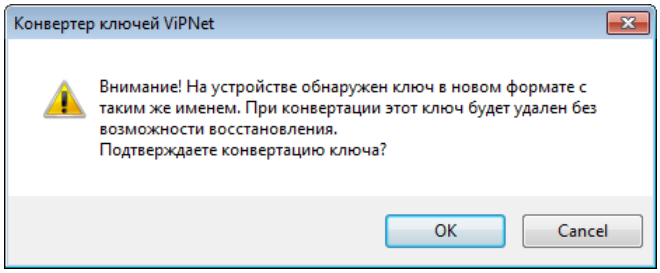


Рисунок 36: Предупреждение о совпадении имен ключей

Внимание! Если на устройстве уже имеется ключ в новом формате с точно таким же именем, что и ключ в старом формате, то при конвертации старого ключа ключ в новом формате будет удален без возможности восстановления.

5 Нажмите кнопку **Конвертировать**.

Внимание! Если в процессе конвертации ключей в новый формат произошел сбой, есть возможность продолжить процесс конвертации. Для этого повторно откройте **Конвертер ключей ViPNet**, запустив файл `converterad.exe` в папке установки программы. Нажмите кнопку **Да** в ответ на вопрос, хотите ли вы продолжить выполнение оставшихся действий.

Способы аутентификации пользователя

В программе ViPNet Монитор предусмотрено три способа аутентификации пользователя: **Пароль**, **Пароль на устройстве**, **Устройство**.

Внимание! Использовать способ аутентификации **Пароль на устройстве** для входа в ПО ViPNet Client крайне не рекомендуется.

По умолчанию установлен способ аутентификации **Пароль**. Администратор сетевого узла может изменить способ аутентификации (см. «Изменение способа аутентификации пользователя» на стр. 258) на вкладке **Ключи** в окне **Настройка параметров безопасности**.

При выборе способов **Пароль на устройстве** и **Устройство** аутентификация пользователя осуществляется с помощью внешних устройств хранения данных (см. «Информация о внешних устройствах хранения данных» на стр. 45). Чтобы использовать какое-либо устройство для аутентификации пользователя, нужно записать на это устройство необходимую ключевую информацию, а на компьютер нужно установить драйверы устройства. Записать ключевую информацию на внешнее устройство можно при изменении способа аутентификации пользователя (см. «Изменение способа аутентификации пользователя» на стр. 258) или в программе УКЦ при создании дистрибутива ключей (в программе ViPNet Manager работа с внешними устройствами невозможна).

Внимание! Если при использовании способов аутентификации **Пароль на устройстве** и **Устройство** внешнее устройство будет отключено, компьютер будет автоматически заблокирован. Для продолжения работы необходимо вновь подключить это внешнее устройство. При необходимости параметры автоматической блокировки компьютера и IP-трафика могут быть изменены (см. «Особенности блокировки компьютера при использовании внешнего устройства для аутентификации пользователя» на стр. 208).

В зависимости от текущего способа аутентификации для входа в программу ViPNet Монитор выполните следующие действия:

1 **Пароль.**

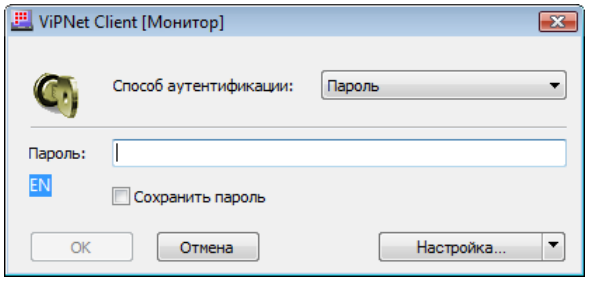


Рисунок 37: Способ аутентификации «Пароль»

Для входа в программу:

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

1.2 В поле **Пароль** введите пароль пользователя сетевого узла.

Если сохранение пароля в реестре разрешено настройками программы (см. «Дополнительные настройки параметров безопасности» на стр. 256), для сохранения пароля можно установить соответствующий флажок.

1.3 Нажмите кнопку **OK**.

2 **Пароль на устройстве** — в этом случае для аутентификации пользователя используется внешнее устройство хранения данных.

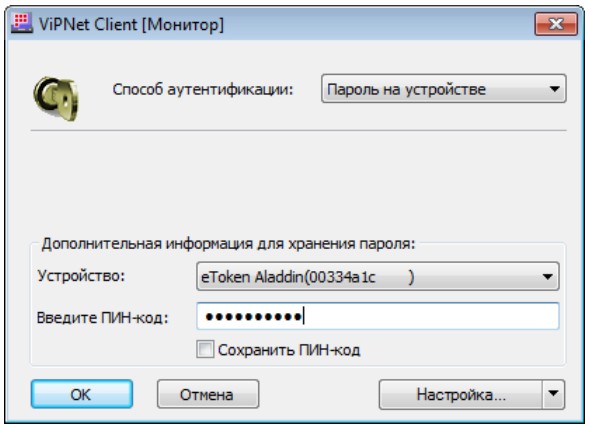


Рисунок 38: Способ аутентификации «Пароль на устройстве»

Для входа в программу:

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

2.2 Подключите внешнее устройство хранения данных.

2.3 В списке **Устройство** выберите внешнее устройство хранения данных, на котором был сохранен парольный ключ пользователя.

2.4 Введите ПИН-код, если требуется. Необходимость ввода ПИН-кода зависит от типа используемого внешнего устройства (см. Рисунок 40 на стр. 78).

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

2.5 Нажмите кнопку **OK**.

Как правило, использование данного способа аутентификации предполагает, что пароль хранится на устройстве и вам не известен. Однако если вы знаете пароль пользователя, то помимо аутентификации с помощью внешнего устройства для входа в программу можно использовать аутентификацию по паролю (см. пункт 1). Данная возможность обеспечивает вход в программу в случае поломки внешнего устройства.

3 **Устройство** — в этом случае для аутентификации используются внешнее устройство и пароль пользователя ViPNet.

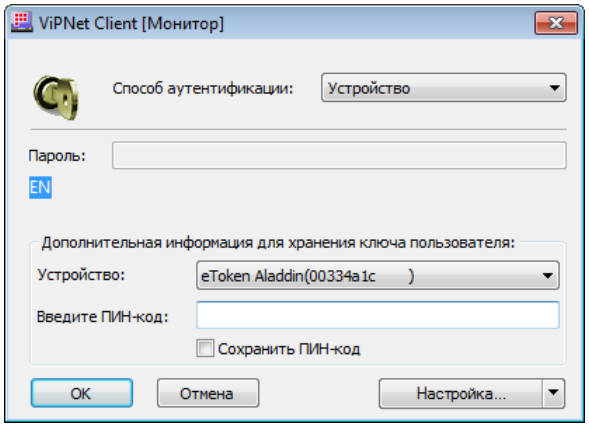


Рисунок 39: Способ аутентификации «Устройство»

Для входа в программу:

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

3.2 Подключите внешнее устройство хранения данных.

3.3 Если требуется, в поле **Пароль** введите пароль пользователя сетевого узла. Необходимость ввода пароля зависит от типа используемого внешнего устройства хранения данных (см. Рисунок 40 на стр. 78).

3.4 В списке **Устройство** выберите внешнее устройство хранения данных, на котором была сохранена личная ключевая информация пользователя.

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

3.6 Нажмите кнопку **ОК**.

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

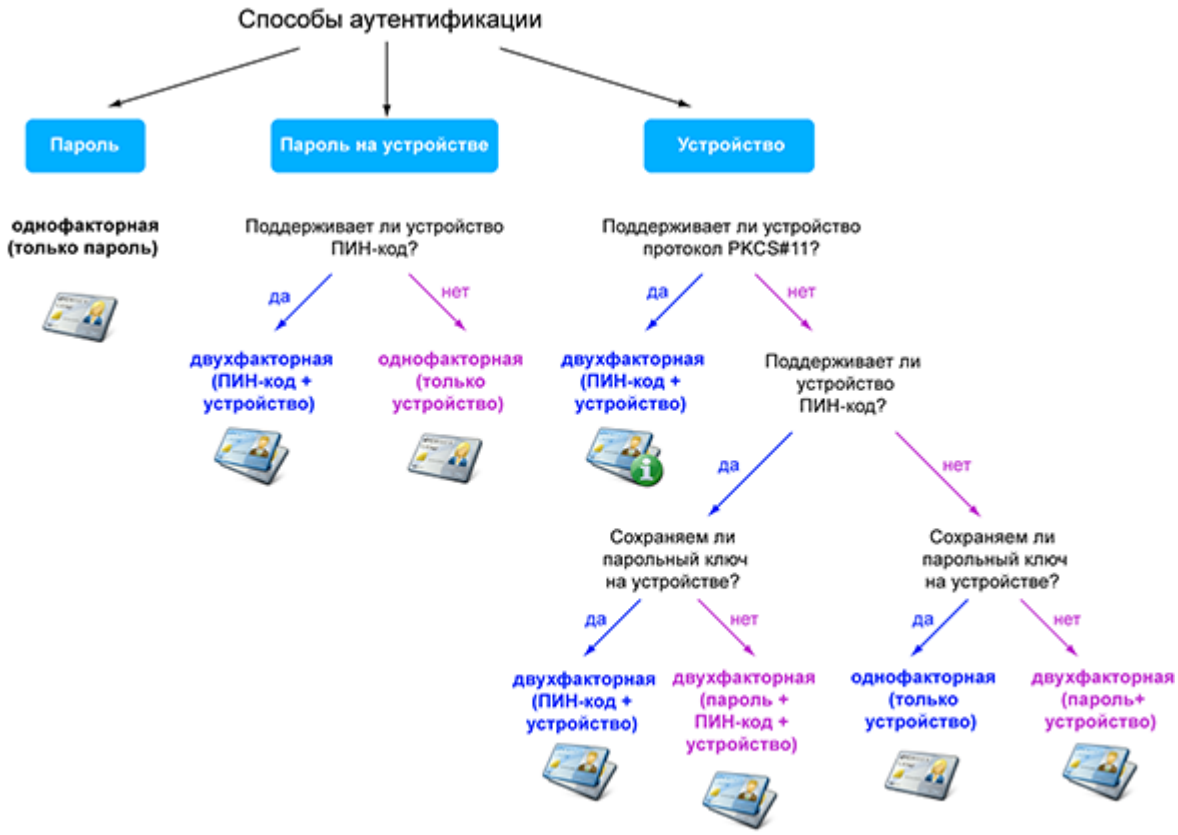


Рисунок 40: Схема соответствия между факторами и способами аутентификации

Интерфейс программы ViPNet Монитор

Окно программы ViPNet Монитор представлено на следующем рисунке:

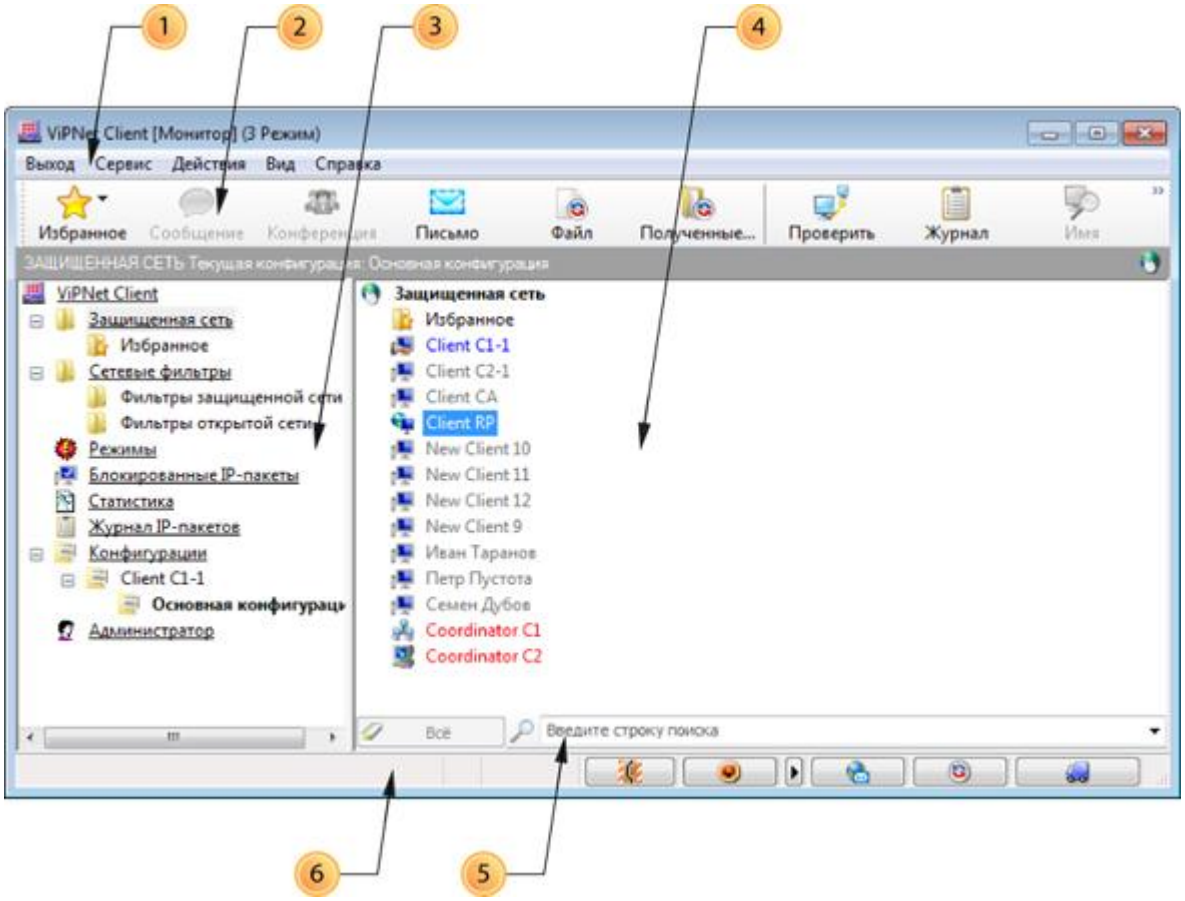


Рисунок 41: Окно программы ViPNet Монитор

Цифрами на рисунке обозначены:

1. Главное меню программы.
2. Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов, в меню **Вид** выберите пункт **Настроить панель.**

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 Manager. Подробнее см. Работа в разделе «Защищенная сеть»(на стр. 81).
- **Сетевые фильтры**. Содержит подразделы с правилами фильтрации IP-трафика:
  - **Фильтры защищенной сети** — предназначен для настройки правил фильтрации защищенного трафика.
  - **Фильтры открытой сети** — предназначен для настройки правил фильтрации открытого трафика.
- **Режимы** — предназначен для выбора режима безопасности (см. «Режимы безопасности» на стр. 128).
- **Блокированные IP-пакеты** — предназначен для просмотра информации о заблокированных IP-пакетах.
- **Статистика** — предназначен для просмотра статистики фильтрации IP-пакетов (см. «Просмотр статистики фильтрации IP-пакетов» на стр. 225).
- **Журнал IP-пакетов** — предназначен для поиска записей в Журнале IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 210).
- **Конфигурации** — предназначен для управления конфигурациями программы ViPNet Монитор (см. «Управление конфигурациями программы» на стр. 227).
- **Администратор** — отображается только после ввода пароля администратора сетевого узла и служит для настройки дополнительных параметров программы (см. «Работа в программе с правами администратора» на стр. 251).

Примечание. Количество и порядок расположения разделов на панели навигации зависит от уровня полномочий пользователя, который определяется в ЦУС или ViPNet Manager.

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

5 Строка поиска. Отображается в разделах **Защищенная сеть**, **Фильтры защищенной сети**, **Фильтры открытой сети** и **Блокированные IP-пакеты**. Для поиска по разделу введите в этой строке часть адреса, имени или другие параметры сетевого узла.

В разделе **Защищенная сеть** поиск ведется 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 **Всё**.

6 Строка состояния. В правой части строки состояния расположены следующие кнопки:

-  — вызов программы «Контроль приложений» (см. документ «ViPNet Контроль приложений. Руководство пользователя»).
-  — блокировка компьютера (см. «Блокировка компьютера и IP-трафика» на стр. 206). Для выбора режима блокировки предназначена кнопка  .
-  — вызов программы «Деловая почта» (см. документ «ViPNet Деловая почта. Руководство пользователя»).
-  — вызов программы «Файловый обмен» (см. «Файловый обмен» на стр. 193).
-  — вызов транспортного модуля MFTP (см. документ «ViPNet MFTP. Руководство администратора»).

Работа в разделе «Защищенная сеть»

Раздел **Защищенная сеть** (см. «Интерфейс программы ViPNet Монитор» на стр. 79) содержит список защищенных узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью или ViPNet Manager.

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

Таблица 4. Обозначение статуса сетевых узлов

Значок	Цвет имени	Статус сетевого узла
	Синий	Свой сетевой узел
	Серый	Клиент в данный момент отключен от сети либо нет данных о его статусе

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

Примечание. Внешний вид значков зависит от используемой операционной системы (в таблице приведены значки для Windows Vista и Windows 7).

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

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

1. Чтобы создать новую папку:
   - В окне программы ViPNet Монитор на левой либо на правой панели щелкните элемент **Защищенная сеть** правой кнопкой мыши.
   - В контекстном меню выберите пункт **Создать новую папку**.

   Новая папка появится на панели навигации, а также в разделе **Защищенная сеть**.
2. Чтобы перенести сетевые узлы в какую-либо папку, в разделе **Защищенная сеть** выберите один или несколько сетевых узлов и перетащите их в нужную папку.
3. Чтобы переименовать папку, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Переименовать**.
4. 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 часть имени, IP-адреса или другие параметры узла в строку поиска (см. «Интерфейс программы ViPNet Монитор» на стр. 79).

Для просмотра свойств сетевого узла дважды щелкните имя узла. Откроется окно **Свойства узла**, в котором приведены общие сведения о сетевом узле и содержатся настройки доступа к узлу (см. «Настройка доступа к узлам сети ViPNet» на стр. 108).

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. 183), выполните одно из действий:

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

Завершение работы с программой

Существует несколько способов завершения работы с программой ViPNet Монитор:

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 выберите пункт **Выход**. В окне подтверждения нажмите **Да**.

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

Отключение защиты IP-трафика

Если требуется отключить защиту трафика с помощью ViPNet Client:

1. В программе ViPNet Монитор установите пятый режим безопасности. В этом режиме шифрование трафика отключено, весь открытый трафик пропускается.
2. После этого можно выйти из программы ViPNet Монитор, защита трафика останется отключенной.

Чтобы отказаться от защиты трафика при загрузке операционной системы:

1. В окне ввода пароля пользователя ViPNet нажмите кнопку **Отмена** или клавишу **Esc**.
2. В окне подтверждения следует нажать кнопку **Да**.

   После загрузки операционной системы защита трафика будет отключена.

Настройка параметров запуска и аварийного завершения программы

Для настройки параметров запуска и экстренного завершения программы:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.
2. В окне **Настройка** на левой панели выберите раздел **Общие > Запуск и аварийное завершение**.
3. Чтобы при запуске программы не производить выбор конфигурации (см. «Управление конфигурациями программы» на стр. 227), 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 вызываться не будет независимо от установки флажка.
4. Чтобы при запуске программы блокировать доступ к рабочему столу компьютера, установите флажок **Блокировать компьютер** (см. «Блокировка компьютера и IP-трафика» на стр. 206). 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 Watch Dog** и в поле **Время до перезагрузки** введите количество секунд, через которое будет происходить перезагрузка.

   Функция Watch Dog отслеживает работоспособность ViPNet Монитор и в случае сбоя аппаратного или программного обеспечения перезапускает ОС компьютера. Использование Watch Dog особенно важно на удаленных компьютерах, доступ к которым проблематичен.

Примечание. В 64-разрядных операционных системах функция Watch Dog не поддерживается.

2

Настройка параметров подключения к сети

Принципы осуществления соединений в сети ViPNet

Узлы сети ViPNet могут быть подключены к внешней сети непосредственно либо взаимодействовать с внешней сетью через различные межсетевые экраны (МЭ), в том числе ViPNet-координатор.

Информацию об узлах ViPNet, параметрах доступа и их активности в данный момент каждый компьютер получает от своего сервера IP-адресов (см. «Выбор сервера IP-адресов» на стр. 90) или от других координаторов (если узел сам является координатором). Таким образом, координатор отвечает за сбор и рассылку информации о сетевых узлах на узлы, для которых он выполняет функции сервера IP-адресов.

Сетевые узлы ViPNet могут располагаться внутри локальных сетей 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 автоматически поддерживает разнообразные протоколы канального уровня. Для создания защищенных VPN-туннелей между сетевыми узлами используются IP-протоколы двух типов (IP/241 и IP/UDP), в которые упаковываются пакеты любых других IP-протоколов.

При взаимодействии любых сетевых узлов между собой, если между ними отсутствуют межсетевые экраны с преобразованием адресов, 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 42: Между сетевыми узлами нет межсетевых экранов

Если между сетевыми узлами находится межсетевой экран, выполняющий преобразование сетевых адресов (в том числе координатор ViPNet), автоматически используется протокол UDP, который позволяет IP-пакетам проходить через межсетевые экраны. Исходный пакет после шифрования упаковывается в UDP-пакет. Для настройки

соединения между узлами на межсетевом экране необходимо указать разрешающее правило для UDP-протокола с фиксированным портом источника. Порт назначения в общем случае не задается, поскольку он регистрируется по пакетам от узла получателя.

Рисунок 43: Сетевые узлы соединяются через межсетевой экран

На сетевых узлах ViPNet можно настроить следующие типы подключения к внешней сети:

1. Непосредственное подключение к внешней сети, межсетевой экран не используется (см. «О подключении без использования межсетевого экрана» на стр. 92). В этом случае никаких настроек параметров межсетевого экрана выполнять не нужно.
2. Подключение через координатор, обеспечивающий трансляцию адресов для сетевых узлов ViPNet. Тип межсетевого экрана — **Координатор** (см. «О подключении через координатор» на стр. 94).
3. Подключение через межсетевой экран, на котором настройка статических правил трансляции адресов затруднительна или невозможна. Тип межсетевого экрана — **С динамической трансляцией адресов** (см. «О подключении через межсетевой экран с динамической трансляцией адресов» на стр. 97).
4. Подключение через межсетевой экран, на котором возможна настройка статических правил трансляции адресов. Тип межсетевого экрана — **Со статической трансляцией адресов** (см. «О подключении через межсетевой экран со статической трансляцией адресов» на стр. 102).

Чтобы избежать настройки типа подключения непосредственно на каждом сетевом узле, рекомендуется задать параметры подключения сетевых узлов централизованно в программе ViPNet Administrator или ViPNet Manager.

Выбор сервера IP-адресов

Сервер IP-адресов — это координатор, от которого абонентский пункт получает информацию об IP-адресах, параметрах доступа и состоянии сетевых узлов, с которыми связан данный абонентский пункт.

В случае изменения IP-адреса абонентского пункта и параметров его подключения к сети новые данные отправляются на сервер IP-адресов. Периодически абонентский пункт подтверждает серверу IP-адресов свое присутствие в сети.

По умолчанию в качестве сервера IP-адресов установлен координатор, на котором данный абонентский пункт зарегистрирован в программе ViPNet Administrator или ViPNet Manager, то есть сервер-маршрутизатор абонентского пункта. Рекомендуется использовать сервер IP-адресов по умолчанию, однако в случае необходимости в качестве сервера IP-адресов можно выбрать любой координатор своей сети, с которым связан данный абонентский пункт.

Чтобы изменить сервер IP-адресов, выполните следующие действия:

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

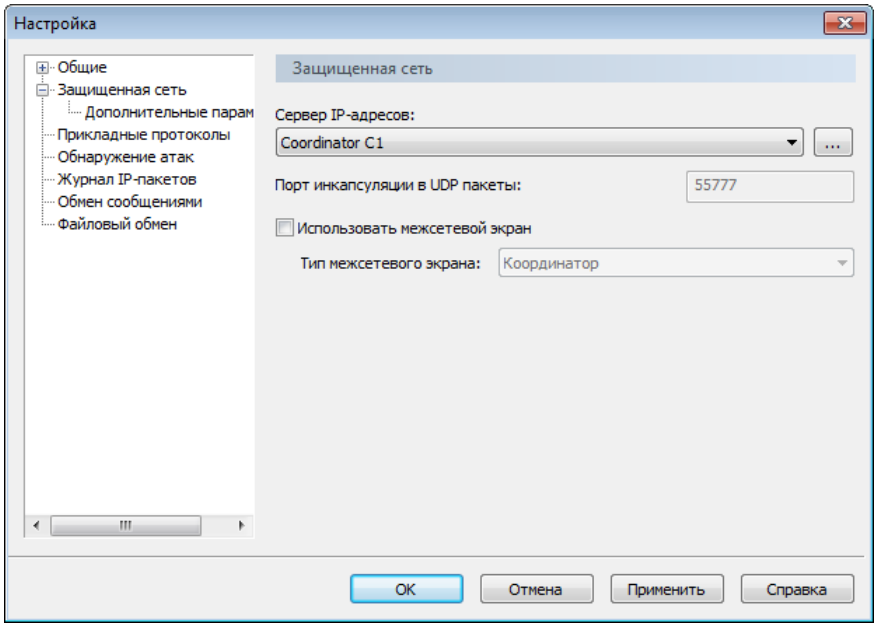


Рисунок 44: Выбор сервера IP-адресов

3 В списке **Сервер IP-адресов** выберите координатор, который требуется назначить сервером IP-адресов.

Если нужного координатора нет в списке, нажмите кнопку  и выберите координатор в окне **Выбор сетевого узла**.

Внимание! Не рекомендуется выбирать в качестве сервера IP-адресов координатор доверенной сети ViPNet (это возможно, если с другой сетью установлено межсетевое взаимодействие). Если выбрать сервер IP-адресов из другой сети ViPNet, абонентский пункт будет получать информацию о состоянии только тех сетевых узлов, которые принадлежат к сети сервера IP-адресов. В этом случае соединение с некоторыми узлами своей сети ViPNet может быть невозможно.

---

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

5 Убедитесь, что указаны верные параметры доступа к выбранному серверу IP-адресов (см. «Настройка доступа к защищенным узлам» на стр. 112).

Подключение без использования межсетевого экрана

О подключении без использования межсетевого экрана

Данный тип подключения следует выбирать на сетевом узле, если он имеет хотя бы один IP-адрес, доступный по общим правилам маршрутизации пакетов любым другим узлам, с которыми данный узел должен устанавливать соединения. Например, это может быть публичный IP-адрес.

Сетевые узлы, использующие такой тип подключения, всегда соединяются друг с другом напрямую по протоколу IP/241. При этом шифрованный трафик от таких клиентов к координаторам, а также к клиентам, использующим в качестве межсетевого экрана координаторы, всегда инкапсулируется в UDP-пакеты.

Внимание! Если на сетевом узле, который имеет частный IP-адрес внутри локальной сети и выходит в Интернет через межсетевой экран, настроено подключение без использования межсетевого экрана, то этот узел не сможет устанавливать соединения с сетевыми узлами ViPNet, расположенными вне локальной сети с ее системой частных IP-адресов.

Настройка подключения без использования межсетевого экрана

Для настройки подключения без использования сетевого экрана:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.
2. В окне **Настройка** выберите раздел **Защищенная сеть**.

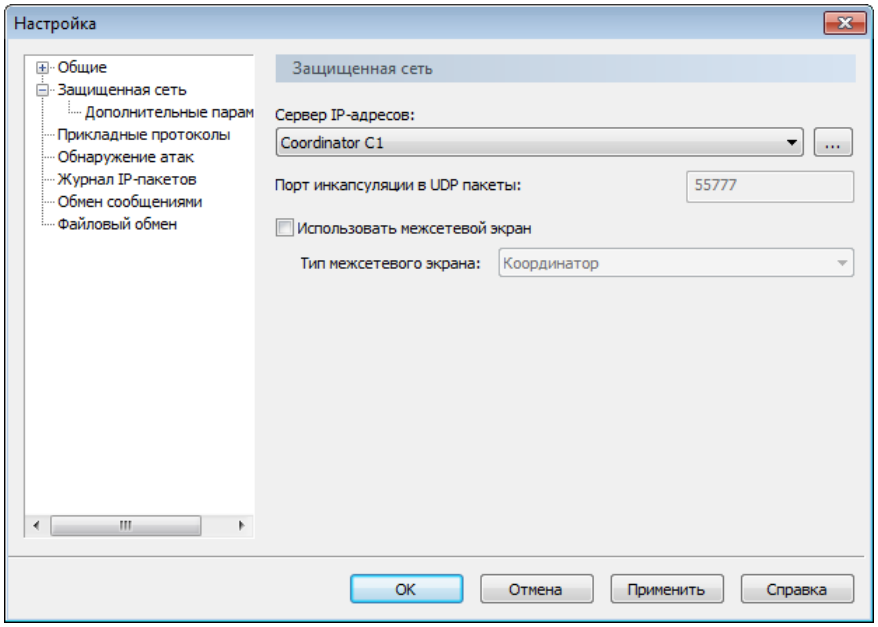


Рисунок 45: Подключение клиента без использования межсетевого экрана

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

Подключение через координатор

О подключении через координатор

Если на границе локальной сети в качестве шлюза установлен ViPNet-координатор, то для абонентских пунктов локальной сети рекомендуется выбрать этот координатор в качестве межсетевого экрана.

Внимание! Для правильной работы данного типа подключения необходимо, чтобы между абонентским пунктом и координатором не было никаких устройств, осуществляющих трансляцию адресов (NAT).

Если клиент использует в качестве межсетевого экрана координатор, то шифрованный трафик между этим клиентом и узлами, которые недоступны напрямую по их адресам, будет перенаправляться через координатор. В этом случае координатор играет роль криптошлюза — маршрутизатора для шифрованных пакетов с функцией трансляции адресов (осуществляется преобразование IP- и MAC-адресов).

Автоматическая маршрутизация шифрованных пакетов клиента через координатор осуществляется без изменения настроек протокола TCP/IP в операционной системе. Настройки сетевого шлюза, используемого по умолчанию, после установки ПО ViPNet не изменяются. В результате маршрутизация нешифрованных пакетов также остается неизменной, и работа в сети может быть продолжена сразу после установки ПО ViPNet. Новые маршруты создаются только для шифрованного IP-трафика.

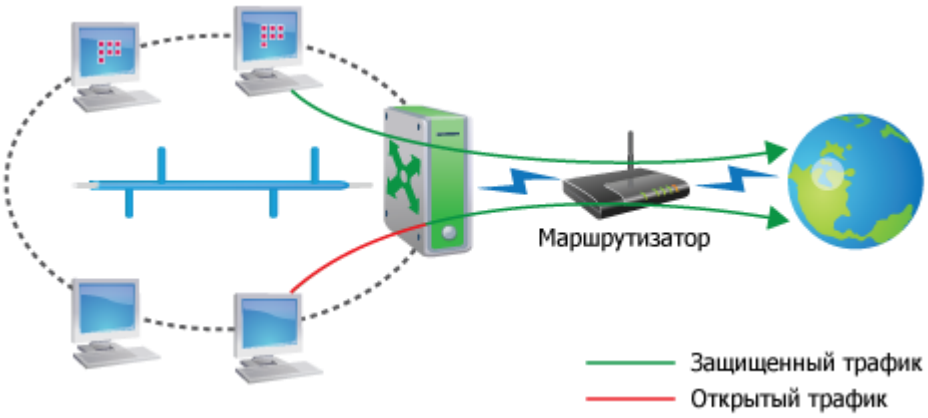


Рисунок 46: Подключение абонентских пунктов через координатор

В качестве межсетевого экрана можно выбрать координатор, не являющийся сервером IP-адресов для данного абонентского пункта.

Эта возможность может быть полезна для мобильного пользователя ViPNet, находящегося в чужой локальной сети. Для работы в сети ViPNet в обычном режиме мобильному пользователю достаточно выбрать в качестве межсетевого экрана координатор, напрямую доступный в этой локальной сети (при наличии связи с этим координатором).

Кроме того, обеспечивается своего рода резервирование криптошлюзов в сети. Если заданный координатор недоступен, то можно выбрать в списке другой подходящий координатор и продолжить работу.

Настройка подключения

Чтобы настроить подключение абонентского пункта через координатор:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.
2. На левой панели окна **Настройка** выберите раздел **Защищенная сеть**.
3. Установите флажок **Использовать межсетевой экран**.
4. Из списка **Тип межсетевого экрана** выберите **Координатор**.
5. По умолчанию в качестве межсетевого экрана будет выбран координатор, указанный в качестве сервера IP-адресов. При необходимости из списка **Координатор** можно выбрать другой координатор. Например, мобильные пользователи ViPNet в разных сетях могут использовать в качестве межсетевого экрана разные координаторы.

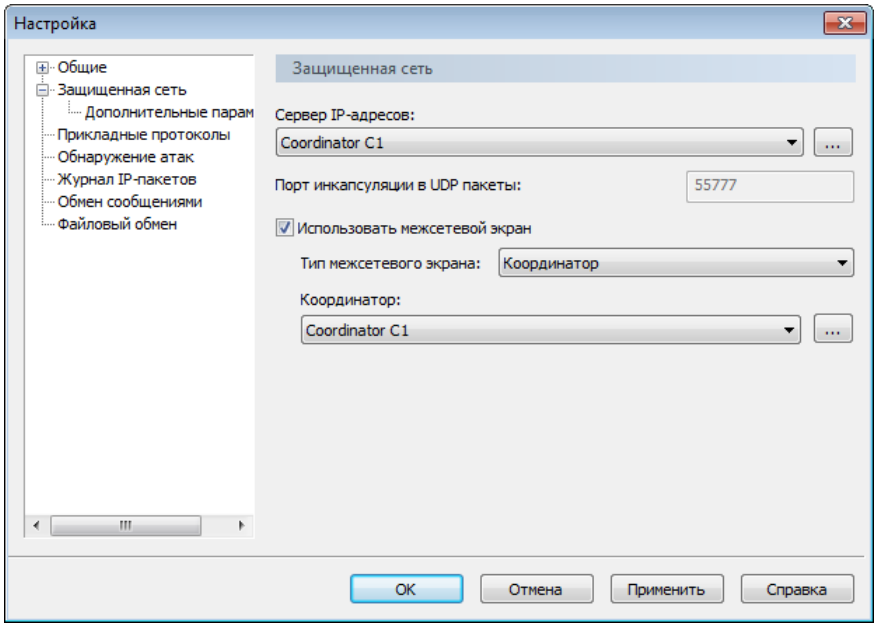


Рисунок 47: Подключение абонентского пункта через координатор

Примечание. Не изменяйте значение в списке **Сервер IP-адресов**, чтобы гарантированно получать от сервера IP-адресов полный список допустимых соединений (другие координаторы могут обладать неполной информацией).

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

Подключение через межсетевой экран с динамической трансляцией адресов

О подключении через межсетевой экран с динамической трансляцией адресов

Данный тип подключения для абонентского пункта следует выбирать в том случае, если в локальной сети нет координатора или невозможно использовать координатор в качестве межсетевого экрана, а соединение с внешней сетью происходит через межсетевой экран, на котором затруднительно настроить статические правила трансляции адресов.

Для правильной работы подключения через межсетевой экран **С динамической трансляцией адресов** во внешней сети должен существовать координатор, доступный по публичному IP-адресу. Адрес используемого межсетевого экрана должен быть указан в сетевых настройках ОС абонентского пункта в качестве шлюза по умолчанию.

Соединение через межсетевой экран **С динамической трансляцией адресов** наиболее универсально и может быть использовано практически в любых ситуациях. Основное его назначение — обеспечить надежное двустороннее соединение с узлами, работающими через межсетевые экраны, при этом настройка статических правил трансляции адресов на межсетевых экранах затруднена или невозможна (в том числе и просто из-за отсутствия полномочий у пользователя). Такая ситуация типична при использовании простейших сетевых NAT-устройств, например, DSL-модемов, беспроводных точек доступа, а также при использовании общего доступа к подключению Интернет (ICS — Internet Connection Sharing) в ОС Windows. Затруднительно также произвести настройки правил трансляции на межсетевых экранах, установленных у провайдера (в домашних сетях, сетях GPRS и других сетях, где провайдер предоставляет частный IP-адрес).

Все NAT-устройства обеспечивают пропускание UDP-трафика благодаря автоматическому созданию так называемых динамических NAT-правил для входящего трафика. Эти правила создаются на основании параметров исходящих пакетов, пропускаемых NAT-устройством.

Например, через NAT-устройство проходит несколько однотипных исходящих пакетов, для них создается динамическое правило. Входящие пакеты, параметры которых соответствуют этому динамическому правилу, пропускаются в течение определенного

промежутка времени (таймаута) после прохождения последнего исходящего пакета. По истечении данного промежутка времени динамическое правило удаляется, и NAT-устройство начинает блокировать входящие пакеты.

Это означает, что внешний источник не может инициировать соединение с сетевым узлом, работающим через NAT-устройство. Внутренний узел должен время от времени передавать исходящий трафик внешнему узлу для сохранения динамического правила в активном состоянии.

Для преодоления этой проблемы на сетевом узле, работающем через NAT-устройство, нужно выбрать тип межсетевого экрана **С динамической трансляцией адресов**. Одновременно должен существовать постоянно доступный ViPNet-координатор, расположенный во внешней сети (схема ниже). Назовем его координатором входящих соединений. Координатор входящих соединений должен быть доступен по публичному IP-адресу или через межсетевой экран со статической трансляцией адресов. Координатор входящих соединений не должен работать через тот же межсетевой экран, что и сетевой узел.

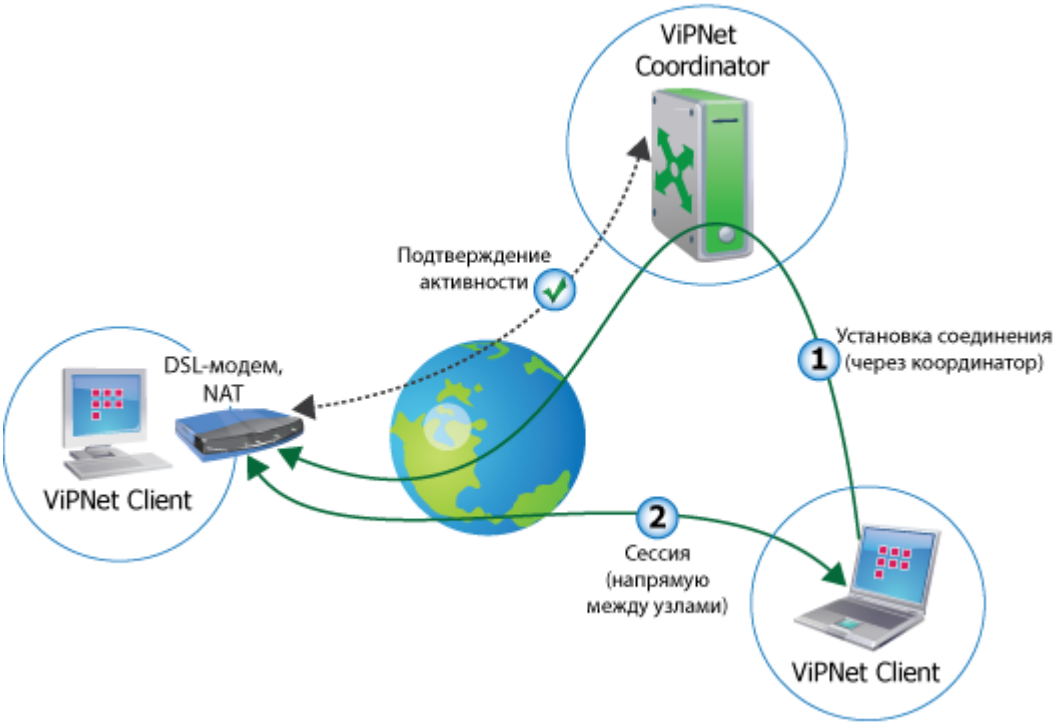


Рисунок 48: Подключение через МЭ с динамической трансляцией адресов

Сетевой узел, работающий через NAT-устройство, периодически отправляет на свой координатор входящих соединений UDP-пакеты, чтобы поддерживать динамическое правило в активном состоянии. По умолчанию период отправки — 25 секунд. Это

позволяет любому внешнему узлу ViPNet в любое время присылать на сетевой узел, работающий через NAT-устройство, IP-пакеты через координатор входящих соединений. При этом ответные исходящие пакеты сетевой узел всегда направляет внешнему узлу напрямую, минуя свой координатор входящих соединений (если внешний узел ViPNet не использует МЭ **С динамической трансляцией адресов**). После получения первого пакета внешний узел, не использующий МЭ **С динамической трансляцией адресов**, также начинает передавать весь трафик напрямую на сетевой узел, работающий через NAT-устройство. Таким образом, образуется прямой обмен UDP-трафиком между узлами ViPNet.

Такая технология позволяет осуществлять постоянный доступ к ViPNet-узлам, работающим через NAT-устройства (так как динамические правила на NAT-устройстве не удаляются). Кроме того, обеспечивается высокая скорость обмена шифрованным трафиком, так как этот обмен использует координаторы входящих соединений только при инициализации, после чего весь обмен трафиком идет напрямую между узлами (схема выше). Следует учитывать, что исходящий трафик от сетевого узла с типом МЭ **С динамической трансляцией адресов** на другой такой же узел всегда идет через координатор входящих соединений другого узла.

Настройка подключения

Чтобы настроить на клиенте подключение через межсетевой экран, на котором невозможно задать статические правила трансляции адресов:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.
2. На левой панели окна **Настройка** выберите раздел **Защищенная сеть**.
3. Убедитесь, что установлен флажок **Использовать межсетевой экран**.
4. Из списка **Тип межсетевого экрана** выберите **С динамической трансляцией адресов**.

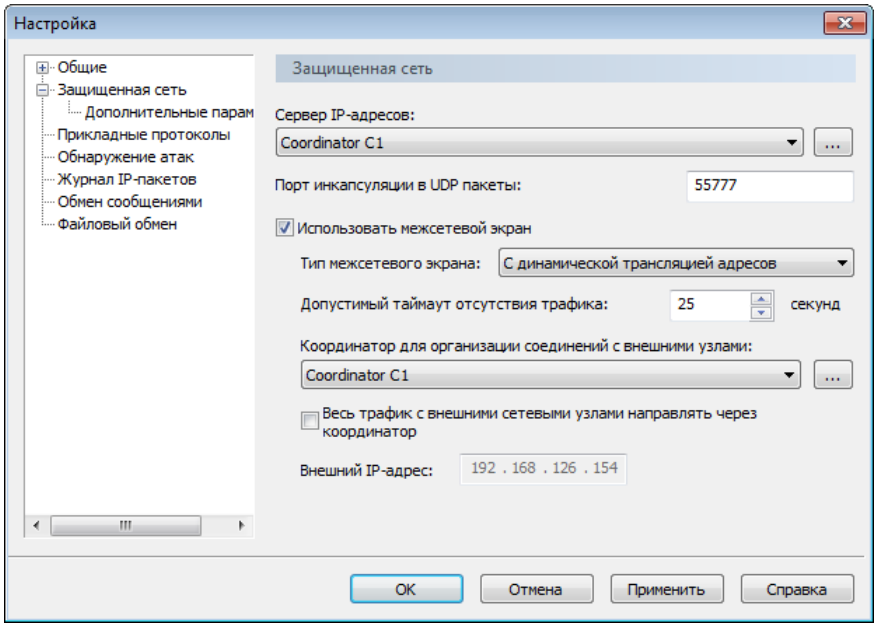


Рисунок 49: Подключение клиента через МЭ с динамической трансляцией адресов

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

Чтобы поддерживать соединение в активном состоянии, клиент периодически посылает UDP-пакеты на свой координатор входящих соединений. По умолчанию интервал отправки пакетов равен 25 секундам. При необходимости это значение можно изменить в поле **Допустимый таймаут отсутствия трафика**. Установленное значение не должно превышать время существования динамического правила на NAT-устройстве.

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

Примечание. Если установлен этот флажок, весь входящий и исходящий трафик будет направляться через координатор входящих соединений. Это может привести к существенному снижению скорости обмена данными. Поэтому данный режим следует использовать только в определенных ситуациях (см. «Особые случаи использования различных типов подключения» на стр. 106).

---

7 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).

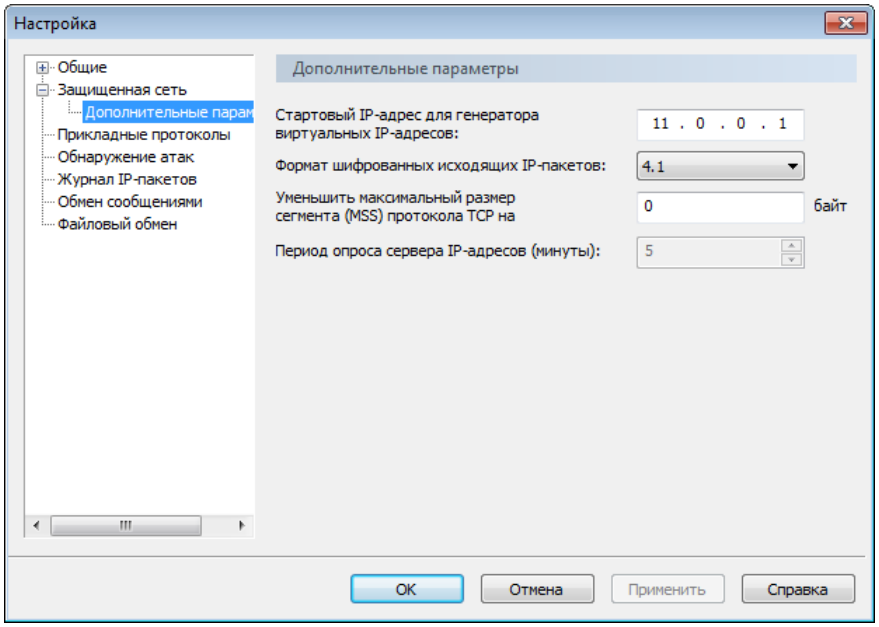


Рисунок 50: Настройка дополнительных параметров

Подключение через межсетевой экран со статической трансляцией адресов

О подключении через межсетевой экран со статической трансляцией адресов

На абонентском пункте данный тип подключения следует использовать только в том случае, если в локальной сети нет координатора или невозможно использовать координатор в качестве межсетевого экрана, а соединение с внешней сетью происходит через межсетевой экран, на котором можно настроить статические правила трансляции адресов.

Рисунок 51: Подключение через МЭ со статической трансляцией адресов

Для правильной работы подключения через межсетевой экран **Со статической трансляцией адресов** адрес используемого межсетевого экрана должен быть указан в сетевых настройках ОС абонентского пункта в качестве шлюза по умолчанию. На межсетевом экране следует настроить статические правила трансляции адресов:

- Пропускать исходящие UDP-пакеты с адресами и портами абонентских пунктов, находящихся за межсетевым экраном;
- Пропускать и перенаправлять входящие UDP-пакеты с портом назначения, заданным в настройках абонентских пунктов.

Внимание! Если несколько абонентских пунктов используют один и тот же межсетевой экран со статической трансляцией адресов, для каждого абонентского пункта должен быть назначен собственный номер порта UDP. В случае использования несколькими абонентскими пунктами одного и того же порта возникают конфликты.

Настройка подключения

Чтобы настроить подключение абонентского пункта через межсетевой экран со статической трансляцией адресов:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.
2. На левой панели окна **Настройка** выберите раздел **Защищенная сеть**.
3. Установите флажок **Использовать межсетевой экран**.
4. Из списка **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 сетевых узлов ViPNet подключены через один межсетевой экран. Каждый сетевой узел должен иметь собственный номер порта.

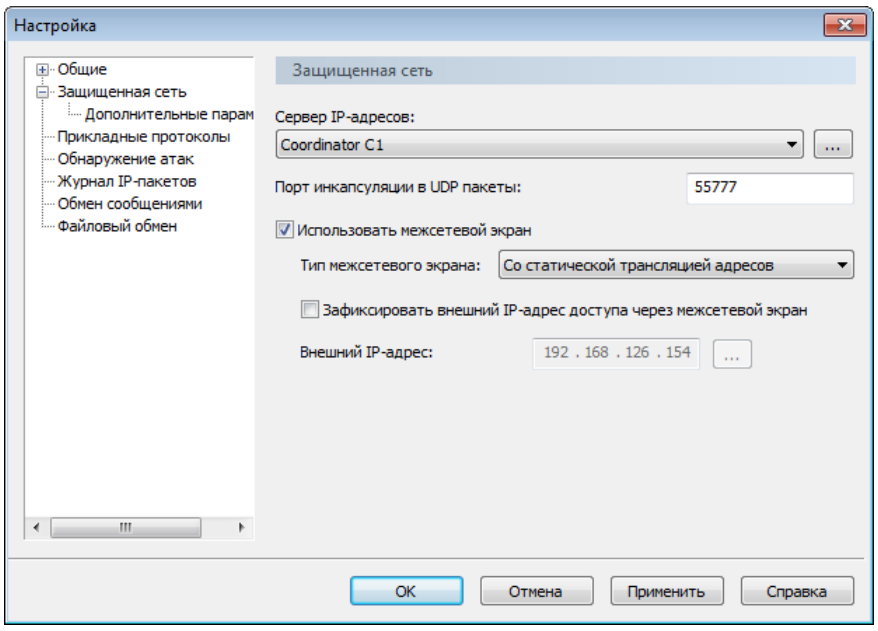


Рисунок 52: Подключение клиента через МЭ со статической трансляцией адресов

6 При необходимости установите флажок **Зафиксировать внешний IP-адрес доступа через межсетевой экран** и выберите требуемый IP-адрес из списка **Внешний IP-адрес**.

Рекомендуется использовать эту настройку, только если межсетевой экран имеет несколько внешних адресов и требуется направлять входящие пакеты через определенный адрес независимо от того, с какого адреса были отправлены исходящие пакеты (см. «Фиксирование внешнего IP-адреса доступа через межсетевой экран» на стр. 104).

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).

Особые случаи использования различных типов подключения

В некоторых случаях необходимо выбрать тип подключения, не соответствующий рекомендациям предыдущих разделов.

Если абонентский пункт доступен по публичному IP-адресу и для него выбран тип межсетевого экрана **Со статической трансляцией адресов** (при этом ни в коем случае не рекомендуется фиксировать внешний адрес доступа), то все остальные связанные с ним сетевые узлы будут уведомлены о том, что этот абонентский пункт будто бы использует несуществующий межсетевой экран. В этом случае абонентский пункт будет доступен по виртуальному IP-адресу (см. «Виртуальные IP-адреса» на стр. 109) и все его соединения с другими сетевыми узлами будут осуществляться только по протоколу UDP. Это бывает удобно, так как некоторые интернет-провайдеры могут блокировать соединения по протоколу IP/241. Тот же результат (возможность использовать виртуальные адреса) можно получить, используя межсетевой экран **С динамической трансляцией адресов**, однако это порождает дополнительный трафик через сервер IP-адресов. Поэтому для перехода к использованию виртуальных адресов первый вариант предпочтительнее.

Если сетевой узел находится в одном сегменте сети с координатором, который установлен на границе этого сегмента, то целесообразно установить для этого сетевого узла режим работы через координатор (использовать этот координатор в качестве межсетевого экрана). Вместе с тем, сетевые узлы будут работоспособны, если выбрать для них подключение через межсетевой экран **С динамической трансляцией адресов** или **Со статической трансляцией адресов**. В этом случае сетевые узлы, которые могут обмениваться между собой широковещательными пакетами, будут устанавливать соединения друг с другом только по реальным IP-адресам. Для обмена шифрованным трафиком с сетевыми узлами ViPNet, которые недоступны для широковещательных пакетов, в качестве шлюза по умолчанию в сетевых настройках ОС Windows на абонентских пунктах требуется задать координатор, находящийся на границе сегмента сети. Это позволяет опытному администратору создавать различные правила маршрутизации для сегментирования сети и организации разграничения доступа к информации по IP-адресу.

Если удаленные пользователи (например, работающие из дома) подключаются к сети через различные межсетевые экраны (на которых невозможно задать статические правила трансляции адресов), им следует выбрать тип межсетевого экрана **С динамической трансляцией адресов** и установить флажок **Весь трафик с внешними сетевыми**

узлами направлять через координатор. В результате взаимодействие с сетевыми узлами ViPNet будет более стабильным, хотя при этом возможно некоторое замедление обмена данными за счет концентрации трафика на сервере IP-адресов.

Настройка доступа к узлам сети ViPNet

Виртуальные IP-адреса

О виртуальных IP-адресах

Технологию виртуальных адресов следует использовать, когда участвующие в соединении сетевые узлы из разных подсетей имеют одинаковые частные IP-адреса. Такие ситуации случаются часто, так как многие устройства (точки доступа Wi-Fi, xDSL и другие) вынуждают использовать в локальных сетях стандартные частные адреса типа 192.168.x.x. Виртуальные адреса позволяют эффективно решить эту проблему.

Также виртуальные адреса 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 передает его приложению после подстановки вместо реального адреса отправителя соответствующего виртуального адреса. 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, с которым он связан. Число формируемых виртуальных адресов зависит от числа реальных адресов и числа туннелируемых адресов узла. Виртуальные адреса никак не зависят от реальных адресов и определяются уникальными идентификаторами сетевых узлов.

Каждый сетевой узел имеет свой собственный список виртуальных адресов для других узлов ViPNet и туннелируемых 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 и так далее).

По умолчанию сетевой узел использует виртуальные адреса для соединения с другими сетевыми узлами, если эти узлы работают через межсетевой экран (см. «Принципы осуществления соединений в сети ViPNet» на стр. 88). Реальные IP-адреса всегда используются для соединения с узлами, от которых данный узел получает широковещательные пакеты, а также в ряде других случаев, когда не ожидается конфликта IP-адресов.

Сетевой узел автоматически начинает взаимодействовать с другим узлом по реальным адресам, если этот узел перестает использовать межсетевой экран либо от него поступают широковещательные пакеты.

Рассмотрим следующий пример. Сетевой узел А соединяется с сетевым узлом В по реальному IP-адресу. Затем узел В меняет тип подключения к сети и начинает использовать межсетевой экран. Узел А начнет автоматически устанавливать соединения с узлом В по виртуальному адресу, только если в настройках узла А включено использование виртуального адреса для узла В.

По умолчанию сетевые узлы ViPNet для соединения с туннелируемыми узлами всегда используют реальные адреса. Чтобы начать использование виртуальных адресов, нужно вручную включить соответствующую функцию.

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.

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 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 и туннелируемые адреса не будут удалены.

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

- Значение первого 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.

При обновлении адресных справочников, при изменении реальных адресов какого-либо узла или при добавлении одиночного туннелируемого адреса сформированные виртуальные адреса не изменяются. 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

На абонентском пункте достаточно настроить параметры доступа только для сервера IP-адресов. Если возможно установить соединение с сервером IP-адресов, то все необходимые параметры доступа к другим сетевым узлам автоматически запрашиваются у сервера IP-адресов.

Примечание. Если IP-адреса и параметры подключения координаторов были заданы в программе ViPNet Administrator или ViPNet Manager, то в программе ViPNet Монитор на сетевом узле не требуется выполнять никаких дополнительных настроек.

Чтобы настроить параметры доступа к защищенному узлу ViPNet, 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** откройте вкладку **IP-адреса**.
4. Чтобы добавить IP-адрес:
   - В группе **IP-адреса** нажмите кнопку **Добавить**.
   - В окне **IP-адрес** укажите реальный адрес сетевого узла.
   - Нажмите кнопку **OK**.

   Введенный IP-адрес будет добавлен в список. Автоматически новому адресу будет сопоставлен виртуальный IP-адрес (см. «Виртуальные IP-адреса» на стр. 109).
5. Если возможен конфликт между указанным IP-адресом и адресами локальной подсети, установите флажок **Использовать виртуальные IP-адреса**.

Примечание. Если сетевой узел, для которого указывается IP-адрес, находится в локальной подсети и для доступа к нему не используется межсетевой экран, использование виртуальных IP-адресов невозможно.

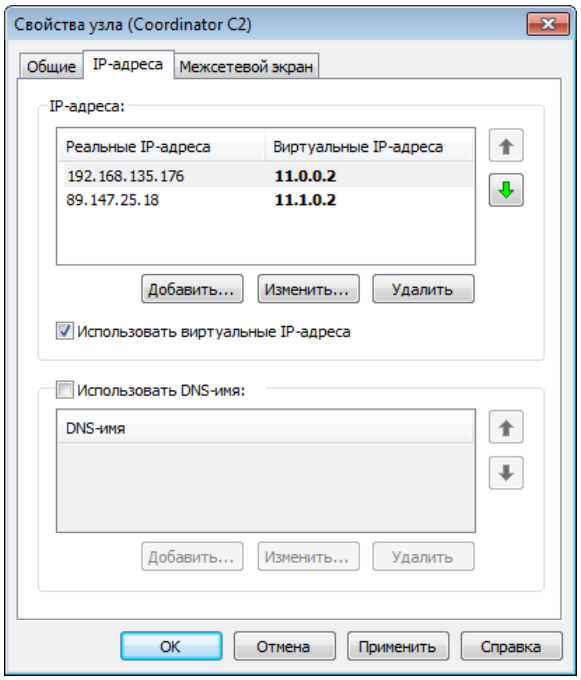


Рисунок 53: IP-адреса сетевого узла

6 Если для доступа к сетевому узлу необходимо использовать DNS-имя:

- Установите флажок **Использовать DNS-имя**.
- Под списком **DNS-имя** нажмите кнопку **Добавить**.
- В окне **DNS-имя** введите DNS-имя сетевого узла и нажмите кнопку **OK**.

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**.

Для абонентского пункта 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 содержится в разделе Настройка и использование служб имен DNS и WINS в сети ViPNet(на стр. 164).

7 Если для доступа к сетевому узлу используется межсетевой экран, откройте вкладку **Межсетевой экран**.

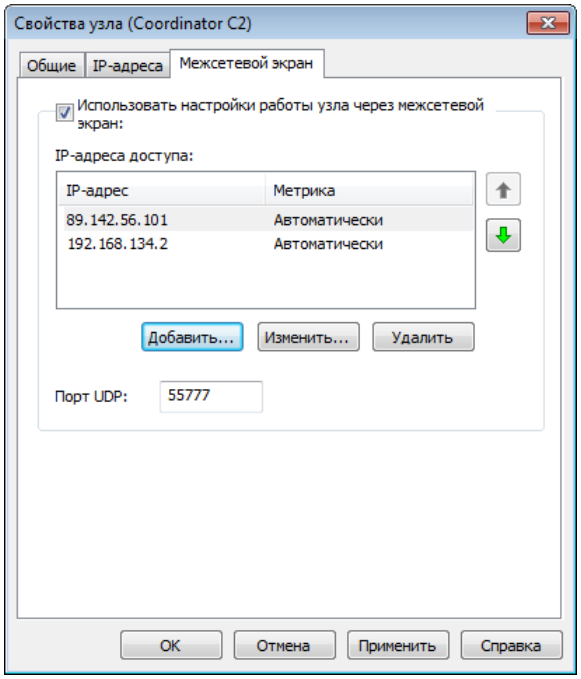


Рисунок 54: Настройка доступа к узлу через межсетевой экран

На вкладке **Межсетевой экран** выполните следующие действия:

- Установите флажок **Использовать настройки работы узла через межсетевой экран**.
- Нажмите кнопку **Добавить**.
- В окне **IP-адрес** укажите IP-адрес межсетевого экрана, используемого для доступа к сетевому узлу, и нажмите кнопку **OK**.
- Если необходимо, добавьте дополнительные IP-адреса.

  Если для координатора указано несколько IP-адресов доступа через межсетевой экран, для этих адресов можно задать метрики (см. «Настройка приоритета IP-адресов доступа к координатору» на стр. 119).
- В поле **Порт UDP** укажите порт доступа через межсетевой экран.

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

Использование псевдонимов для защищенных узлов

Для удобства восприятия 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 **Настройки**.
- В окне **Настройка** в разделе **Общие** установите флажок **Отображать псевдонимы ViPNet-пользователей**.

Чтобы воспользоваться созданными псевдонимами пользователей сети ViPNet на других сетевых узлах:

1. На компьютере, где уже созданы псевдонимы, выполните экспорт псевдонимов в файл:
   - **1.1** В программе ViPNet Монитор в меню **Сервис** выберите пункт **Экспорт псевдонимов**.
   - **1.2** Укажите путь к файлу, в котором будут сохранены псевдонимы.
2. Отправьте файл экспорта пользователям сети ViPNet, которые будут использовать псевдонимы на своих сетевых узлах.
3. Выполните импорт файла псевдонимов:

3.1 В программе ViPNet Монитор в меню **Сервис** выберите пункт **Импорт псевдонимов**.

3.2 Укажите путь к файлу, в котором сохранены псевдонимы.

Настройка доступа к туннелируемым узлам

Примечание. Если настройки параметров туннелирования для всех координаторов были сделаны в программе ViPNet Administrator или ViPNet Manager, то в программе ViPNet Монитор на сетевом узле не требуется выполнять никаких дополнительных настроек. Сетевой узел сможет устанавливать соединения с туннелируемыми узлами.

Чтобы настроить соединение сетевого узла ViPNet с туннелируемыми узлами:

1. В окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**.
2. В разделе **Защищенная сеть** дважды щелкните координатор, который осуществляет туннелирование требуемого открытого узла.
3. В окне **Свойства узла** на вкладке **Туннель** установите флажок **Использовать IP-адреса для туннелирования**.

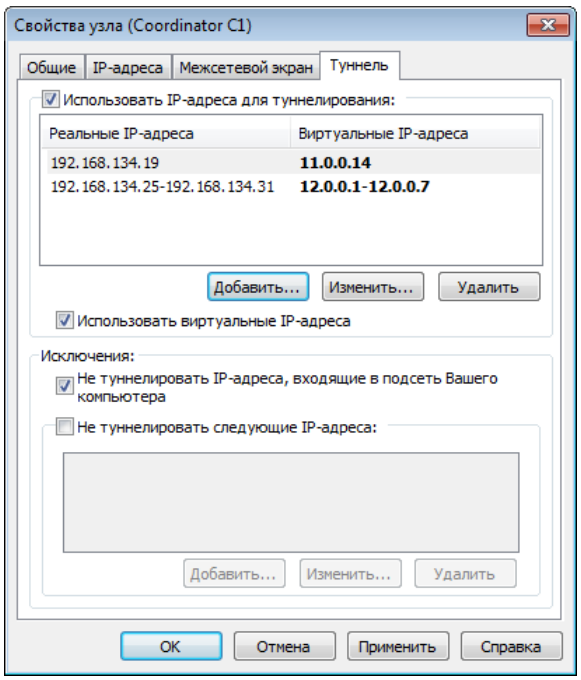


Рисунок 55: Адреса туннелируемых узлов

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. 112). Следует иметь в виду, что на первом месте в этом списке должно стоять зарегистрированное на DNS-сервере имя координатора.

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

5 Если абонентский пункт когда-либо работает удаленно и при этом должен устанавливать соединение с туннелируемыми узлами в своей (исходной) сети, IP-адреса этих ресурсов следует добавить в список туннелируемых адресов. В этом случае должен быть установлен флажок **Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера**. Иначе соединение между абонентским пунктом и туннелируемым узлом будет невозможно, если они находятся в одной подсети.

6 Если при соединении с какими-либо 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.

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 пакетов при выполнении опроса для определения доступности адреса. Соединение устанавливается по тому адресу, доступность которого быстрее определяется в результате опроса.

- Опросы осуществляются периодически, период задается на координаторе в окне **Настройка** в разделе **Защищенная сеть > Дополнительные параметры**. По умолчанию период опроса других координаторов равен 15 минутам, период опроса координатора абонентскими пунктами 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 проверкой наличия соединения по выбранному каналу.

- При запуске программы ViPNet Монитор и при проверке соединения с координатором (см. «Проверка соединения с сетевым узлом» на стр. 202) всегда осуществляется проверка доступности всех каналов связи с целью выбора для работы с координатором канала с наименьшей метрикой.

- 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. 112).

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

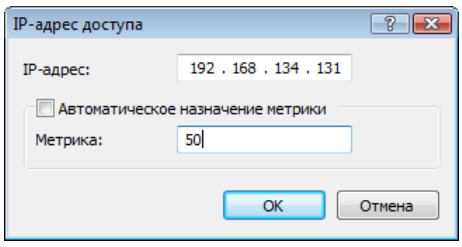


Рисунок 56: Назначение метрики

6 Чтобы метрика определялась автоматически, установите флажок **Автоматическое назначение метрики.**

   Чтобы изменить метрику, снимите флажок **Автоматическое назначение метрики** и в поле **Метрика** введите значение метрики в миллисекундах (допустимые значения от 1 до 9999).

7 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.

4

Интегрированный сетевой экран

Основные принципы фильтрации трафика

Фильтрации подвергается весь трафик, который проходит через сетевой узел:

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

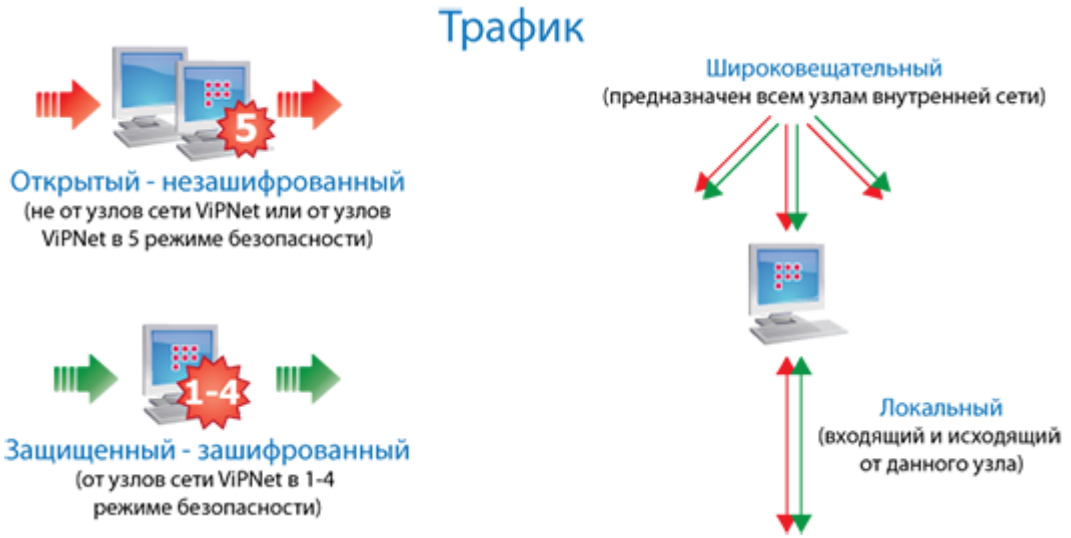


Рисунок 57: Виды трафика, для которых устанавливаются различные правила фильтрации

Примечание. В ПО ViPNet локальными и широковещательными называются следующие типы IP-пакетов:

- IP-пакет называется **локальным** для некоторого сетевого узла, если этот сетевой узел является отправителем или получателем данного пакета.
- IP-пакет называется **широковещательным**, если IP-адрес или MAC-адрес назначения данного пакета является широковещательным адресом.

Для того чтобы правильно настроить правила фильтрации, необходимо понимать основные принципы фильтрации трафика различного типа:

1 Наибольшую опасность представляет трафик из открытой сети, где источник атаки бывает очень сложно обнаружить. Также непросто принять адекватные оперативные

меры по пресечению атаки. Поэтому открытый трафик подвергается последовательной комплексной фильтрации.

Правила фильтрации открытого IP-трафика являются результатом действия:

- выбранного режима безопасности (см. «Режимы безопасности» на стр. 128);
- списка правил фильтрации трафика для соединений (см. «Правила фильтрации трафика» на стр. 131);
- системы обнаружения атак (см. «Настройка системы обнаружения атак» на стр. 144).

Инициализация ViPNet-драйвера выполняется на начальном этапе загрузки Windows, то есть до инициализации остальных служб и драйверов операционной системы. Работа ViPNet-драйвера до авторизации пользователя ViPNet (см. «Способы аутентификации пользователя» на стр. 75) не зависит от настроек фильтров открытой сети, а определяется текущим режимом безопасности и рядом фильтров по умолчанию, необходимых для работы сетевых служб, которые запускаются до авторизации пользователя ViPNet:

- В первом режиме блокируется весь открытый IP-трафик без исключений.
- Во втором режиме блокируется весь IP-трафик, за исключением следующих соединений:
  - Все соединения для работы службы DHCP вне зависимости от направления соединения по протоколу UDP и портам источника и назначения 67-68.
  - Исходящие соединения netbios-ns по протоколу UDP с портами источника и назначения 137.
  - Исходящие соединения netbios-dgm по протоколу UDP с портами источника и назначения 138.
  - Исходящие соединения для работы службы DNS по протоколу UDP с любым портом источника и 53 портом назначения.
- В третьем режиме пропускаются все исходящие соединения и входящие соединения службы DHCP (протокол UDP, порты источника и назначения 67-68).
- В четвертом режиме разрешен весь открытый IP-трафик, защита снята.

Подробнее о режимах безопасности см. раздел Режимы безопасности(на стр. 128).

Фильтрация трафика осуществляется с учетом установленных соединений. Соединение устанавливается, когда в соответствии с правилами фильтрации трафика пропускается входящий или исходящий IP-пакет. Параметры такого IP-пакета регистрируются. На основании этих параметров создается временное правило для пропускания последующих пакетов в прямом и обратном направлении. Правило существует, пока есть трафик, соответствующий параметрам данного соединения.

Кроме того, в рамках созданного соединения по протоколам TCP, UDP, ICMP всегда пропускаются следующие ICMP-сообщения об ошибках:

- тип 3 — адресат недоступен;
- тип 4 — замедление источника;
- тип 11 — истечение времени;
- тип 12 — неверный параметр.

Если в течение определенного промежутка времени пакеты, соответствующие параметрам данного соединения, не поступают, соединение разрывается.

Если входящий или исходящий пакет не соответствует ни одному правилу в рамках соединения и ни одному из заданных пропускающих правил, то пакет блокируется. Такой метод контроля обеспечивает высокий уровень безопасности, позволяя открывать минимальное число протоколов и портов для доступа к открытым ресурсам своей сети. Таким образом, 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.

Открытый IP-пакет проходит проверку на соответствие различным правилам в следующей последовательности:

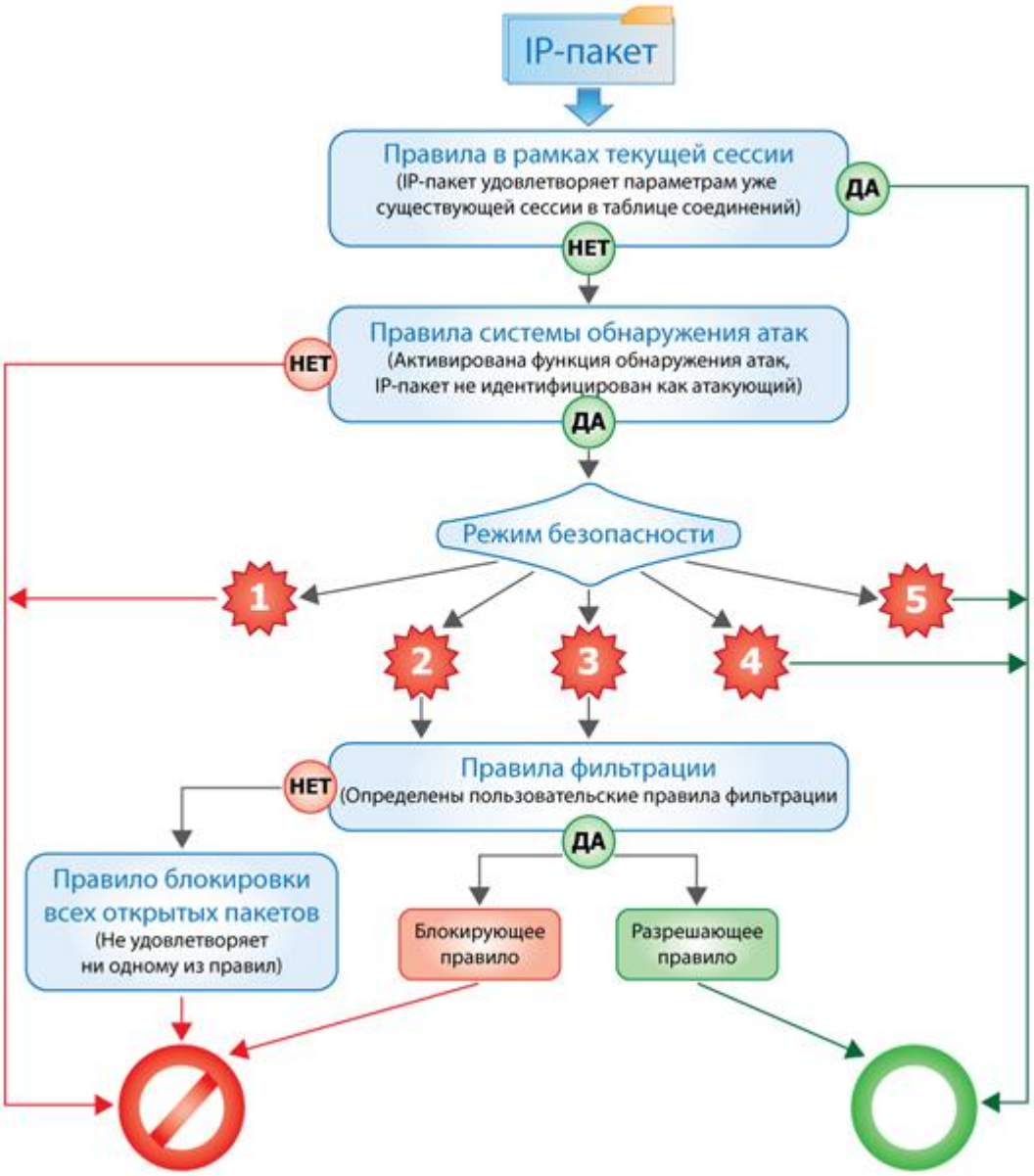


Рисунок 58: Уровни фильтрации открытого трафика

1.1 Правила в рамках уже существующих соединений. Если для пакета в таблице соединений есть подходящее правило, то пакет пропускается, иначе – следующая проверка.

1.2 Блокирующие правила системы обнаружения атак. Если обнаружена атака, то пакет блокируется, иначе – следующая проверка.

1.3 Блокирующее правило первого режима безопасности. Если на сетевом интерфейсе включен первый режим, то пакет блокируется, иначе – следующая проверка.

1.4 Правило второго режима безопасности направляет пакет на дальнейшую проверку.

1.5 Пропускающее правило третьего режима безопасности. Если на сетевом интерфейсе включен третий режим и это исходящий локальный пакет, то пакет пропускается, иначе — следующая проверка.

1.6 Пропускающее правило четвертого режима безопасности. Если на сетевом интерфейсе включен данный режим и это локальный пакет, то пакет пропускается, иначе — следующая проверка.

1.7 Пропускающее правило пятого режима безопасности. Если на сетевом интерфейсе включен данный режим, то пакет пропускается, иначе — следующая проверка.

1.8 Блокирующие и пропускающие правила пользователя. Если пакет соответствует одному из правил фильтрации, заданных пользователем, то пакет пропускается или блокируется в соответствии с этим правилом, иначе – следующая проверка.

1.9 Блокирующее правило для всех открытых пакетов. Пакет, не соответствующий ни одному из предыдущих правил, блокируется.

2 Внутри защищенной сети, благодаря криптографической аутентификации трафика, невозможно провести атаку, источник которой нельзя было бы однозначно идентифицировать и устранить (в том числе в случае атаки на туннелируемый узел со стороны защищенного узла).

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

Поэтому трафик между защищенными узлами проходит только фильтры (см. «Правила фильтрации трафика» на стр. 131), заданные по умолчанию или настроенные пользователем. Эти сетевые фильтры не зависят от сетевого интерфейса, с которого поступил пакет, и определяют правила пропускания трафика для конкретных протоколов, портов и направления передачи. Эти правила в основном предназначены для разграничения прав пользователей защищенных узлов сети ViPNet.

3 Структура фильтров для открытого трафика отличается от структуры фильтров защищенной сети. Подробнее об основных отличиях и структуре сетевых фильтров для открытого и защищенного трафика читайте в разделе Правила фильтрации трафика(на стр. 131).

Режимы безопасности

Режим безопасности определяет основное правило фильтрации открытого IP-трафика. Дополнительные правила фильтрации для определенных IP-адресов, протоколов и портов можно настроить в разделе **Фильтры открытой сети.**

Весь IP-трафик из защищенной сети считается доверенным, поэтому режимы безопасности не влияют на фильтрацию защищенного трафика. По умолчанию разрешены любые соединения с сетевыми узлами ViPNet, с которыми у данного абонентского пункта есть связь, вне зависимости от текущего режима безопасности.

При работе в открытой сети рекомендуется использовать один из трех режимов безопасности:

- Первый режим безопасности (**Блокировать IP-пакеты всех соединений**). Блокируется весь IP-трафик независимо от того, какие правила фильтрации заданы в разделе **Фильтры открытой сети**. Данный режим обеспечивает максимальный уровень защиты компьютера и эквивалентен физическому отключению компьютера от открытой сети. Абонентский пункт будет доступен только для защищенных сетевых узлов.

- Второй режим безопасности (**Блокировать все соединения кроме разрешенных**). Взаимодействие с любыми ресурсами открытой сети невозможно без создания специального правила фильтрации в разделе **Фильтры открытой сети**. По умолчанию разрешены лишь некоторые безопасные типы трафика, позволяющие компьютеру получить IP-адрес и подготовиться к работе в сети. Взаимодействие с другими сетевыми узлами ViPNet возможно без ограничений. Данный режим рекомендуется для опытных пользователей, которым необходима тонкая настройка разрешенных типов трафика.

- Третий режим безопасности (**Пропускать все исходящие соединения кроме запрещенных**). По умолчанию разрешены все соединения, инициируемые с вашего компьютера. Если соединение инициировано извне и не разрешено определенными правилами фильтрации, оно будет заблокировано. Рекомендуется использовать данный режим безопасности на абонентских пунктах, которым требуется безопасное взаимодействие с открытыми ресурсами локальной или внешней сети.

Оставшиеся два режима безопасности следует использовать только в течение короткого времени для тестовых целей:

- Четвертый режим безопасности (**Пропускать все соединения**). Если включен четвертый режим, компьютер не защищен от несанкционированного доступа из сети независимо от того, какие правила фильтрации настроены в разделе **Фильтры открытой сети**.

- Пятый режим безопасности (**Пропускать IP-пакеты без обработки**). В данном режиме отключена любая обработка IP-трафика. Журнал регистрации IP-пакетов не ведется.

По умолчанию установлен третий режим безопасности. Он обеспечивает достаточный уровень защиты и необходимую для работы в сети функциональность.

Изменение режима безопасности

Чтобы изменить режим безопасности, выполните следующие действия:

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

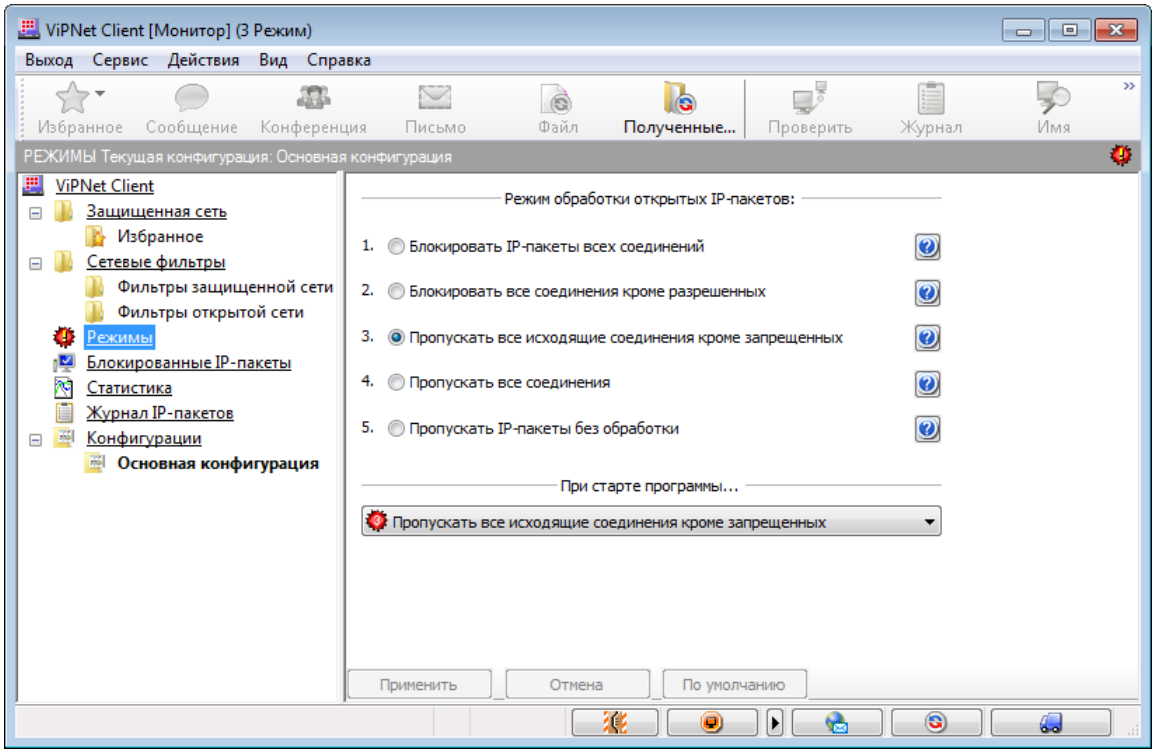


Рисунок 59: Режимы безопасности на абонентском пункте

2 На правой панели выберите требуемый режим безопасности.

3 Если необходимо сменить режим безопасности, устанавливаемый при запуске программы ViPNet Монитор и при загрузке компьютера, из списка **При старте программы** выберите требуемый режим.

Примечание. При смене конфигурации устанавливается тот режим безопасности, который был выбран в списке **При старте программы** в момент сохранения конфигурации (см. «Управление конфигурациями программы» на стр. 227).

4 Нажмите кнопку **Применить**.

5 Чтобы восстановить режим безопасности по умолчанию (третий), нажмите кнопку **По умолчанию**, затем нажмите кнопку **Применить**.

Режим безопасности можно изменить с помощью контекстного меню, щелкнув правой кнопкой мыши значок ViPNet Монитор в области уведомлений.

Примечание. Если установить четвертый или пятый режим безопасности при работе в операционной системе Windows XP SP2 (или более поздней версии Windows), Центр обеспечения безопасности Windows сообщит, что сетевой экран ViPNet Firewall выключен (если уведомления центра обеспечения безопасности не отключены)

Правила фильтрации трафика

Чтобы блокировать или пропускать IP-пакеты в зависимости от IP-адреса отправителя, используемого протокола или порта, требуется настроить фильтрацию сетевого трафика.

Общие сведения о сетевых фильтрах

Сетевые фильтры создаются отдельно для защищенного и открытого трафика. С помощью фильтров для открытой сети на защищенном узле можно разрешить либо запретить обмен IP-пакетами определенного типа с открытыми узлами, то есть с узлами, на которых не установлено программное обеспечение ViPNet с функцией шифрования трафика.

Примечание. К открытым узлам относятся также компьютеры с программным обеспечением ViPNet CryptoService и ViPNet Registration Point.

С помощью фильтров защищенной сети можно ограничить обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел имеет связь. По умолчанию любые соединения с защищенными узлами разрешены фильтром **<Все защищенные узлы>** (см. «Фильтры защищенной сети, настроенные по умолчанию» на стр. 133).

Списки сетевых фильтров представлены на правой панели в окне **ViPNet Client [Монитор]** в разделах **Фильтры защищенной сети** и **Фильтры открытой сети**.

Сетевые фильтры в программе ViPNet Client имеют следующие особенности:

- Фильтры защищенной сети и фильтры открытой сети разделены на группы:
  - **Локальные фильтры** определяют правила фильтрации для нешироковещательных IP-пакетов, которыми сетевой узел обменивается с внешними сетевыми устройствами.
  - **Широковещательные фильтры** определяют правила фильтрации пакетов, адреса назначения которых являются широковещательными. Такие адреса используются для рассылки пакетов на все компьютеры в локальной сети.

  Настройки фильтров в каждой группе независимы друг от друга.

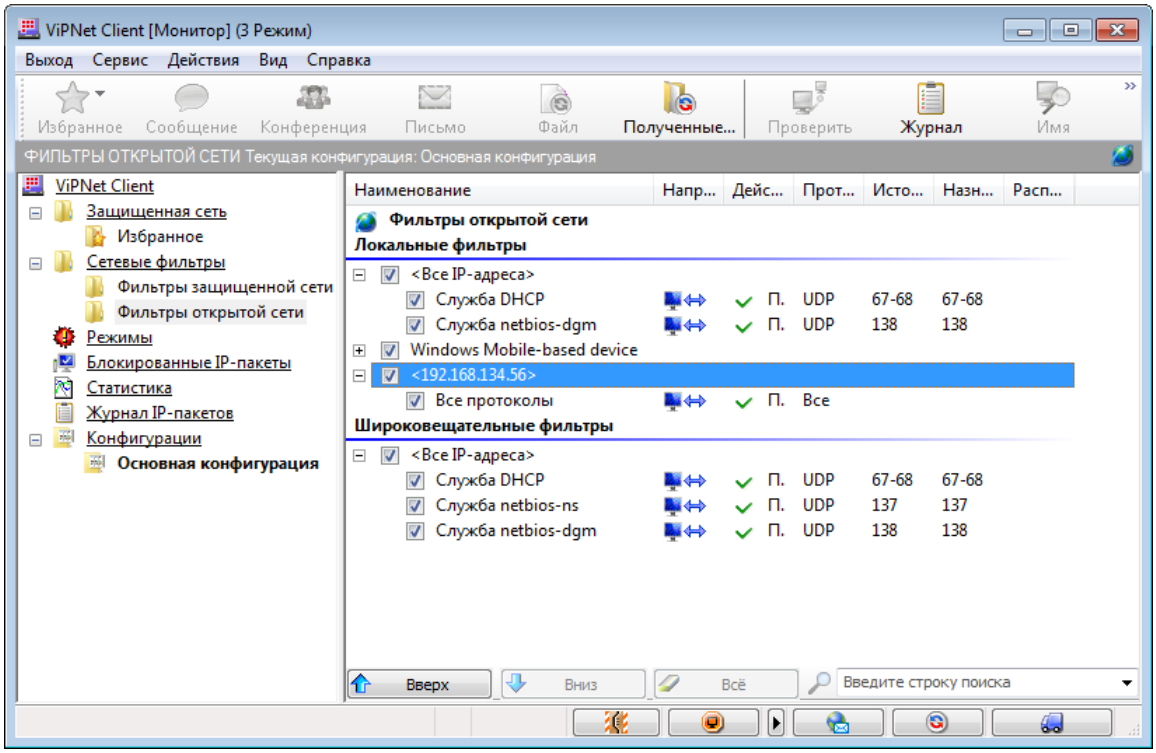


Рисунок 60: Фильтры открытой сети в ViPNet Client

- Сетевые фильтры имеют двухуровневую структуру.

  На первом уровне находятся правила, в которых задается список IP-адресов или защищенных узлов ViPNet, на которые распространяется действие фильтров, создаваемых на втором уровне.

  Фильтры привязаны к конкретным правилам и определяют действие, применяемое к IP-пакетам, в соответствии с заданными параметрами: протокол, порты, типы, коды, направление соединения, расписание действия данного фильтра.

- Действие правила определяется фильтрами. Фильтры могут пропускать (✓) или блокировать (✗) IP-пакеты, соответствующие заданным параметрам.

  Чтобы изменить действие правила, двойным щелчком откройте фильтр и из списка **Действие фильтра** выберите требуемое значение (см. «Создание фильтров» на стр. 140).

  Правило включено, если установлен флажок рядом с именем правила (☑). Если флажок снят (☐), то правило отключено. То же самое относится к фильтрам. Чтобы включить или отключить правило или фильтр, установите или снимите соответствующий флажок.

- Внутри каждой группы IP-пакеты проверяются на соответствие правилам по порядку сверху вниз, в соответствии с расположением правил в списке. Когда пакет

блокируется или пропускается первым подходящим правилом, последующие правила уже не оказывают никакого влияния на данный пакет. Порядок правил можно изменять с помощью кнопок **Вверх** и **Вниз**, с помощью перетаскивания правила можно перемещать и копировать (при нажатой клавише **Ctrl**).

- Внутри правила IP-пакеты также проверяются на соответствие фильтрам по порядку сверху вниз, в соответствии с положением фильтров в списке. Когда срабатывает первый подходящий фильтр, последующие фильтры не оказывают на данный пакет никакого влияния. Порядок фильтров можно изменять с помощью кнопок **Вверх** и **Вниз**, с помощью перетаскивания фильтры можно перемещать и копировать (при нажатой клавише **Ctrl**).

- При фильтрации открытого трафика всех протоколов установленные соединения имеют приоритет над другими правилами фильтрации. Если был разрешен некоторый трафик в определенном направлении, для пропускания такого трафика создается временное соединение. Автоматически будет пропущен и ответный трафик, удовлетворяющий параметрам данного соединения. При фильтрации защищенного трафика такое правило действует только для протокола TCP.

Фильтры защищенной сети, настроенные по умолчанию

В программе ViPNet Монитор в разделе **Фильтры защищенной сети** по умолчанию заданы следующие правила:

- В группе **Локальные фильтры** правило **<Все защищенные узлы>**. Это правило распространяется на все защищенные узлы сети ViPNet, с которыми связан данный узел, и содержит единственный фильтр **Все протоколы** с действием **Пропускать**, разрешающий любые соединения.

- В группе **Широковещательные фильтры** правило **<Все защищенные узлы>**. Это правило распространяется на все защищенные узлы сети ViPNet, с которыми связан данный узел, и содержит фильтры, разрешающие пропускание входящих и исходящих широковещательных пакетов по следующим протоколам и портам:
  - Служебные пакеты сети ViPNet (UDP, порты 2046, 2048, 2050).
  - Пакеты службы DHCP (UDP, порты 67 и 68), предназначенные для автоматического получения компьютерами IP-адресов.
  - Пакеты netbios-ns (UDP, порт 137) и netbios-dgm (UDP, порт 138), предназначенные для организации работы службы NetBIOS, осуществляющей регистрацию и проверку имен компьютеров в локальной сети.
  - Служебные пакеты кластера ViPNet (UDP, порт 2060). Этот фильтр отображается только при использовании ПО ViPNet Cluster.

Примечание. В версиях программы ViPNet Монитор 3.1.0 и ниже для обеспечения работы службы DHCP служили фильтры bootps и bootpc. Если обновить ViPNet Монитор до текущей версии, эти фильтры останутся в списке и не будут заменены на фильтр службы DHCP.

Фильтры открытой сети, настроенные по умолчанию

В программе ViPNet Client в разделе **Фильтры открытой сети** по умолчанию заданы следующие правила:

- В группе **Локальные фильтры**:
  - **<Все IP-адреса>**. Это правило распространяется на все IP-адреса и содержит фильтры с действием **Пропускать**, разрешающие создание локальных нешироковещательных соединений по следующим протоколам и портам:
    - Пакеты службы DHCP (UDP, порты 67 и 68), предназначенные для автоматического получения компьютерами IP-адресов.
    - Пакеты netbios-dgm (UDP, порт 138), предназначенные для организации работы службы NetBIOS, осуществляющей регистрацию и проверку имен компьютеров в локальной сети.
  - **Windows Mobile-based device**. Это правило содержит фильтры с действием **Пропускать**, предназначенные для обеспечения синхронизации компьютера с КПК (на базе Windows Mobile 5.0/6.x) при помощи ActiveSync 4.x (или с помощью Центра устройств Windows Mobile на Windows Vista и Windows 7). Подробнее см. раздел Синхронизация компьютера с КПК (на стр. 250).
- В группе **Широковещательные фильтры** правило **<Все IP-адреса>.** Это правило распространяется на все IP-адреса и содержит фильтры с действием **Пропускать,** разрешающие пропускание входящих и исходящих широковещательных пакетов по следующим протоколам и портам:
  - Пакеты службы DHCP (UDP, порты 67 и 68), предназначенные для автоматического получения компьютерами IP-адресов.
  - Пакеты netbios-ns (UDP, порт 137) и netbios-dgm (UDP, порт 138), предназначенные для организации работы службы NetBIOS, осуществляющей регистрацию и проверку имен компьютеров в локальной сети.

Примечание. В версиях программы ViPNet Монитор 3.1.0 и ниже для обеспечения работы службы DHCP служили фильтры bootps и bootpc. Если обновить ViPNet Монитор до текущей версии, эти фильтры останутся в списке и

не будут заменены на фильтр службы DHCP.

Создание правил для защищенной сети

Чтобы создать новое правило фильтрации трафика для защищенной сети (см. «Общие сведения о сетевых фильтрах» на стр. 131), выполните следующие действия:

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

2 В разделе **Фильтры защищенной сети** щелкните правой кнопкой мыши заголовок группы фильтров, в которой требуется создать новое правило, и в контекстном меню выберите пункт **Создать правило**.

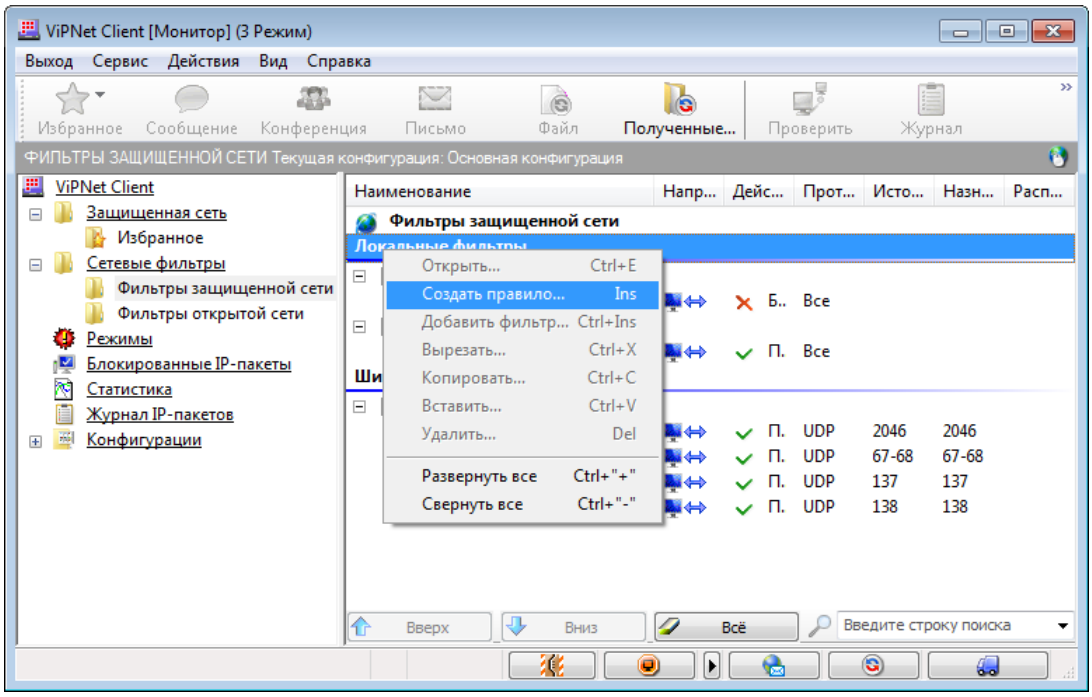


Рисунок 61: Создание правила для защищенной сети

3 В зависимости от того, какая группа правил выбрана, откроется одно из следующих окон: **Широковещательное правило** или **Локальное правило**.

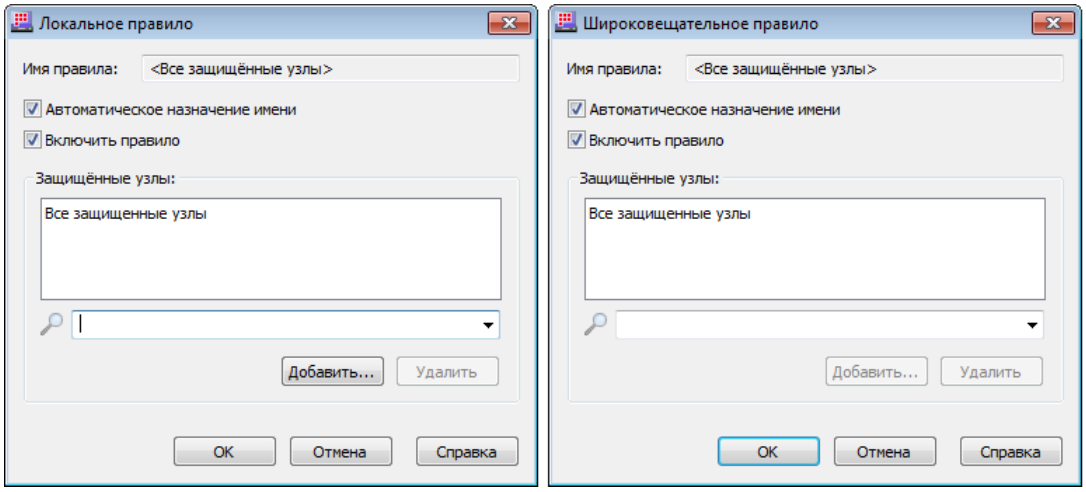


Рисунок 62: Локальное и широковещательное правила для защищенной сети

4 Если требуется самостоятельно задать имя правила, снимите флажок **Автоматическое назначение имени.** По умолчанию имя правила будет назначено автоматически.

5 Убедитесь, что установлен флажок **Включить правило**, иначе созданное правило будет отключено. После создания правила его всегда можно включить или отключить.

6 При создании локального правила в списке **Защищенные узлы** укажите узлы ViPNet, на которые будет распространяться действие правила. По умолчанию правило действует для всех защищенных узлов.

Широковещательное правило можно создать только для всех сетевых узлов, то есть изменить список **Защищенные узлы** для широковещательного правила невозможно.

Чтобы добавить узлы в список:

- Нажмите кнопку **Добавить.**
- В окне **Выбор сетевого узла** укажите один или несколько узлов и нажмите кнопку **Выбрать.**

Чтобы удалить сетевые узлы из списка, выберите их и нажмите кнопку **Удалить.**

7 Для сохранения правила нажмите кнопку **OK**. Сразу после этого откроется окно для добавления фильтра к созданному правилу (см. «Создание фильтров» на стр. 140).

Чтобы отказаться от создания фильтра, нажмите кнопку **Отмена.**

Создание правил для открытой сети

Чтобы создать новое правило фильтрации трафика для открытой сети (см. «Общие сведения о сетевых фильтрах» на стр. 131), выполните следующие действия:

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

2 В разделе **Фильтры открытой сети** щелкните правой кнопкой мыши заголовок группы фильтров, в которой требуется создать новое правило, и в контекстном меню выберите пункт **Создать правило**.

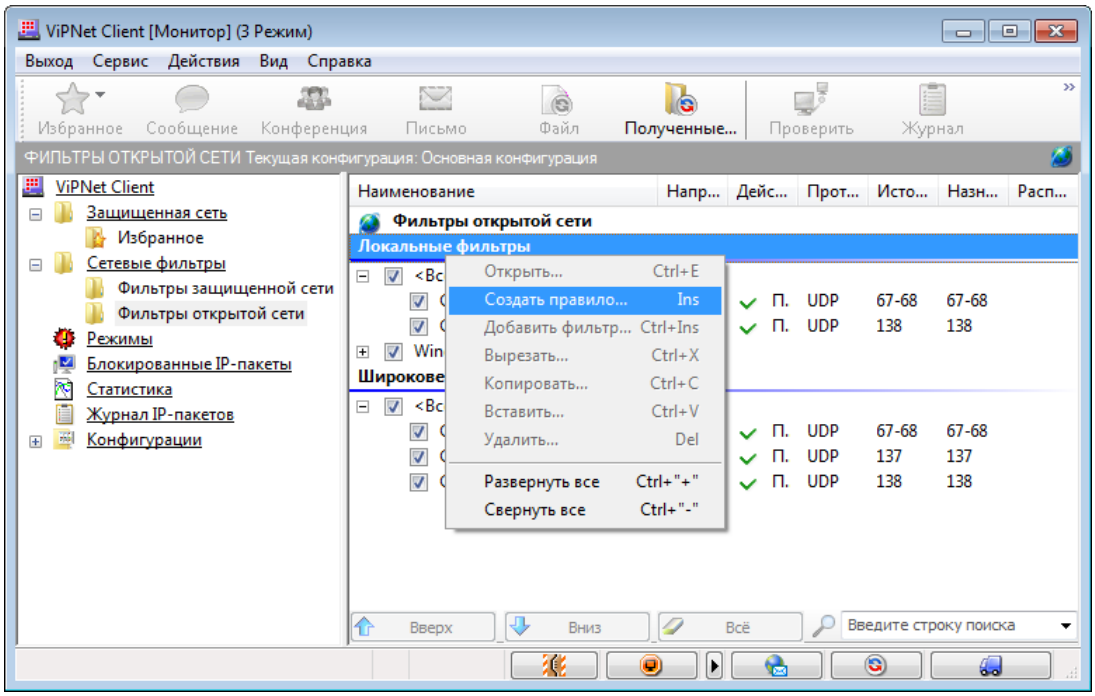


Рисунок 63: Создание нового правила для открытой сети

3 В зависимости от того, какая группа правил выбрана, откроется одно из следующих окон: **Широковещательное правило** или **Локальное правило**.

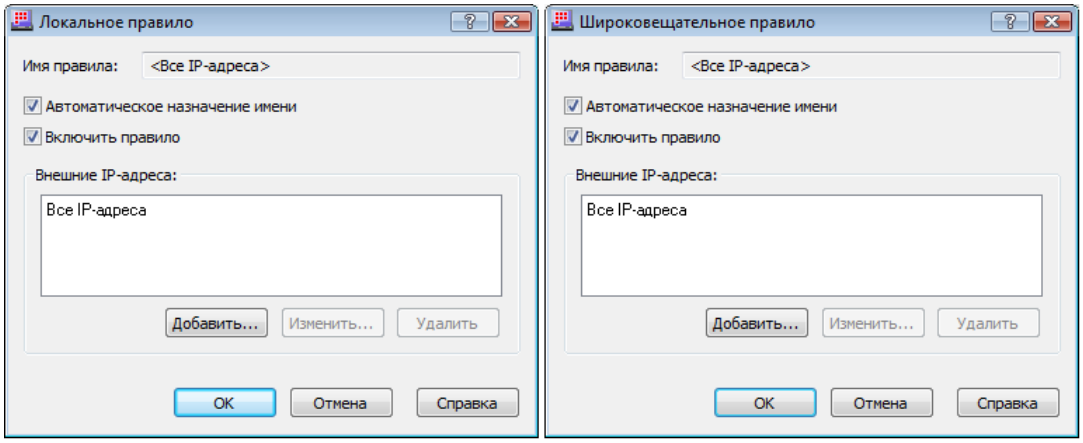


Рисунок 64: Создание локального правила и широковещательного правила в ViPNet Client

4 Если требуется самостоятельно задать имя правила, снимите флажок **Автоматическое назначение имени.** По умолчанию имя правила будет назначено автоматически.

5 Убедитесь, что установлен флажок **Включить правило**, иначе созданное правило будет отключено. После создания правила его всегда можно включить или отключить.

6 Задайте IP-адреса внешних устройств, трафик с которыми должен фильтроваться в соответствии с создаваемым правилом.

Чтобы задать IP-адрес:

- Нажмите кнопку **Добавить.**

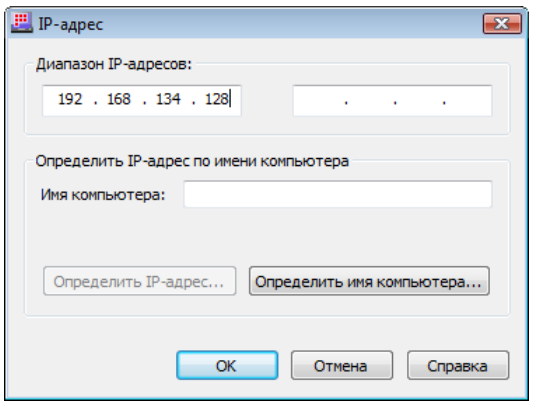


Рисунок 65: Добавление IP-адреса или имени компьютера

- В окне **IP-адрес** выполните одно из действий:

Если известны IP-адреса узлов, которые требуется включить в правило:

- В поле **Диапазон IP-адресов** введите IP-адрес или диапазон IP-адресов для фильтрации. При вводе диапазона IP-адресов задайте начальный и конечный адрес диапазона.
- Чтобы найти имя компьютера по введенному IP-адресу, нажмите кнопку **Определить имя компьютера**. В окне **Определить имя/IP-адрес** нажмите кнопку **Начать поиск**, результат будет отображен в поле **Результаты поиска**.

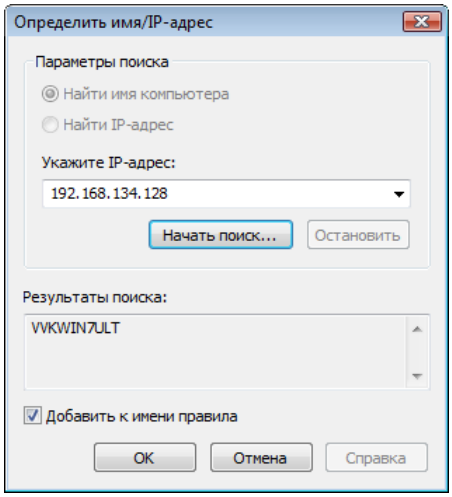


Рисунок 66: Поиск имени компьютера

Если IP-адреса неизвестны, но известны сетевые имена компьютеров или их URL-адреса (для веб-сайтов, FTP-серверов и пр.):

- В поле **Имя компьютера** введите имя или URL-адрес компьютера, трафик с которым должен фильтроваться в соответствии с создаваемым правилом.
- Чтобы найти IP-адрес компьютера по введенному имени, нажмите кнопку **Определить IP-адрес**. В окне **Определить имя/IP-адрес** нажмите кнопку **Начать поиск**, результат будет отображен в поле **Результаты поиска**.

o Задав IP-адреса, нажмите кнопку **OK**. Чтобы выйти без сохранения изменений, нажмите кнопку **Отмена**.

7 Для сохранения правила нажмите кнопку **OK**. Сразу после этого откроется окно для добавления фильтра к созданному правилу (см. «Создание фильтров» на стр. 140).

Чтобы отказаться от создания фильтра, нажмите кнопку **Отмена**.

Создание фильтров

Чтобы добавить к правилу фильтр, выполните следующие действия:

1. Щелкните правой кнопкой мыши правило, к которому требуется добавить фильтр.
2. В контекстном меню выберите пункт **Добавить фильтр**.
3. В зависимости от типа правила, для которого создается фильтр, откроется одно из окон: **Локальный фильтр** или **Широковещательный фильтр**.

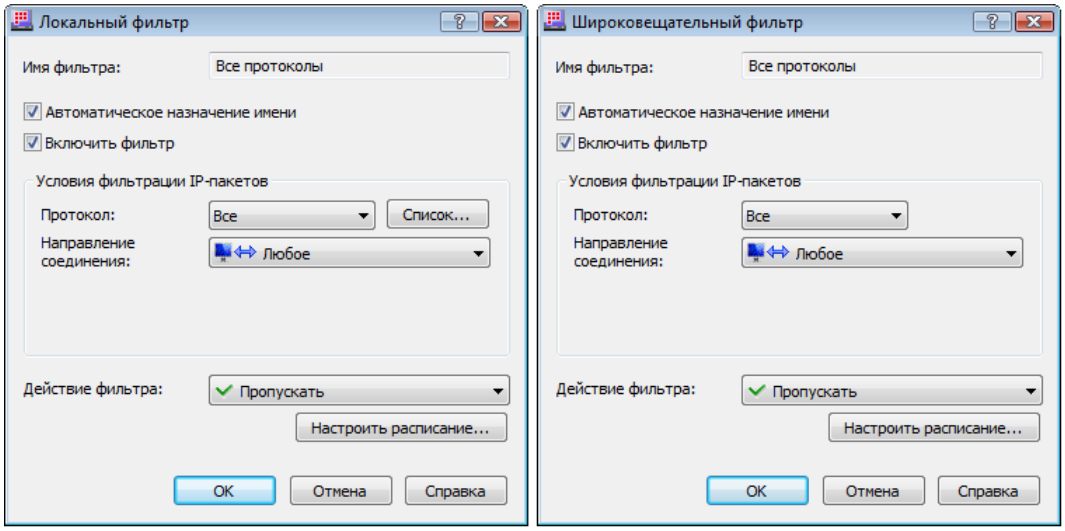


Рисунок 67: Создание фильтров протоколов для локального правила и широковещательного правила

4. Если требуется самостоятельно задать имя фильтра, снимите флажок **Автоматическое назначение имени.** По умолчанию имя фильтра назначается автоматически.
5. Убедитесь, что установлен флажок **Включить фильтр**, иначе созданный фильтр будет отключен. После создания фильтра его можно включить или отключить в любой момент.
6. Задайте параметры фильтра:
   - Из списка **Протокол** выберите протокол для фильтрации. Правило, к которому будет добавлен создаваемый фильтр, будет обрабатывать только IP-пакеты, переданные с помощью указанного протокола. Если требуемый протокол отсутствует в списке, нажмите кнопку **Список** и в открывшемся окне добавьте протокол.
   - Из списка **Направление соединения** выберите направление передачи IP-пакетов. Если выбрать **Любое**, то направление передачи IP-пакетов не будет учитываться при фильтрации.

7 Из списка **Действие фильтра** выберите действие (**Пропускать** или **Блокировать**), которое будет применяться к IP-пакетам, соответствующим параметрам фильтра.

8 Чтобы настроить расписание работы фильтра, нажмите кнопку **Настроить расписание**. С помощью расписания можно задать интервалы активности фильтра.

В окне **Расписание** выполните следующие действия:

- Установите флажок **Использовать расписание действия фильтра**.
- Из списка **Расписание** выберите тип расписания (**Ежедневное** или **Еженедельное**). Если требуется, чтобы фильтр был активен в некоторые дни недели, выберите **Еженедельное** расписание.
- Из списка **Фильтр действует** выберите, когда фильтр будет активен: **В указанное время** или **Все время кроме указанного.**
- Выбрав **Ежедневное** расписание, укажите время начала и время конца интервала.
- Выбрав **Еженедельное** расписание, с помощью флажков укажите, в какие дни недели фильтр должен быть активен. Для каждого из выбранных дней укажите время начала и время конца интервала.
- Выполнив необходимые настройки, нажмите кнопку **OK**.

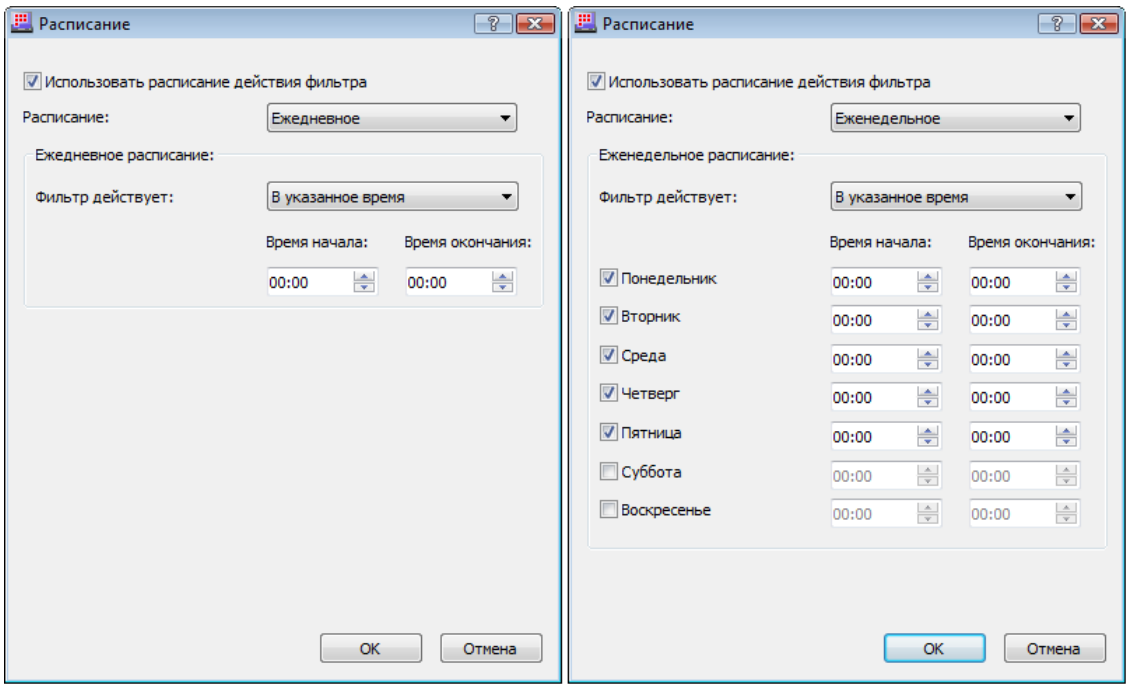


Рисунок 68: Настройка расписания для фильтра протоколов

9 Выполнив настройку фильтра, нажмите кнопку **OK**. Созданный фильтр будет добавлен к выбранному правилу. Если для фильтра настроено расписание работы, справа от его имени отображается значок  .

Практический пример использования сетевых фильтров

Рассмотрим следующий пример использования сетевых фильтров.

Допустим, в компании используется почтовый сервер, на котором установлена программа ViPNet Монитор. Этот почтовый сервер должен иметь возможность обмениваться информацией с внешними узлами для следующих целей:

- Через защищенный почтовый сервер осуществляется обмен сообщениями электронной почты с внешними почтовыми серверами.
- В компании используются системы бесперебойного питания (UPS), позволяющие отправлять на защищенный почтовый сервер определенные сообщения о своем статусе. Установить программное обеспечение ViPNet или настроить туннелирование на данных устройствах не представляется возможным или целесообразным.

Отправка сообщений на почтовый сервер осуществляется по протоколу SMTP. Чтобы организовать обмен сообщениями с внешними почтовыми серверами и прием сообщений от системы бесперебойного питания, на защищенном почтовом сервере необходимо создать сетевые фильтры, разрешающие прием и передачу IP-пакетов по 25-му порту TCP (стандартный порт для протокола SMTP).

Чтобы создать сетевой фильтр для обмена почтовыми сообщениями с внешними адресатами, на защищенном почтовом сервере выполните следующие действия:

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

2 В разделе **Фильтры открытой сети** создайте правило для всех IP-адресов, так как IP-адреса внешних почтовых серверов заранее неизвестны.

Для этого в группе **Локальные фильтры** щелкните правой кнопкой мыши правило **Все IP-адреса** и в контекстном меню выберите пункт **Добавить фильтр**.

Примечание. Если в группе **Локальные фильтры** отсутствует правило **Все IP-адреса**, его необходимо создать (см. «Создание правил для открытой сети» на стр. 137).

3 В окне **Локальный фильтр** укажите следующие параметры:

- В списке **Протокол** выберите значение **TCP**.
- Если в программе ViPNet Монитор выбран второй режим безопасности (см. «Режимы безопасности» на стр. 128), в списке **Направление соединения** выберите значение **Любое**, так как в этом случае необходимо разрешить как входящие соединения, так и исходящие.

  Если в программе ViPNet Монитор выбран третий режим безопасности, в списке **Направление соединения** выберите значение **Входящие**, так как в этом случае исходящие соединения разрешены по умолчанию, требуется разрешить только входящие соединения.
- В списке **Порт источника** выберите значение **Все**.
- В списке **Порт назначения** выберите значение **Номер** и в появившемся справа списке укажите номер порта **25-smtp**.
- В списке **Действие фильтра** сохраните значение по умолчанию — **Пропускать**.

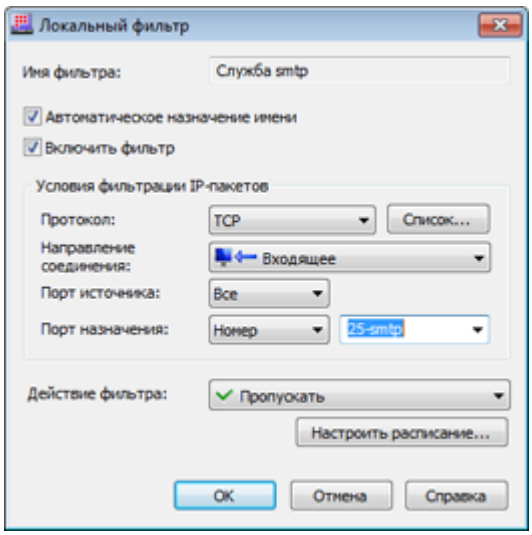


Рисунок 69: Пример настройки разрешающего правила для протокола SMTP

4 Нажмите кнопку **OK**.

Таким образом, на защищенном почтовом сервере организован обмен сообщениями с открытыми узлами по протоколу SMTP.

Настройка системы обнаружения атак

Система обнаружения атак (intrusion detection system, IDS) служит для обнаружения и предотвращения действий злоумышленников («хакеров»), целью которых может быть получение несанкционированного доступа к компьютеру либо вывод его из строя.

Система обнаружения атак работает на сетевом уровне, благодаря чему имеет ряд достоинств:

- Возможность обнаруживать и блокировать сетевые пакеты до обработки их стеком TCP/IP.
- Возможность блокировать на ранней стадии атаки, направленные на перегрузку ОС, приводящие к отказу в обслуживании.

Кроме того, система IDS способна обнаруживать исходящие атаки (как будто злоумышленник находится за вашим компьютером). Это полезно в том случае, если ваша ОС каким-либо образом используется злоумышленником в качестве атаки на какую-либо третью ОС (например, с помощью «троянских» программ).

Если система обнаружения атак обнаружит пакет, соответствующий параметрам одной из типовых атак, этот пакет будет заблокирован. Для пакетов, заблокированных системой обнаружения атак, в **Журнале IP-пакетов** (см. «Работа с журналом IP-пакетов» на стр. 210) указан код события и название предполагаемой атаки.

Для настройки системы обнаружения атак выполните следующие действия:

1. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.
2. На левой панели окна **Настройка** выберите раздел **Обнаружение атак**.

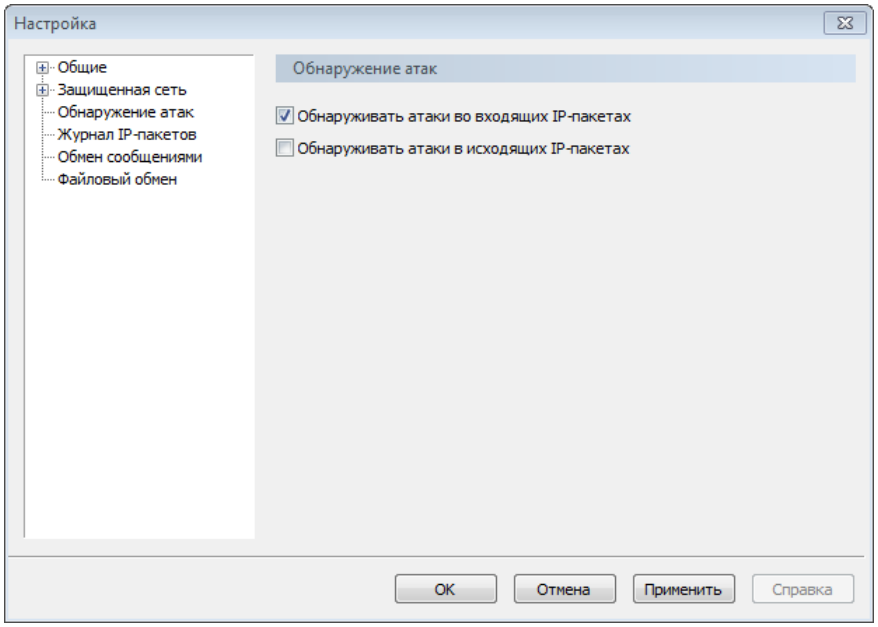


Рисунок 70: Настройка системы обнаружения атак

3 Чтобы включить систему обнаружения атак для входящего трафика, установите флажок **Обнаруживать атаки во входящих IP-пакетах**.

4 Чтобы включить систему обнаружения атак для исходящего трафика, установите флажок **Обнаруживать атаки в исходящих IP-пакетах**.

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

5

Настройка параметров обработки прикладных протоколов

Общие сведения о прикладных протоколах

Функционирование сетевых сервисов, например, таких как, IP-телефония, DNS-служба, FTP-служба, обеспечивается прикладными протоколами, которые регламентируют передачу IP-адреса в теле пакета. Поведение подобного рода может привести к отсутствию сервиса на защищаемых ресурсах в случае использования технологии виртуальных IP-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 разрешающее правило фильтрации, следовательно, соединение будет заблокировано.

Решить перечисленные проблемы позволяет обработка прикладных протоколов, которая обеспечивает:

- Подмену виртуального IP-адреса в теле пакета на реальный IP-адрес в случае использования технологии виртуальных IP-адресов.
- Активацию разрешающего правила фильтрации IP-трафика для дополнительного соединения на случайно выбранный порт, открываемого прикладным протоколом.

Примечание. В программе ViPNet Монитор обработка прикладных протоколов осуществляется для открытого и защищенного трафика.

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 открытой сети и режимом безопасности в программе ViPNet Монитор.

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 зависимости от выбранного режима безопасности необходимо выполнить следующие настройки в программе ViPNet Монитор:

1. Для разрешения управляющего соединения в активном и пассивном режимах при использовании второго режима безопасности следует дополнительно в фильтрах открытой сети (см. «Создание фильтров» на стр. 140) разрешить исходящее соединение на порт 21 FTP-сервера.
2. Для разрешения дополнительного соединения на случайно выбранный порт:
   - В активном режиме при использовании второго или третьего режима безопасности для активации разрешающего правила фильтрации следует включить обработку протокола FTP.
   - В пассивном режиме при использовании второго режима безопасности (см. «Режимы безопасности» на стр. 128) следует включить обработку протокола FTP. При использовании третьего режима безопасности настройка дополнительных правил фильтрации и обработка прикладных протоколов не требуется.

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 необходимо включить обработку протокола SIP и выполнить дополнительные настройки в программе ViPNet Монитор:

1. Чтобы SIP-клиент мог принять запрос на установление сеанса связи или принять ответ на запрос при использовании второго или третьего режима безопасности, в фильтрах открытой сети следует разрешить входящее соединение на порт 5060.
2. Чтобы SIP-клиент мог отправить запрос на установление сеанса связи или ответ на запрос при использовании второго режима безопасности, в фильтрах открытой сети следует разрешить исходящее соединение на порт 5060. При использовании третьего режима безопасности настройка дополнительных правил фильтрации не требуется.

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 NetBIOS разработан в виде интерфейса для обеспечения сетевых операций ввода/вывода и управления соответствующим транспортным протоколом. Работа протокола основана на следующих службах:
  - Служба имен NetBIOS Name Service. Обеспечивает разрешение имен сетевых узлов, использующих NetBIOS, в IP-адреса при обмене данными между приложениями сетевых узлов.
  - Служба датаграмм NetBIOS Datagram Service. Обеспечивает обмен данными без установления прямого подключения и без подтверждения приема между двумя сетевыми узлами, использующими NetBIOS.
  - Служба сессий NetBIOS Session Service. Обеспечивает дуплексный упорядоченный обмен данными с подтверждением приема между двумя сетевыми узлами, использующими NetBIOS.
- Протокол H.323 обеспечивает работу программ для проведения мультимедиаконференций 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, видеозвонков, а также мультимедийной информации.
- Протокол IRC (Internet Relay Chat) позволяет общаться пользователям в режиме реального времени через Интернет с помощью таких IRC-клиентов, как X-Chat, Opera Chat, Konversation, ChatZilla, Pidgin.

- Протокол CU-SeeMe обеспечивает работу программы для проведения видеоконференции в реальном времени через IP-сети, в том числе Интернет. Протокол осуществляет многоклиентскую видеоконференцию с участием сервера конференций, отвечающего за распределение видеовызовов между ее участниками. А также позволяет проводить видеоконференцию между двумя CU-SeeMe-клиентами, не используя при этом сервер.

Примечание. Список поддерживаемых программой ViPNet Монитор прикладных протоколов задан по умолчанию, нельзя добавить протоколы или удалить протоколы из списка.

Настройка параметров обработки прикладных протоколов

Примечание. В программе ViPNet Монитор настройка параметров обработки прикладных протоколов осуществляется для открытого и защищенного видов трафика.

Чтобы выполнить настройку параметров обработки прикладного протокола:

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

2 На левой панели окна **Настройка** выберите раздел **Прикладные протоколы**.

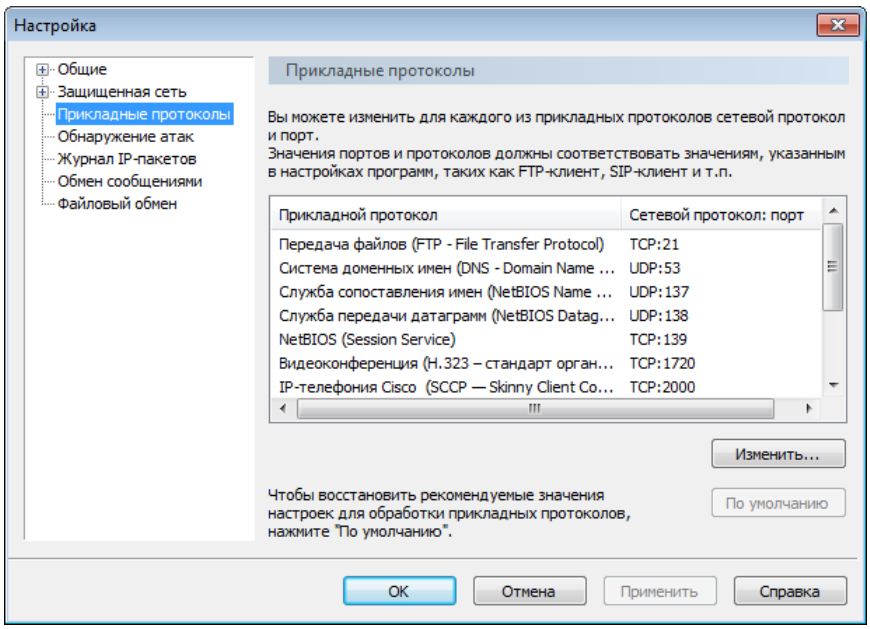


Рисунок 71: Раздел «Прикладные протоколы»

В разделе **Прикладные протоколы** приведен список поддерживаемых программой прикладных протоколов (см. «Описание прикладных протоколов» на стр. 150).

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 окна зависит от выбранного 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 выключить сетевой протокол, снимите соответствующий флажок.
- Чтобы отключить обработку прикладного протокола:
  - Отключите все сетевые протоколы.
  - В окне предупреждения нажмите кнопку **OK.**

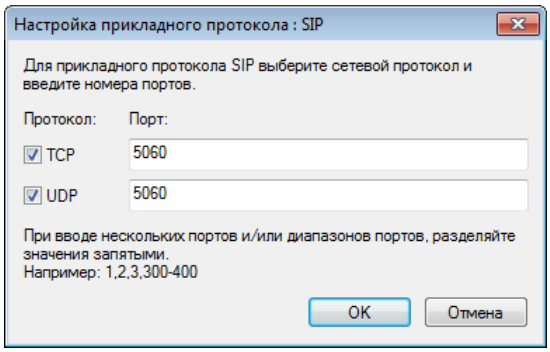


Рисунок 72: Настройка параметров обработки прикладного протокола

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 разделе **Прикладные протоколы** нажмите кнопку **Применить**.

6 Чтобы восстановить настройки по умолчанию, в разделе **Прикладные протоколы** нажмите кнопку **По умолчанию**.

6

Интеграция с программой ViPNet SafeDisk-V

Обеспечение интеграции ViPNet Client с ViPNet SafeDisk-V: порядок действий

Для того чтобы использовать программу ViPNet SafeDisk-V совместно с программой ViPNet Client, необходимо выполнить действия из приведенного ниже списка.

	Действие	Ссылка
☐	Администратору сети ViPNet зарегистрировать сетевой узел в прикладной задаче «Секретный диск» в Центре управления сетью.	«ViPNet Administrator Центр управления сетью. Руководство администратора»
☐	Администратору сети ViPNet создать в УКЦ для пользователей нового сетевого узла полные дистрибутивы ключей и передать их доверенным способом или сформировать в ЦУСе и отправить справочники на уже созданный ранее сетевой узел.	«ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора» «ViPNet Administrator Центр управления сетью. Руководство администратора»
☐	Пользователю, обладающему правами администратора в ОС Windows, установить на сетевой узел программу ViPNet SafeDisk-V.	«ViPNet SafeDisk-V. Руководство пользователя»
☐	Изучить информацию об интеграции ViPNet Client с ViPNet SafeDisk-V.	Общие сведения об интеграции ViPNet Client с ViPNet SafeDisk-V(на стр. 158)
☐	Администратору сетевого узла или пользователю сетевого узла, обладающему максимальным уровнем полномочий, при необходимости изменить настройки интеграции ViPNet Client с ViPNet SafeDisk-V в соответствии с корпоративной политикой безопасности. Для этого: • изменить настройки существующих конфигураций; • создать новые защищенные и незащищенные конфигурации.	Настройка параметров работы с ViPNet SafeDisk-V для текущей конфигурации программы ViPNet Монитор(на стр. 162)

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

Общие сведения об интеграции ViPNet Client с ViPNet SafeDisk-V

Программа ViPNet SafeDisk-V предназначена для защиты конфиденциальной информации, хранящейся 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.

При записи данных в подключенный контейнер они автоматически зашифровываются, при чтении данных они автоматически расшифровываются. 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.

Для того чтобы была возможна интеграция программы ViPNet Client с программой ViPNet SafeDisk-V, обе программы должны быть установлены на одном сетевом узле. Пользователь сможет запустить программу ViPNet SafeDisk-V только в том случае, если программа ViPNet Монитор запущена.

Внимание! Программное обеспечение ViPNet SafeDisk-V интегрировано с ПО ViPNet Client версий 3.2 и выше.Чтобы на сетевом узле можно было использовать программу ViPNet SafeDisk-V, он должен быть зарегистрирован в прикладной задаче «Секретный диск» в Центре управления сетью (см. «Центр управления сетью (ЦУС)»).

Доступ к защищенной информации, хранящейся в контейнерах SafeDisk, имеет только пользователь программы ViPNet Client. Кроме того, доступ к контейнерам SafeDisk-V можно регулировать в зависимости от текущей конфигурации программы ViPNet Монитор (см. «Защищенные и незащищенные конфигурации ViPNet Монитор» на стр. 160).

Параметры работы с контейнерами для текущей конфигурации можно настроить в программе ViPNet Монитор (см. «Настройка параметров работы с ViPNet SafeDisk-V для текущей конфигурации программы ViPNet Монитор» на стр. 162).

Подробная информация о программе ViPNet SafeDisk-V содержится в документе «ViPNet SafeDisk-V. Руководство пользователя».

При работе с программой ViPNet SafeDisk, не интегрированной с программой ViPNet Client, обновление ключей контейнера необходимо проводить самостоятельно с помощью меню программы ViPNet SafeDisk. При совместной работе ViPNet SafeDisk-V с ViPNet Client обновление ключей контейнера ViPNet SafeDisk-V выполняется при обновлении ключей абонентского пункта и ключей пользователя ViPNet. Такая возможность появилась благодаря тому, что при работе ViPNet SafeDisk-V совместно с ViPNet Client ключи контейнера защищены ключами абонентского пункта и ключами пользователя сети ViPNet (см. рисунок ниже).

Рисунок 73: Схема иерархии защиты ключа контейнера в ПО ViPNet SafeDisk и ПО ViPNet SafeDisk-V, интегрированного с ViPNet Client

Защищенные и незащищенные конфигурации ViPNet Монитор

Если на сетевом узле разрешено использование программы ViPNet SafeDisk-V, для каждой конфигурации программы ViPNet Монитор (см. «Управление конфигурациями программы» на стр. 227) на этом узле можно разрешить или запретить использование контейнеров SafeDisk-V. Конфигурации, в которых разрешено использование контейнеров SafeDisk-V, называются защищенными. Конфигурации, в которых использование контейнеров SafeDisk-V запрещено, называются незащищенными.

Дополнительно можно разрешить автоматическое подключение контейнеров SafeDisk-V при выборе защищенной конфигурации.

По умолчанию все создаваемые конфигурации являются защищенными, автоматическое подключение контейнеров не разрешено.

Параметры работы с контейнерами SafeDisk-V для различных конфигураций программы ViPNet Монитор может настраивать администратор сетевого узла (см. «Работа в программе с правами администратора» на стр. 251) или пользователь, обладающий максимальным уровнем полномочий.

Примечание. Изменение настроек интеграции возможно для всех конфигураций ViPNet Монитор, за исключением конфигураций «Открытый Интернет» и «Интернет».

Программа ViPNet Монитор имеет следующие предустановленные конфигурации:

- «Основная конфигурация». Данная конфигурация является защищенной, в ней по умолчанию разрешена работа с контейнерами и не разрешено автоматическое подключение контейнеров.
- «Открытый Интернет» (см. «Конфигурация „Открытый Интернет“» на стр. 229) и «Интернет». Данные конфигурации предназначены для работы с ресурсами Интернета и не позволяют установить соединение с каким-либо сетевым узлом ViPNet. Конфигурации являются незащищенными, и работа с контейнерами SafeDisk-V в них запрещена, так как при обмене потенциально опасным трафиком в Интернете конфиденциальная информация должна быть изолирована.

Конфигурация «Открытый Интернет» создается в том случае, если абонентский пункт связан с координатором, который зарегистрирован в прикладной задаче «Сервер Открытого Интернета».

Конфигурация «Интернет» создается в том случае, если пользователь имеет специальный уровень полномочий «h» (см. «Классификация полномочий. Приложение к документации ViPNet CUSTOM»).

Контроль над использованием контейнеров SafeDisk-V осуществляется следующим образом:

- Если программа ViPNet Монитор не запущена, невозможно запустить программу ViPNet SafeDisk-V.
- При завершении программы ViPNet Монитор все контейнеры SafeDisk-V автоматически отключаются, завершается работа программы ViPNet SafeDisk-V.
- При выборе незащищенной конфигурации все подключенные контейнеры SafeDisk-V отключаются, подключение контейнеров невозможно.
- При выборе защищенной конфигурации можно подключать контейнеры SafeDisk-V.

  Если для защищенной конфигурации разрешено автоматическое подключение контейнеров, при выборе этой конфигурации будут подключены контейнеры, имеющие атрибут **Автоматически подключать контейнер при входе в ViPNet SafeDisk-V** (см. документ «ViPNet SafeDisk-V. Руководство пользователя»).

Примечание. Во всех перечисленных сценариях перед отключением контейнеров все приложения, использующие файлы контейнеров, и все окна, отображающие содержимое контейнеров, должны быть закрыты.

Допустим, корпоративная политика безопасности требует отключать контейнеры SafeDisk-V при работе в Интернете, чтобы снизить риск утечки конфиденциальной информации. В этом случае для защищенных конфигураций можно запретить работу в Интернете с помощью выбора режима безопасности (см. «Режимы безопасности» на стр. 128) или настройки фильтров для открытой сети (см. «Создание правил для открытой сети» на стр. 137). Тогда для работы в Интернете потребуется сменить защищенную конфигурацию на незащищенную. При этом смена конфигурации произойдет только после того, как будут закрыты все приложения, использующие файлы контейнеров ViPNet SafeDisk-V, закрыты все окна, отображающие содержимое контейнеров, и отключены все контейнеры.

Настройка параметров работы с ViPNet SafeDisk-V для текущей конфигурации программы ViPNet Монитор

По умолчанию все создаваемые конфигурации (см. «Управление конфигурациями программы» на стр. 227) программы ViPNet Монитор являются защищенными. Конфигурации «Открытый Интернет» и «Интернет» являются незащищенными, и для этих конфигураций невозможно разрешить использование контейнеров.

Чтобы изменить параметры работы с контейнерами ViPNet SafeDisk-V для текущей конфигурации программы ViPNet Монитор, выполните следующие действия:

1. Загрузите конфигурацию, которую нужно изменить, или создайте новую конфигурацию (см. «Управление конфигурациями программы» на стр. 227).
2. В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.
3. На левой панели окна **Настройка** выберите раздел **SafeDisk-V**.

Примечание. Раздел **SafeDisk-V** будет доступен только в том случае, если сетевой узел зарегистрирован в прикладной задаче «Секретный диск» в ЦУСе.

4. Чтобы разрешить или запретить использование контейнеров SafeDisk-V при работе в текущей конфигурации, установите или снимите флажок **Разрешить использование контейнеров SafeDisk-V**. По умолчанию этот флажок установлен.

Внимание! Разрешить или запретить использование контейнеров ViPNet SafeDisk-V может только пользователь, обладающий максимальным уровнем полномочий, или администратор сетевого узла (см. «Работа в программе с правами администратора» на стр. 251).

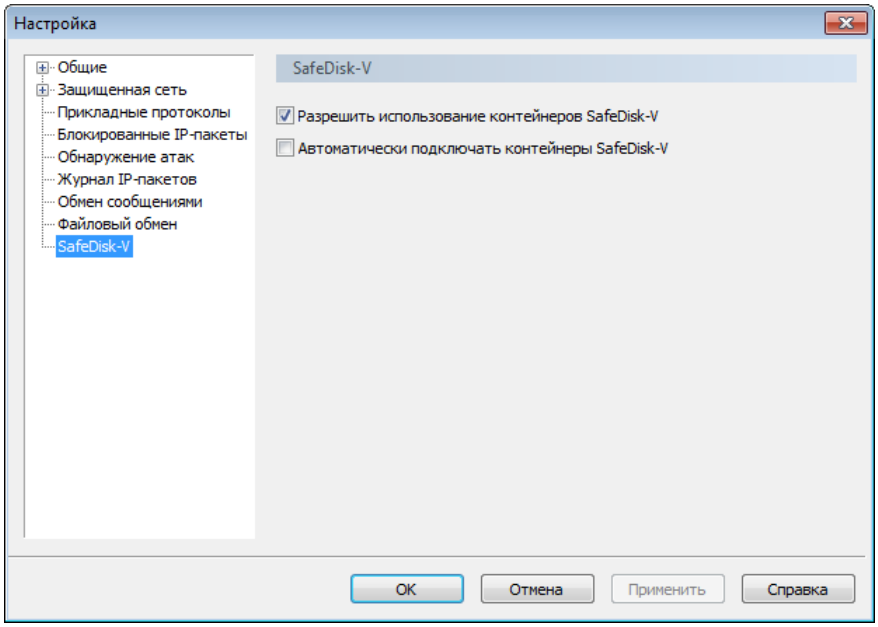


Рисунок 74: Настройка параметров работы с контейнерами SafeDisk-V

5 Чтобы разрешить или запретить автоматическое подключение контейнеров при загрузке защищенной конфигурации установите или снимите флажок **Автоматически подключать контейнеры SafeDisk-V**. По умолчанию этот флажок не установлен.

Если флажок **Автоматически подключать контейнеры SafeDisk-V** установлен, при выборе текущей конфигурации будут автоматически подключены контейнеры, имеющие атрибут **Автоматически подключать контейнер при входе в ViPNet SafeDisk-V** (см. документ «ViPNet SafeDisk-V. Руководство пользователя»).

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

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, т. е. обнаружение IP-адреса компьютера по его имени.

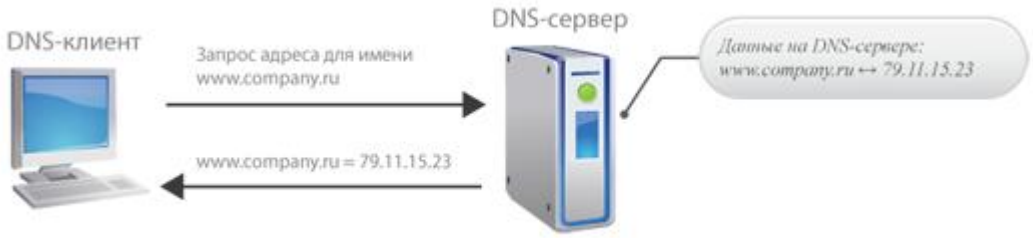


Рисунок 75: Общий принцип работы службы DNS

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, т. е. 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 76: 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 адреса (см. «Виртуальные IP-адреса» на стр. 109), реально не существующие в сети и уникальные на каждом сетевом узле. Поэтому ПО ViPNet автоматически выполняет специальную обработку протоколов служб DNS и WINS.

Такая обработка требуется для того, чтобы предоставить приложениям, которые обращаются к службам DNS и WINS, правильную информацию об IP-адресах защищенных компьютеров. Если ПО ViPNet установлено на DNS (WINS) сервере или DNS (WINS) сервер туннелируется координатором, то технология ViPNet на этом сервере обеспечивает публикацию виртуальных IP-адресов других защищенных компьютеров. Вместе с тем существует возможность использовать для доступа к узлам ViPNet не только IP-адреса, но и DNS-имена.

Необходимость в использовании служб имен в ПО ViPNet возникает в следующих случаях:

- Требуется обеспечить доступ к сетевому узлу одновременно со стороны защищенных и открытых компьютеров по некоторому IP-адресу, не принадлежащему этому сетевому узлу, например через NAT-устройство.

  Таким образом, на DNS-сервере можно опубликовать не только виртуальные или реальные IP-адреса некоторого сетевого узла, но и любые удобные IP-адреса других устройств, через которые IP-пакет может быть передан на этот сетевой узел. ПО ViPNet, получив такой IP-адрес, проверяет доступность сетевого узла через этот адрес и в случае успешного подключения к узлу регистрирует его, а также реальные адреса этого узла или соответствующие им виртуальные адреса, предоставляя возможность приложениям работать по этим адресам.

- Требуется обеспечить доступ к координатору, внешний IP-адрес которого или IP-адрес доступа к которому через внешнее устройство может изменяться. В этом случае координатор или внешнее устройство должно поддерживать технологию динамического DNS (DYN DNS), которая осуществляет автоматическую регистрацию IP-адресов устройств на заданном DNS-сервере.

Примечание. Настройка NetBIOS-имен в ПО ViPNet не поддерживается.

Наиболее безопасным решением является установка ПО ViPNet на DNS (WINS) сервер или туннелирование этого сервера некоторым координатором (см. «Защищенный DNS (WINS) сервер» на стр. 170). Вместе с тем можно обеспечить безопасную работу и с открытыми (публичными) серверами служб имен (см. «Незащищенный DNS (WINS) сервер» на стр. 171).

Защищенный DNS (WINS) сервер

Особенности использования

- 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 компьютеров автоматически регистрируются на DNS (WINS) сервере, то поддержка виртуальных адресов осуществляется автоматически. Драйвер ViPNet выполняет подмену адреса в IP-пакете на виртуальный или реальный IP-адрес. В результате на сервере имен регистрируется нужный IP-адрес.
- Если к защищенному DNS (WINS) серверу обращается открытый компьютер, то этому компьютеру сообщаются реальные IP-адреса защищенных узлов, даже если для них опубликованы виртуальные IP-адреса.

Рекомендации по настройке

- В случае, если DNS (WINS) сервер туннелируется координатором, этот DNS (WINS) сервер не следует располагать в одной подсети с сетевыми узлами, которые на нем зарегистрированы. Однако если это все же необходимо, следует обеспечить доступность этих сетевых узлов с координатора по реальным IP-адресам.
- Во избежание конфликтов рекомендуется располагать туннелируемые DNS (WINS) серверы за отдельным сетевым интерфейсом координатора.
- В случае, если DNS (WINS) сервер виден с защищенных сетевых узлов по виртуальному IP-адресу, то IP-адрес этого DNS (WINS) сервера необходимо удалить с DHCP-сервера (см. «DHCP (Dynamic Host Configuration Protocol)»), на котором зарегистрированы эти защищенные сетевые узлы.
- Если DNS (NetBios) имена и соответствующие им IP-адреса защищенных компьютеров регистрируются на DNS (WINS) сервере вручную, следует соблюдать следующее правило:
    - Для защищенного компьютера регистрируется его виртуальный или реальный IP-адрес, по которому этот защищенный компьютер виден в программе ViPNet Монитор, установленной на DNS (WINS) сервере. Если DNS (WINS) сервер туннелируется, необходимые адреса нужно найти в программе ViPNet Монитор на координаторе, осуществляющем туннелирование DNS (WINS) сервера.

Незащищенный DNS (WINS) сервер

Особенности использования

Публичные DNS-серверы могут быть подвержены различным сетевым атакам с целью заставить защищенный компьютер обратиться на атакующий компьютер. Если такая атака (путем подмены IP-адреса запрашиваемого сетевого ресурса) удастся, то злоумышленник может попытаться получить интересующую его информацию с защищенного компьютера.

Для предотвращения такого рода атак для всех защищенных прикладных серверов (см. «Защищенные прикладные серверы»), доступных с данного узла, в настройках программы ViPNet Монитор на сетевом узле следует задать DNS-имена (см. «Настройка доступа к защищенным узлам» на стр. 112). Тогда даже в случае успешной атаки соединение с подставным сервером не произойдет, поскольку переадресованная информация будет зашифрована и недоступна атакующему компьютеру.

Рекомендации по настройке

Если DNS (WINS) сервер не защищен с помощью ПО ViPNet, необходимо:

- Публиковать на DNS (WINS) сервере только реальные IP-адреса защищенного компьютера (сетевого узла или туннелируемого ресурса), а если DNS-имена заданы в настройках программы ViPNet Монитор, то также и IP-адреса доступа к сетевому узлу через внешние устройства. То есть публикуется любой реальный IP-адрес, по которому пакет может достигнуть сетевого узла (например, адрес межсетевого экрана или координатора, через который работает сетевой узел, или непосредственно адрес сетевого узла).
- Обеспечить доступность защищенных компьютеров, адреса которых зарегистрированы на DNS (WINS) сервере, со всех сетевых узлов:
    - по реальным IP-адресам;
    - если необходимы виртуальные адреса, зарегистрировать DNS (NetBIOS) имена этих защищенных компьютеров в программе ViPNet Монитор, используемой на сетевых узлах.

При использовании открытого DNS-сервера DNS-имена защищенных компьютеров, как сказано выше, рекомендуется задавать в настройках ПО ViPNet (см. «Настройка доступа к защищенным узлам» на стр. 112).

Использование защищенного DNS-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-серверы определяются поставщиком услуг Интернета. Однако для работы со многими корпоративными приложениями требуется использовать DNS-сервер корпоративной сети. Использование корпоративного DNS-сервера позволяет обращаться к серверам и другим узлам корпоративной сети по их именам, а не по IP-адресам. При этом преобразование DNS-имен в IP-адреса обеспечивается как для адресов корпоративной сети, так и для адресов Интернета.

Необходимые условия

Для удаленного доступа к корпоративным ресурсам 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. 97).
- В сетевых настройках операционной системы должен быть задан IP-адрес корпоративного DNS-сервера.

Регистрация защищенного DNS-сервера средствами ПО ViPNet

Рассмотрим следующий пример. Сотрудник, работающий в главном офисе на ноутбуке с установленным ПО ViPNet Client, подключается к защищенному корпоративному DNS-серверу по адресу 10.0.0.25.

Этот сотрудник отправляется со своим ноутбуком в командировку в другой офис. Теперь DNS-сервер главного офиса доступен по IP-адресу 11.0.0.3. Сотруднику нужно подключиться через Интернет к корпоративным ресурсам главного офиса. Для этого на ноутбуке в ОС Windows нужно изменить настройки сетевых подключений. Это неудобно, так как после возвращения в главный офис настройки нужно будет вернуть в исходное состояние.

Однако можно добиться того, чтобы программа ViPNet Монитор следила за текущим IP-адресом видимости DNS (WINS) сервера и автоматически изменяла настройки на всех сетевых интерфейсах компьютера. Для этого нужно записать идентификатор и реальный IP-адрес корпоративного DNS (WINS) сервера в специальный файл `DNS.TXT`.

Примечание. Если используемые DNS-серверы перечислены в файле `DNS.TXT`, задавать адреса серверов в сетевых настройках Windows не требуется.

При использовании файла `DNS.TXT` на всех сетевых адаптерах компьютера списки IP-адресов DNS (WINS) серверов будут дополнены IP-адресами, по которым в данный момент доступны указанные в файле `DNS.TXT` сетевые узлы ViPNet и туннелируемые узлы. 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` сетевым узлам и туннелируемым ресурсам.

Формат записей в файле `DNS.TXT` отличается в зависимости от того, установлен ли корпоративный DNS (WINS) сервер на защищенном узле или туннелируется координатором.

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

Чтобы внести запись о корпоративном DNS (WINS) сервере в файл DNS.TXT:

1. В любом текстовом редакторе (лучше Notepad) создайте пустой текстовый файл `DNS.TXT`.
2. Сохраните файл в папке `\DATABASES\DNSWINSLIST`, находящейся в папке установки ПО VIPNet. Если папка не существует, создайте ее.
3. Введите в созданный файл следующую информацию:

```
[DNSLIST]
ID00=0001000b;
[WINSLIST]
ID00=0001000b;
```

где: 0001000b — идентификатор сетевого узла ViPNet, на котором установлен DNS (WINS) сервер;

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

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.

4 Сохраните файл и закройте его.

В результате, независимо от того, по какому адресу в данный момент времени доступен DNS (WINS) сервер, можно будет беспрепятственно подключиться к корпоративным ресурсам.

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

Если корпоративный DNS (WINS) сервер туннелируется координатором

Чтобы внести запись о корпоративном DNS (WINS) сервере в файл DNS.TXT:

1 В любом текстовом редакторе (лучше Notepad) создайте пустой текстовый файл DNS.TXT.

2 Сохраните файл в папке \DATABASES\DNSWINSLIST, находящейся в папке установки ПО ViPNet. Если папка не существует, создайте ее.

3 Введите в созданный файл следующую информацию:

```
[DNSLIST]
ID00=000100ca-10.0.0.25;
[WINSLIST]
ID00=0001000b;
```

где: 000100ca — идентификатор координатора, туннелирующего DNS (WINS) сервер;

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

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.

В отличие от ситуации, когда корпоративный DNS (WINS) сервер установлен непосредственно на сетевом узле ViPNet, здесь к идентификатору координатора через тире требуется добавить IP-адрес туннелируемого этим координатором DNS (WINS) сервера. Если координатор туннелирует несколько серверов, их можно перечислить в одной строке через точку с запятой без пробелов. Например, `ID00=000100ca-10.0.0.25;10.0.0.30;`

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

4 Сохраните файл и закройте его.

В результате, независимо от того, по какому адресу в данный момент времени доступен DNS (WINS) сервер, можно будет беспрепятственно подключиться к корпоративным ресурсам.

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

Формат файла DNS.TXT

В общем виде файл `DNS.TXT` может иметь следующий формат:

```
[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.

Настройка параметров подключения к DNS (WINS) серверу в ОС Windows

Примечание. Если используемые DNS-серверы перечислены в файле DNS.TXT (см. «Регистрация защищенного DNS-сервера средствами ПО ViPNet» на стр. 173), задавать адреса серверов в сетевых настройках Windows не требуется.

Чтобы задать IP-адрес DNS-сервера и (или) WINS-сервера в сетевых настройках операционной системы, выполните следующие действия:

1. Нажмите кнопку **Пуск** и в меню выберите **Панель управления**.
2. В **Панели управления** дважды щелкните **Центр управления сетями и общим доступом** (**Сетевые подключения** в Windows XP).
3. Для просмотра статуса сетевого подключения:
   - Если используется ОС Windows 7, в **Центре управления сетями и общим доступом** щелкните имя подключения.

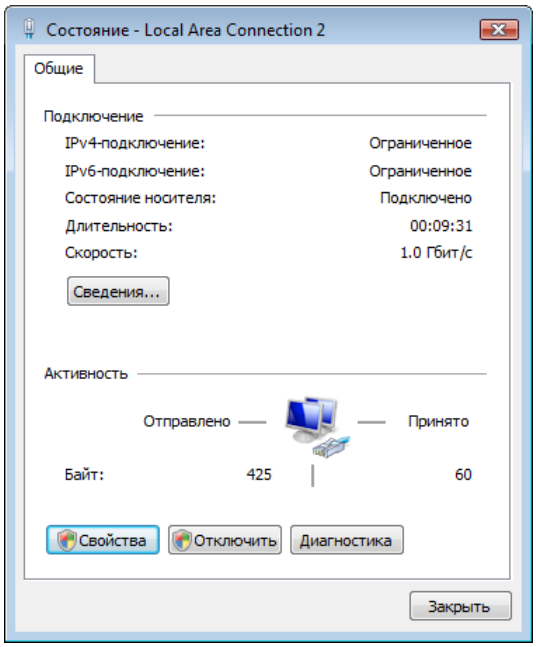


Рисунок 77: Просмотр состояния сетевого подключения

- Если используется ОС Windows Vista, в **Центре управления сетями и общим доступом** щелкните ссылку **Просмотр состояния**.
- Если используется ОС Windows XP, дважды щелкните значок подключения.

Откроется окно просмотра состояния сетевого подключения.

4 На вкладке **Общие** нажмите кнопку **Свойства**. Откроется окно свойств сетевого подключения.

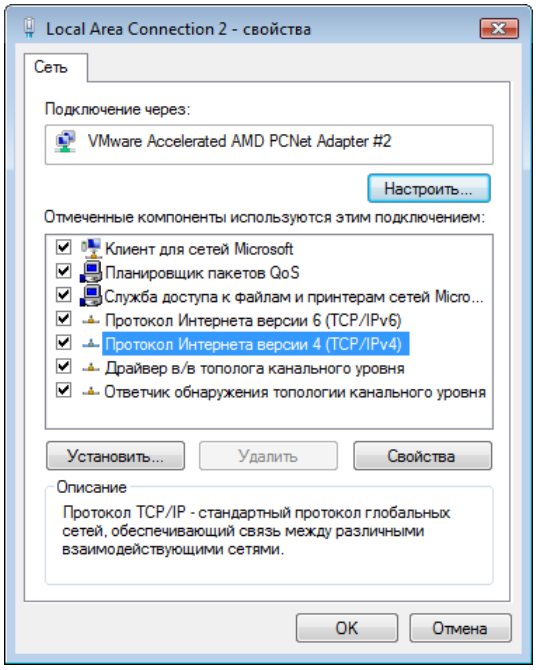


Рисунок 78: Просмотр свойств сетевого подключения

5 В списке компонентов, используемых подключением:

- В случае использования Windows 7 или Windows Vista выберите **Протокол Интернета версии 4 (TCP/IPv4)**.
- В случае использования Windows XP выберите **Протокол Интернета (TCP/IP)**.

Нажмите кнопку **Свойства**. Откроется окно свойств протокола.

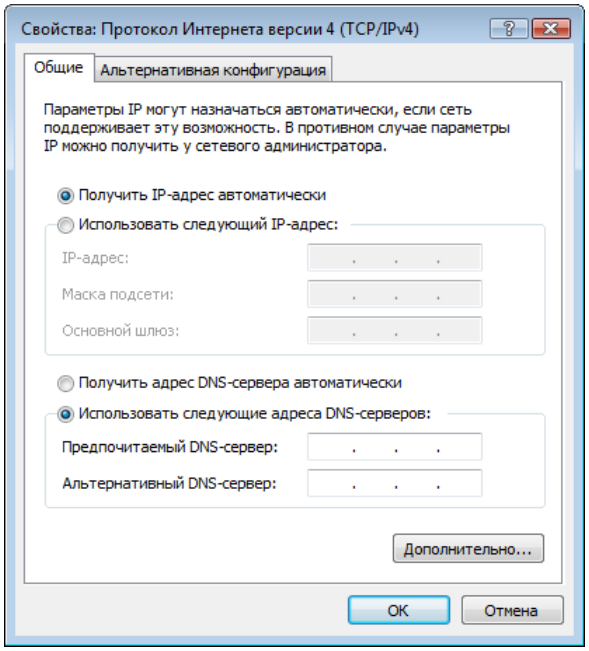


Рисунок 79: Свойства протокола TCP/IPv4

Чтобы задать адрес корпоративного DNS-сервера:

1 На вкладке **Общие** выберите **Использовать следующие адреса DNS-серверов**. В поле **Предпочитаемый DNS-сервер** введите IP-адрес предпочтительного корпоративного DNS-сервера. В случае необходимости в поле **Альтернативный DNS-сервер** можно ввести IP-адрес другого корпоративного DNS-сервера.

Внимание! Следует указать реальный IP-адрес DNS-сервера, если он доступен по реальному адресу, и виртуальный IP-адрес, если сервер доступен по виртуальному адресу (см. «Виртуальные IP-адреса» на стр. 109).

В случае, если с удаленного рабочего места необходимо организовать как доступ к защищенным корпоративным ресурсам, так и доступ в Интернет, следует также зарегистрировать IP-адрес открытого DNS-сервера.

---

2 Можно задать адреса дополнительных DNS-серверов и определить приоритет их использования. Для этого выполните следующие действия:

- Нажмите кнопку **Дополнительно**. Откроется окно **Дополнительные параметры TCP/IP**.

- Откройте вкладку **DNS**.

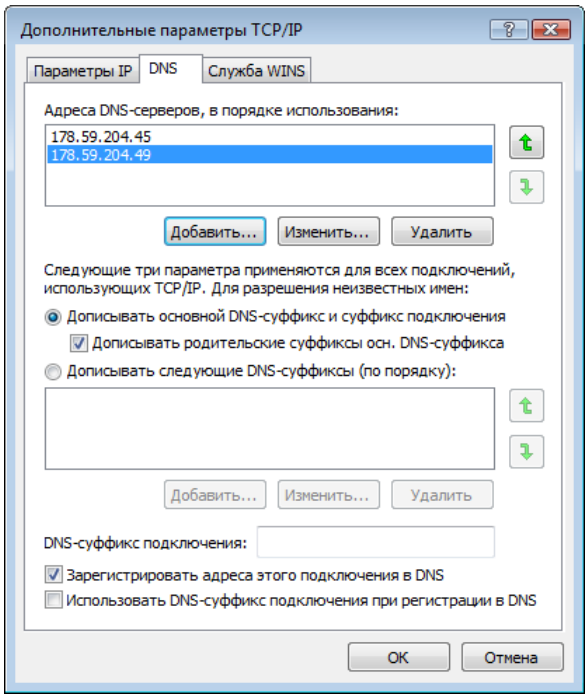


Рисунок 80: Задание дополнительных DNS-серверов

- Для добавления DNS-сервера нажмите кнопку **Добавить**. Откроется окно **DNS-сервер TCP/IP**.

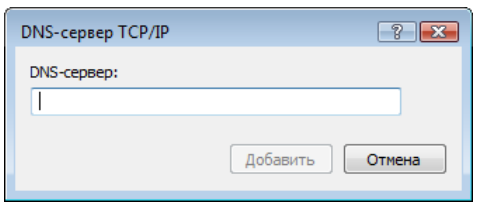


Рисунок 81: Добавление адреса DNS-сервера

- В поле **DNS-сервер** введите IP-адрес сервера и нажмите кнопку **Добавить**.
- Чтобы изменить порядок использования DNS-серверов, используйте стрелки справа от списка серверов.
- Во всех окнах нажмите кнопку **OK**.

Чтобы задать адрес корпоративного WINS-сервера:

1. Нажмите кнопку **Дополнительно**. Откроется окно **Дополнительные параметры TCP/IP**.

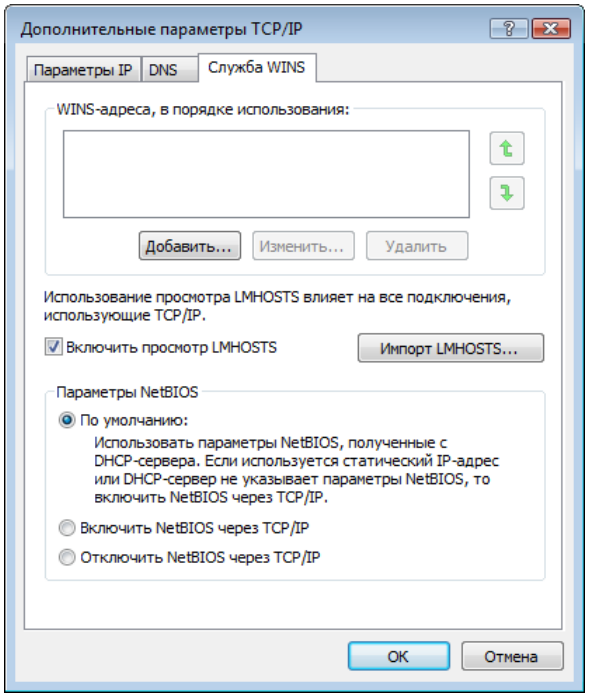


Рисунок 82: Задание адреса WINS-сервера

2 На вкладке **Служба WINS** нажмите кнопку **Добавить**. Откроется окно **WINS-сервер TCP/IP**.

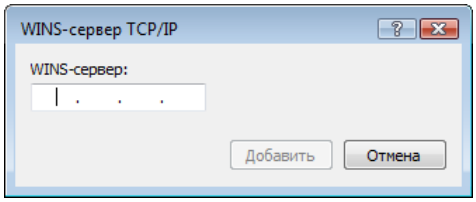


Рисунок 83: Ввод IP-адреса WINS-сервера

3 В поле **WINS-сервер** введите IP-адрес сервера и нажмите кнопку **Добавить**.

Внимание! Следует указать реальный IP-адрес WINS-сервера, если он доступен по реальному адресу, и виртуальный IP-адрес, если сервер доступен по виртуальному адресу (см. «Виртуальные IP-адреса» на стр. 109).

---

4 В случае необходимости повторите предыдущие шаги, чтобы добавить дополнительные WINS-серверы.

5 Чтобы изменить порядок использования WINS-серверов, используйте стрелки справа от списка серверов.

6 Во всех окнах нажмите кнопку **OK**.

В результате выполнения вышеописанных действий будет обеспечен доступ к корпоративным серверам и ресурсам как с использованием понятных DNS-имен, так и по IP-адресам. При этом сохранится возможность работы в Интернете.

8

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».

Программа ViPNet Монитор также имеет следующие полезные функции:

- Проверка соединения с другим сетевым узлом ViPNet.
- Блокировка компьютера.

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.

Процесс обмена сообщениями между пользователями ViPNet называется сеансом. Все сообщения, полученные и отправленные в течение сеанса, записываются в протокол сеанса. Протокол сеанса можно сохранить как текстовый файл. Если в рамках сеанса отправить сообщение какому-либо пользователю, его ответ придет в том же сеансе и будет сохранен в том же протоколе.

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 и создан новый протокол.

Новые сообщения – это сообщения, которые пользователь еще не обработал (не принял, не ответил или не удалил), но мог прочитать в окне **Новые сообщения.**

Непрочтенные сообщения – это новые сообщения, которых пользователь еще не видел.

Различие между сеансом обмена сообщениями и конференцией

Программу обмена защищенными сообщениями можно использовать двумя способами:

- Обмен сообщениями с другими пользователями ViPNet. Вы можете отправлять сообщения одному или нескольким пользователям одновременно и получать от них ответы. При этом пользователи 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 правой панели выберите один или несколько сетевых узлов и на панели инструментов нажмите кнопку **Обмен защищенными сообщениями.**

- Конференция с другими пользователями ViPNet. Вы можете отправлять сообщения одновременно нескольким пользователям и получать от них ответы. Отличие от сеанса обмена сообщениями заключается в том, что все участники конференции будут получать сообщения от других участников.

Чтобы начать конференцию, в окне программы ViPNet Монитор на панели навигации выберите раздел **Защищенная сеть**, затем на правой панели выберите несколько сетевых узлов и на панели инструментов нажмите кнопку **Защищенная конференция**.

Интерфейс программы обмена защищенными сообщениями

Прием и отправка сообщений выполняются в окне **Оперативный обмен защищенными сообщениями**, которое представлено на следующем рисунке:

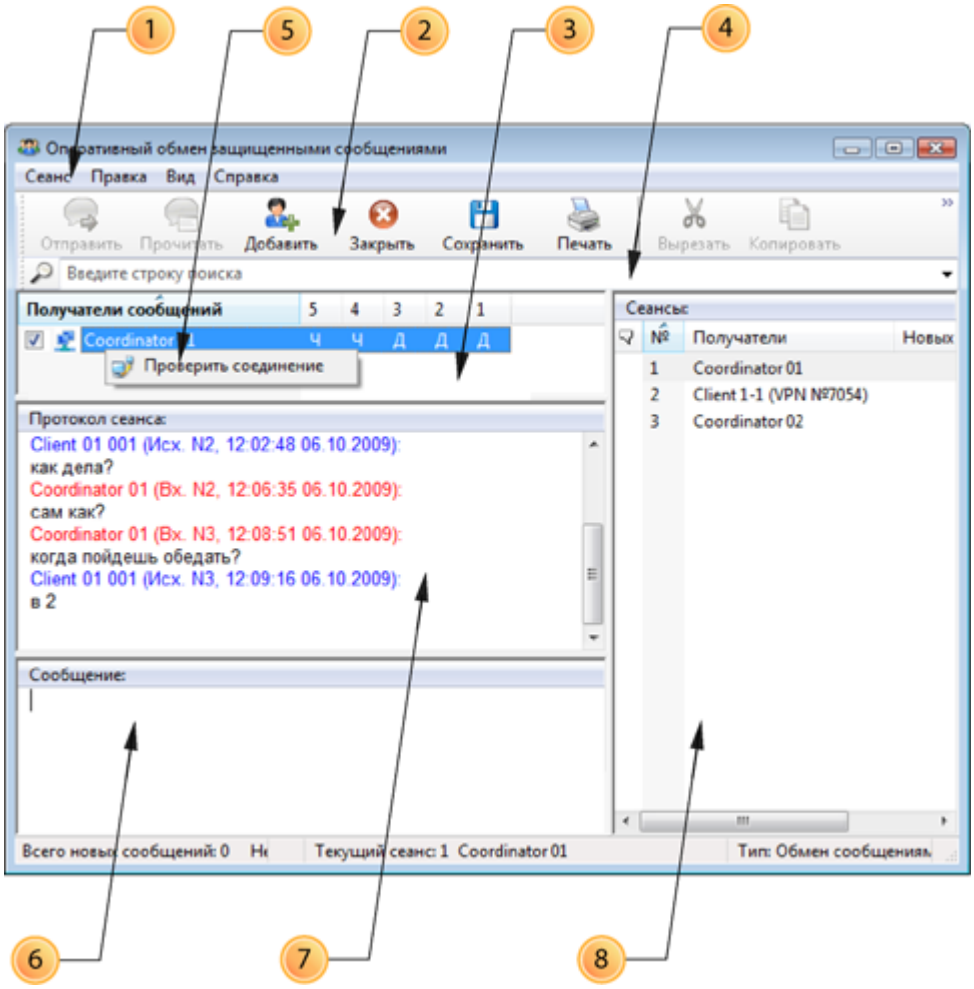


Рисунок 84: Окно обмена защищенными сообщениями

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 **Получатели сообщений.**

5 Контекстное меню, вызываемое щелчком правой кнопки мыши по имени получателя. Позволяет проверить соединение с получателем (см. «Проверка соединения с сетевым узлом» на стр. 202).

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. 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

Колонка	Описание
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.

Отправка мгновенных сообщений

Для обмена мгновенными сообщениями:

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

2. В разделе **Защищенная сеть** выберите сетевой узел, пользователю которого нужно отправить сообщение. Чтобы выбрать несколько узлов, зажмите клавишу **Ctrl** и по очереди щелкните нужные сетевые узлы.

   Чтобы отфильтровать список сетевых узлов, в строку поиска, расположенную внизу раздела **Защищенная сеть**, введите часть имени нужного сетевого узла.

   Рисунок 85: Поиск в списке сетевых узлов ViPNet

3. Если требуется:

   - Начать сеанс обмена защищенными сообщениями с выбранными пользователями, нажмите кнопку **Сообщение** .

   Примечание. Если выбрано несколько пользователей, будет открыт один новый сеанс обмена сообщениями, однако его участники смогут отправлять ответные сообщения только инициатору сеанса.

   - Начать конференцию с участием выбранных пользователей, нажмите кнопку **Конференция** .

Чтобы начать сеанс обмена сообщениями или конференцию, можно также использовать меню **Действие** или соответствующие пункты в контекстном меню сетевого узла.

Новый сеанс будет открыт в окне **Оперативный обмен защищенными сообщениями** (см. Рисунок 84 на стр. 186).

Примечание. Если окно **Оперативный обмен защищенными сообщениями** уже открыто, в этом окне в меню **Сеанс** можно выбрать пункт **Новый**, а затем щелкнуть **Обмен сообщениями** или **Конференция**. Далее в окне **Выбор сетевого узла** следует указать получателей сообщения.

---

4 В окне **Оперативный обмен защищенными сообщениями** 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 меню **Сеанс** выберите пункт **Настройка**, откроется окно **Настройка**. В разделе **Обмен сообщениями** в группе **Назначить горячие клавиши** выберите **Ctrl+Enter: отправка сообщения, Enter: перевод строки** или наоборот.

Прием мгновенных сообщений

При поступлении новых сообщений в области уведомлений появляется мигающий значок . Способ уведомления о новом сообщении можно изменить. Для этого выполните следующие действия:

1 В окне **Оперативный обмен защищенными сообщениями** в меню **Сеанс** выберите пункт **Настройка**.

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.**

При получении новых сообщений:

1 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**.

Если в окне **Настройка** в разделе **Обмен сообщениями** установлен флажок **Показывать новые сообщения в отдельном окне**, откроется окно **Новые сообщения**.

Примечание. По умолчанию флажок **Показывать новые сообщения в отдельном окне** установлен. Если этот флажок снят, новые сообщения будут автоматически открываться в окне **Оперативный обмен защищенными сообщениями**.

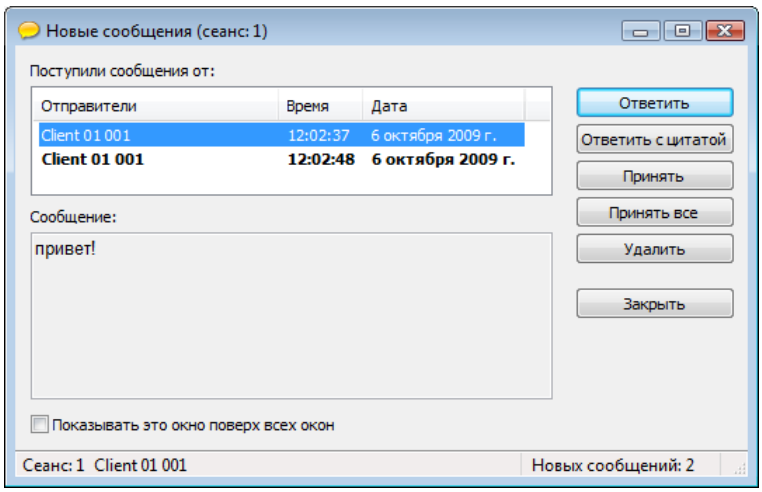


Рисунок 86: Новые сообщения в отдельном окне

В заголовке окна **Новые сообщения** указан номер сеанса. В строке состояния этого окна приведены номер сеанса, имена участников сеанса и число новых сообщений, относящихся к указанному сеансу.

Сообщения отображаются в списке в порядке поступления, атрибуты непрочитанных сообщений выделены полужирным шрифтом.

Если в окне **Оперативный обмен защищенными сообщениями** переключиться на другой сеанс, в окне **Новые сообщения** отобразятся данные о новых сообщениях выбранного сеанса.

2 Чтобы прочесть сообщение, выберите его в списке. Содержание сообщения будет отображено в поле **Сообщение**.

Примечание. Если сообщение отображается более трех секунд, отправителю автоматически отправляется уведомление о прочтении (на компьютере отправителя в окне **Оперативный обмен защищенными сообщениями** статус сообщения изменяется на **Ч**).

3 Чтобы прочесть сообщение и сохранить его в протоколе сеанса, в окне **Новые сообщения** нажмите кнопку **Принять**.

4 Чтобы сохранить в протоколе сеанса все новые сообщения, нажмите кнопку **Принять все**.

5 Чтобы ответить на сообщение, выберите его из списка и нажмите кнопку **Ответить** или **Ответить с цитатой**.

Совет. При ответе с цитатой в начало каждой строки цитируемого сообщения добавляется символ «больше» («>»). Такая строка отображается на панели **Протокол сеанса** курсивным шрифтом синего цвета. Такого же результата можно добиться, вручную добавив знак «>» в начало строки при вводе сообщения.

6 Чтобы удалить сообщение, выберите его из списка и нажмите кнопку **Удалить**.

7 Чтобы закрыть окно **Новые сообщения**, нажмите кнопку **Закрыть**.

Прекращение обмена сообщениями

Чтобы закрыть сеанс обмена сообщениями:

1 В окне **Оперативный обмен защищенными сообщениями** на панели **Сеансы** выберите сеанс, который требуется закрыть.

2 Выполните одно из действий:

- В меню **Сеанс** выберите пункт **Закрыть**.
- Нажмите клавишу **F8**.
- Нажмите кнопку **Закрыть**  на панели инструментов.

По умолчанию перед закрытием сеанса программа предложит сохранить протокол в текстовом файле.

3 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**  .

  Все открытые сеансы будут закрыты. По умолчанию перед закрытием программа предложит сохранить протоколы сеансов.

Файловый обмен

Пользователи сети ViPNet могут пересылать друг другу файлы по защищенному каналу VPN. При этом нет ограничений на размер и тип файлов. Для отправки файла можно использовать как программу ViPNet Монитор, так и контекстное меню Windows.

Интерфейс программы «Файловый обмен»

Информация о файлах, отправленных и принятых с помощью «Файлового обмена», отображается в окне программы, которое открывается каждый раз при отправке или приеме файлов. Также программу «Файловый обмен» можно вызвать с помощью кнопки  в окне программы ViPNet Монитор (см. «Способы аутентификации пользователя» на стр. 75).

Внешний вид окна программы «Файловый обмен» представлен на следующем рисунке.

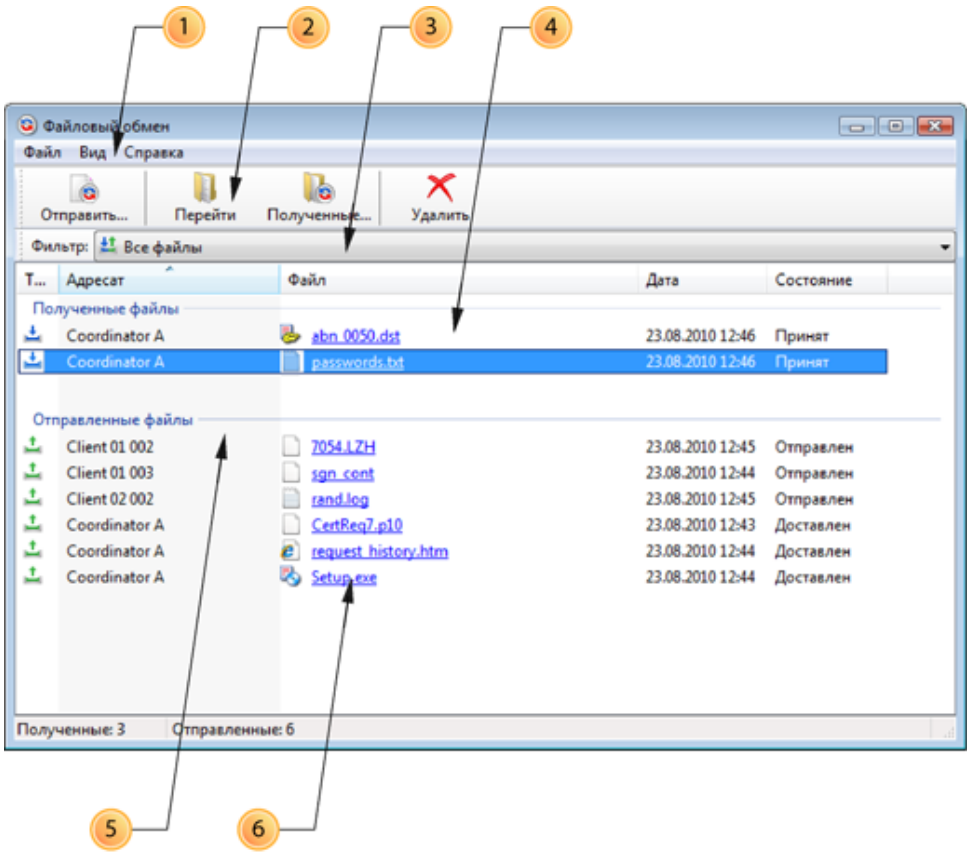


Рисунок 87: Окно файлового обмена

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.
   - Полученные файлы.
   - Отправленные файлы.
4. Группа **Полученные файлы**. В этой группе отображаются файлы, полученные от пользователей других сетевых узлов ViPNet.
5. Группа **Отправленные файлы**. В этой группе отображаются файлы, отправленные пользователям других сетевых узлов ViPNet.
6. Ссылка для перехода в папку, в которой находится файл.

Отправка файлов с помощью 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 внизу раздела **Защищенная сеть** (см. Рисунок 85 на стр. 188).
3. Выполните одно из действий:
   - Нажмите кнопку **Файл**  на панели инструментов.
   - В меню **Действие** выберите пункт **Отправить файл.**
   - Щелкните сетевой узел правой кнопкой мыши и в контекстном меню выберите пункт **Отправить файл.**
4. В окне **Открыть** 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 87 на стр. 193), в котором отображается информация об отправленных файлах и их статус.

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 **Файловый обмен** в меню **Файл** выберите пункт **Настройка**.

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.

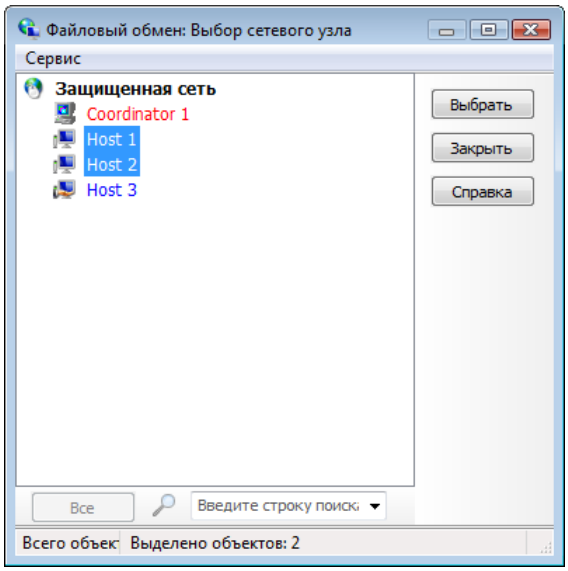


Рисунок 88: Выбор получателя для отправляемых файлов

4 Выбрав получателей, нажмите кнопку **Выбрать**. Файлы будут отправлены выбранным получателям.

5 Откроется окно **Файловый обмен** (см. Рисунок 87 на стр. 193), в котором отображается информация об отправленных файлах и их статус.

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 **Файловый обмен** в меню **Файл** выберите пункт **Настройка**.

Прием файлов

При поступлении файлов от другого пользователя ViPNet:

1. Программа выдаст сообщение о принятом файле, в области уведомлений появится значок программы файлового обмена .

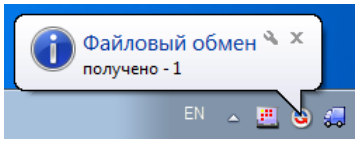


Рисунок 89: Уведомление о принятом файле

> **Примечание.** Для настройки уведомлений в окне **Файловый обмен** в меню **Файл** выберите пункт **Настройка**.

2. Чтобы просмотреть полученные файлы, щелкните значок файлового обмена в области уведомлений. Откроется окно **Файловый обмен** (см. Рисунок 87 на стр. 193).

3. В окне **Файловый обмен** в группе **Полученные файлы** выберите нужный файл и выполните одно из действий:

   - Щелкните имя файла в колонке **Файл.**
   - Нажмите кнопку **Полученные** 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 **Полученные** 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 **Полученные**, 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:

- Microsoft Portrait.
- VNC Viewer.
- Remote Desktop Connection.
- Radmin Viewer.

Подробнее о работе с программами Radmin Viewer, VNC Viewer и Remote Desktop Connection можно прочесть в разделе Удаленное управление сетевыми узлами ViPNet(на стр. 230).

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 т.д. 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:

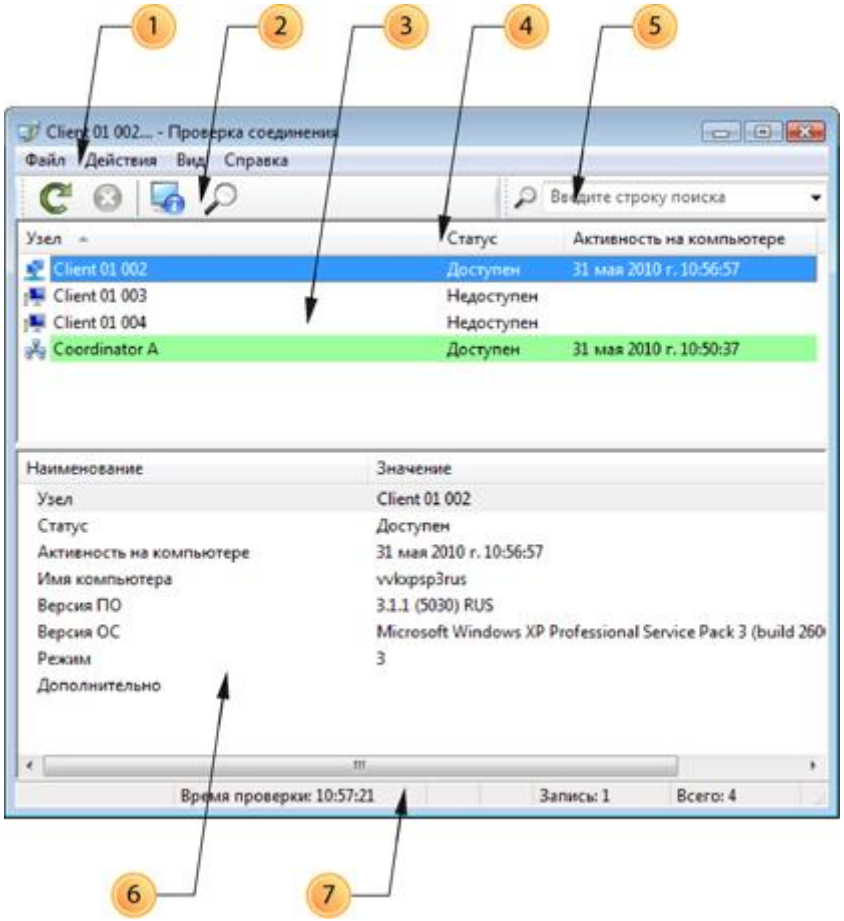


Рисунок 90: Окно проверки соединения

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 текущий статус:

Цвет имени	Статус сетевого узла
Фиолетовый	Сетевой узел доступен, но последние 15 минут не проявлял активности на компьютере.

Цвет имени	Статус сетевого узла
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 статусе сетевого узла 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**.

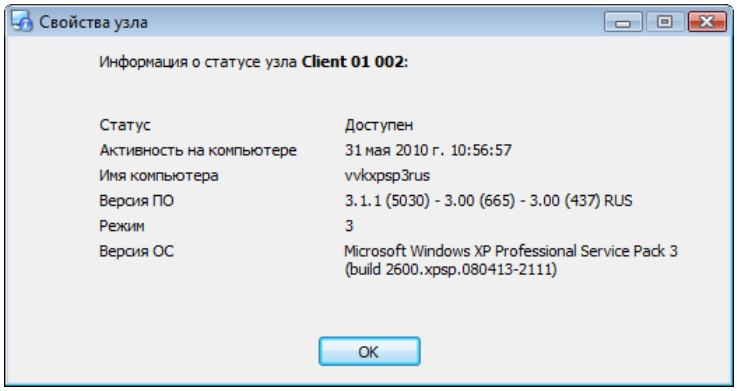


Рисунок 91: Подробная информация о статусе сетевого узла

- Чтобы отправить на один из сетевых узлов в окне **Проверка соединения** письмо «Деловой почты», 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**. 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.

Блокировка компьютера и IP-трафика

С помощью ViPNet Монитор можно запретить доступ ко всем приложениям на компьютере, блокировать весь IP-трафик или выполнить оба эти действия одновременно.

Чтобы выполнить блокировку:

1. В строке состояния окна программы ViPNet Монитор нажмите кнопку **Блокировать IP-трафик**  .

   По умолчанию в строке состояния отображается кнопка последнего использовавшегося режима блокировки. Если функция блокировки используется впервые, в строке состояния отображается кнопка **Блокировать компьютер**.

2. Если требуется выбрать другой режим блокировки, щелкните стрелку справа от кнопки блокировки  и в меню выберите один из пунктов:

   - **Блокировать компьютер и IP-трафик.** При выборе данного режима будет закрыт доступ ко всем приложениям на компьютере, весь IP-трафик заблокирован. Появится окно для снятия блокировки компьютера. Чтобы разблокировать компьютер, требуется ввести пароль пользователя Windows. После разблокировки компьютера на Рабочем столе появится окно ввода пароля с сообщением «IP-трафик заблокирован». Чтобы продолжить работу, требуется ввести пароль пользователя ViPNet Монитор и нажать **OK**.
   - **Блокировать компьютер.** При выборе данного режима доступ ко всем приложениям на компьютере будет закрыт, однако IP-трафик не будет заблокирован. Появится окно для снятия блокировки компьютера. Чтобы продолжить работу, требуется ввести пароль пользователя Windows.
   - **Блокировать IP-трафик.** При выборе данного режима весь входящий и исходящий IP-трафик будет заблокирован, окно ViPNet Монитор будет скрыто, а на Рабочем столе появится окно ввода пароля с сообщением «IP-трафик заблокирован». Для разблокирования требуется ввести пароль пользователя ViPNet Монитор и нажать **OK**.

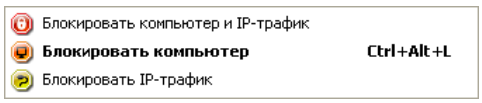


Рисунок 92: Меню блокировки компьютера

Последний использовавшийся (текущий) режим блокировки выделен в меню полужирным шрифтом. Кнопка этого режима отображается в строке состояния окна ViPNet Монитор, а также сохраняется в текущей конфигурации программы.

Внимание! Не используйте функцию блокировки при удаленной работе на данном компьютере (например, с помощью Remote Desktop Connection). Если IP-трафик (или компьютер и IP-трафик) будет заблокирован с помощью программы ViPNet Монитор, удаленный доступ к компьютеру будет невозможен.

Параметры, влияющие на блокировку компьютера

В окне программы ViPNet Монитор в разделе **Администратор** можно задать интервал автоматической блокировки компьютера (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 252). Если мышь и клавиатура не используются в течение заданного интервала времени, автоматически применяется текущий режим блокировки компьютера.

Если в окне **Настройка** в разделе **Общие** установлен флажок **Отображать кнопку блокировки IP-трафика и компьютера поверх всех окон**, в правом нижнем углу экрана будет отображаться большая полупрозрачная кнопка блокировки. По нажатию этой кнопки включается текущий режим блокировки.

Рисунок 93: Кнопка блокировки в углу экрана

Чтобы компьютер был заблокирован сразу после запуска программы ViPNet Монитор:

1. В меню **Сервис** выберите пункт **Настройки**.
2. В окне **Настройка** в разделе **Общие** откройте подраздел **Запуск и аварийное завершение**.
3. В группе **При запуске приложения** установите флажок **Блокировать компьютер**.
4. Нажмите кнопку **Применить**.

Особенности блокировки компьютера при использовании внешнего устройства для аутентификации пользователя

Если для аутентификации пользователя используется внешнее устройство (а именно, задан способ аутентификации **Пароль на устройстве** или **Устройство**), при отключении этого устройства автоматически включается режим блокировки компьютера и IP-трафика. Чтобы продолжить работу, необходимо подключить устройство, снять блокировку компьютера (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.

Режим блокировки, который устанавливается после отключения устройства, можно изменить с помощью дополнительных настроек программы (см. «Дополнительные настройки программы ViPNet Монитор» на стр. 252). Для задания режима блокировки используются флажки **Блокировать IP-трафик** и **Блокировать компьютер** в группе параметров **При отключении устройства аутентификации**. По умолчанию оба флажка установлены, что обеспечивает автоматическую защиту компьютера и трафика в случае отключения устройства. Чтобы не использовать блокировку при отключении устройства, нужно снять оба флажка.

Функция автоматической блокировки при отключении устройства действует для любых внешних устройств, кроме iButton, Smartcard Athena, Аккорд-5MX (см. «Информация о внешних устройствах хранения данных» на стр. 45).

9

Административные функции

Работа с журналом IP-пакетов

В разделе **Журнал IP-пакетов** на основе различных параметров поиска можно сгенерировать 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 **Журнал IP-пакетов**.

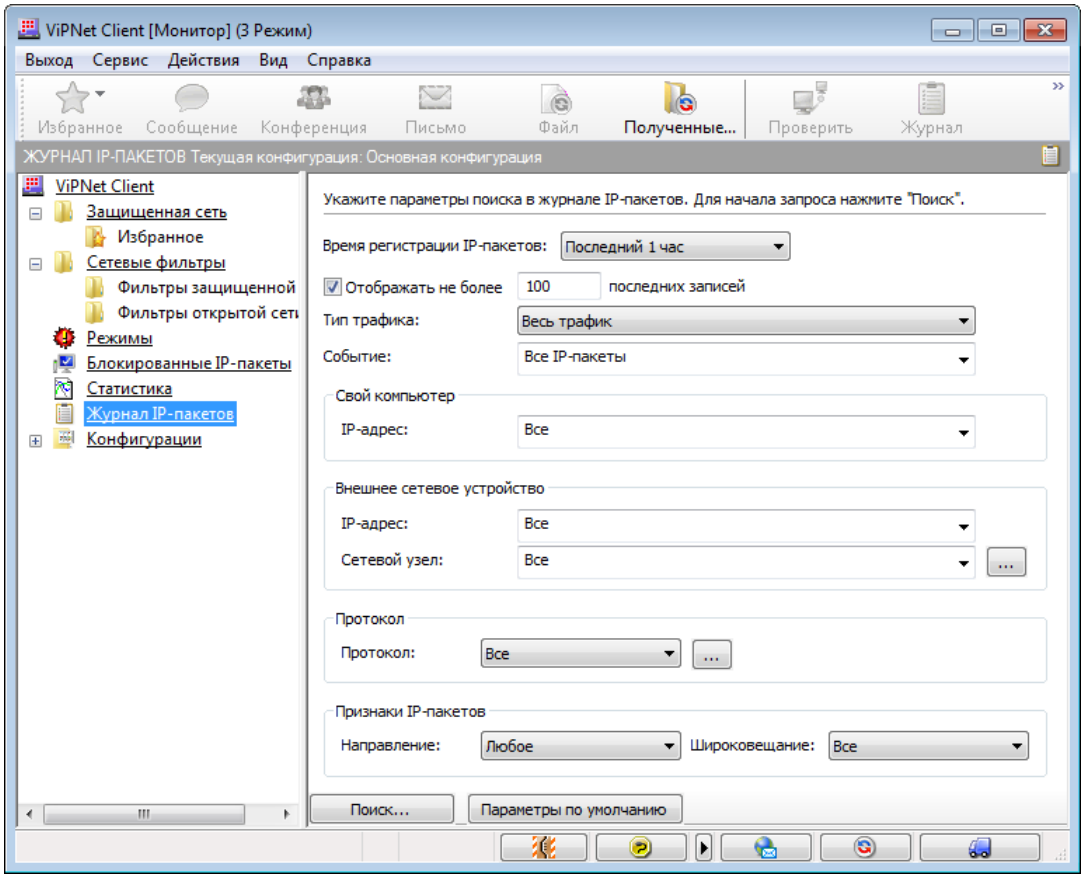


Рисунок 94: Настройка параметров поиска по журналу IP-пакетов

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 **Тип трафика** выберите один из пунктов:
  - **Весь трафик** — будут отображены записи обо всех IP-пакетах.
  - **Защищенный** — будут отображены записи о зашифрованных IP-пакетах, отправителем или получателем которых является данный сетевой узел.
  - **Открытый** — будут отображены записи об открытых IP-пакетах, отправителем или получателем которых является данный сетевой узел.
- 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. 357).
- В группе **Свой компьютер** укажите IP-адрес своего компьютера.
- В группе **Внешнее сетевое устройство** укажите IP-адрес 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 **Широковещание** укажите, какие пакеты требуется найти (**Все**, **Широковещательные**, **Нешироковещательные**).
- 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**.

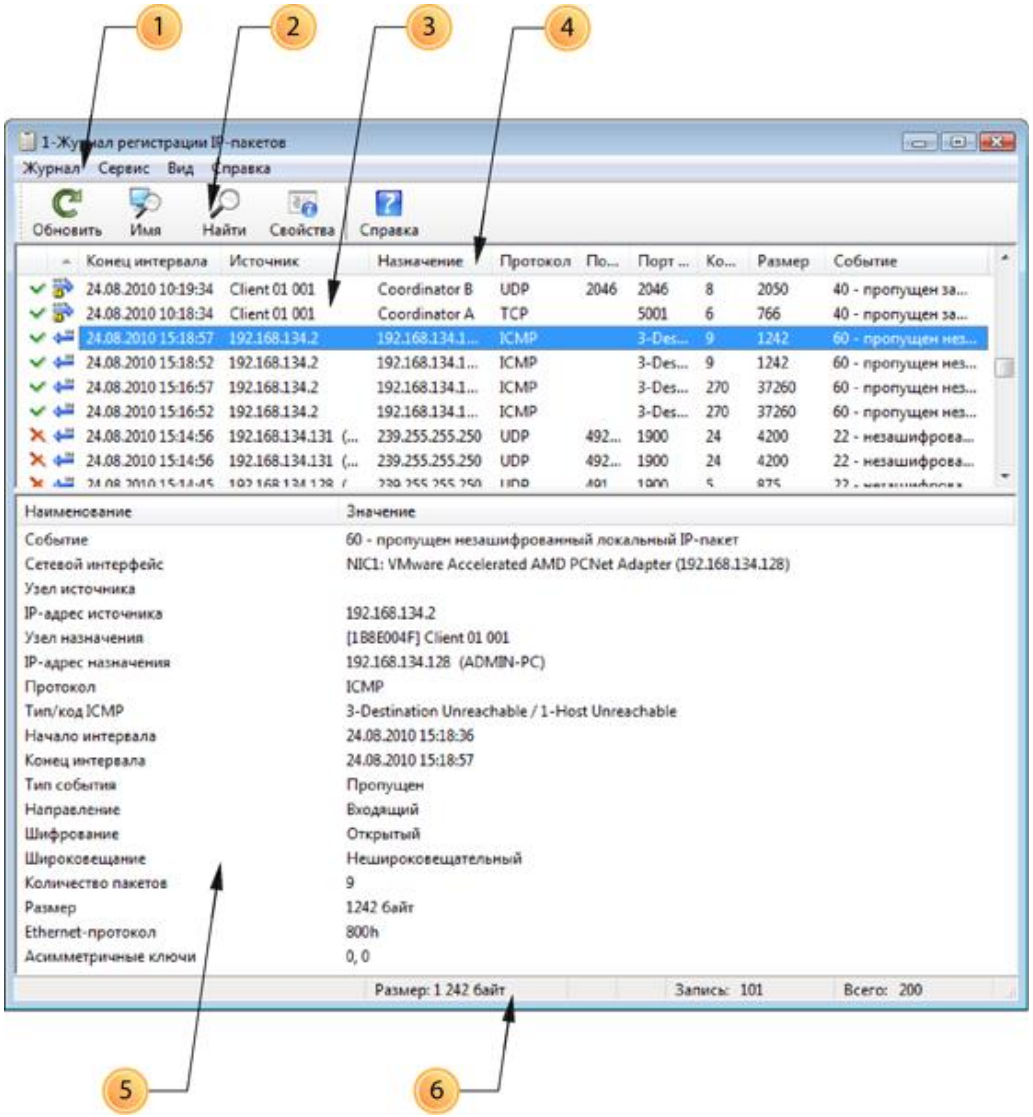


Рисунок 95: Просмотр журнала IP-пакетов

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 следующей таблице:

Название колонки	Описание
Тип события	Типы событий обозначаются следующими значками: — IP-пакеты заблокированы. — IP-пакеты пропущены. — IP-пакеты блокированы системой обнаружения атак. — IP-пакеты относятся к служебным событиям.
Свойства пакета	Свойства IP-пакетов обозначаются следующими значками: — открытые входящие IP-пакеты. — открытые исходящие IP-пакеты. — зашифрованные входящие IP-пакеты. — зашифрованные исходящие IP-пакеты.

Название колонки	Описание
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(на стр. 218).
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. 357).
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 виде веб-страницы.** Таблица с результатами поиска будет открыта в вашем веб-браузере. В строке адреса будет указан путь к файлу отчета.
- **Просмотр в Microsoft 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**.

Выделение 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**.

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**.

- 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.

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 качестве администратора (см. «Работа в программе с правами администратора» на стр. 251).

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 абонентского пункта, можно указать только параметры, доступные на абонентских пунктах.

---

5 Задайте параметры поиска (см. «Настройка параметров поиска IP-пакетов» на стр. 210) и нажмите кнопку **Поиск**.

Просмотр архивных 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** (см. «Настройка параметров регистрации IP-пакетов в журнале» на стр. 218). 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. 210).

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.

Настройка параметров регистрации IP-пакетов в журнале

Чтобы настроить параметры журнала IP-пакетов:

1 В главном окне ViPNet Монитор в меню **Сервис** выберите пункт **Настройки**.

2 На левой панели окна **Настройка** выберите раздел **Журнал IP-пакетов**.

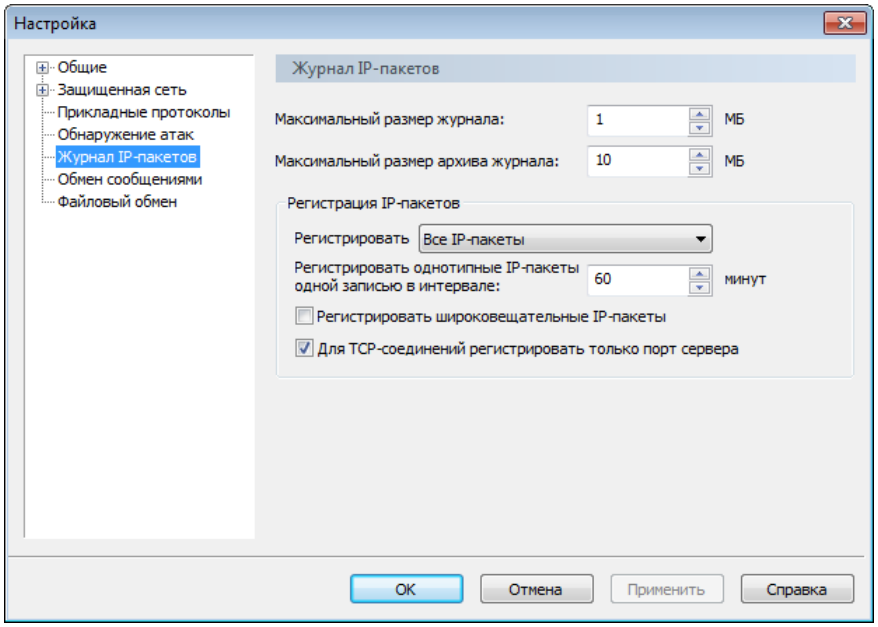


Рисунок 96: Настройка параметров журнала IP-пакетов

3 Задайте значения следующих параметров:

- В поле **Максимальный размер журнала** укажите размер журнала в мегабайтах (по умолчанию 1 МБ). 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**.

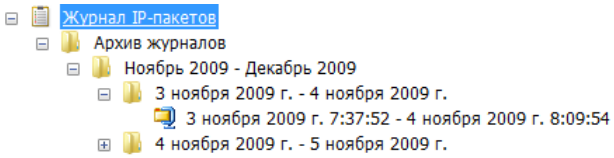


Рисунок 97: Архив журнала IP-пакетов

- В поле **Максимальный размер архива журнала** укажите размер архива в мегабайтах (по умолчанию 10 МБ). 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.

- Укажите, следует ли регистрировать **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 т.д.) 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 колонке **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 колонках **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 блокированных IP-пакетов

Примечание. В программе ViPNet Монитор версий 3.2 и выше удалена функция уведомления при блокировании IP-пакетов.

В разделе **Блокированные IP-пакеты** программы ViPNet Монитор содержится информация об IP-адресах узлов открытой сети, пакеты от которых были заблокированы программой ViPNet Client, и о параметрах этих пакетов.

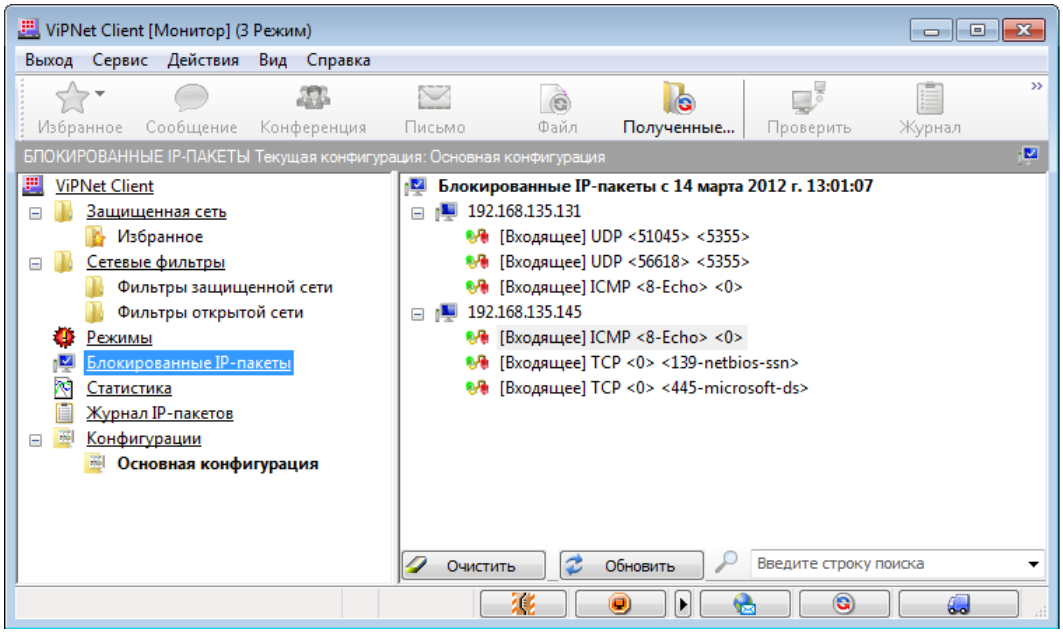


Рисунок 98: Список блокированных IP-пакетов

В списке отображаются записи об IP-пакетах, которые были заблокированы с момента, указанного в заголовке на панели просмотра, до текущего момента. Список очищается при запуске программы ViPNet Монитор или по нажатию кнопки **Очистить.**

По умолчанию разделе **Блокированные IP-пакеты** может быть отображено не более 300 IP-адресов, для каждого IP-адреса — не более 30 записей по каждому порту. При достижении указанных ограничений самые старые записи заменяются новыми.

Для управления отображением списка блокированных IP-пакетов выполните следующие действия:

- Чтобы очистить список блокированных пактов, нажмите кнопку **Очистить.**
- Чтобы обновить отображаемый список блокированных IP-пакетов, нажмите кнопку **Обновить.**
- Для быстрого поиска по разделу **Блокированные IP-пакеты** введите в расположенную внизу строку поиска часть IP-адреса или параметр, который требуется найти. В результате в списке будут отображены только те элементы, названия которых содержат введенный фрагмент текста.

Для получения более подробных сведений о заблокированных IP-пакетах выполните следующие действия:

- Чтобы узнать имя компьютера по IP-адресу, щелкните IP-адрес правой кнопкой мыши и в контекстном меню выберите пункт **Определить имя.**
- Чтобы просмотреть информацию о параметрах IP-пакета в отдельном окне, щелкните запись пакета правой кнопкой мыши, в контекстном меню выберите пункт **Открыть.**
- Для поиска информации о пакетах определенного типа, перейдите к журналу IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 210). Для этого:
  - В разделе **Блокированные IP-пакеты** выделите записи об IP-адресах либо записи о протоколах, информацию о которых требуется посмотреть.
  - Щелкните правой кнопкой мыши и в появившемся контекстном меню выберите **Журнал регистрации IP-пакетов.**
  - Откроется раздел **Журнал IP-пакетов**, где в качестве параметров поиска подставлены параметры выделенных IP-адресов и протоколов.
  - Чтобы произвести поиск в соответствии с установленными автоматически параметрами, в разделе **Журнал IP-пакетов** нажмите кнопку **Поиск.**

Создание правила доступа на основе параметров блокированных IP-пакетов

Если необходимо пропускать IP-пакеты с параметрами, соответствующими параметрам заблокированых IP-пакетов, следует создать правило фильтрации открытого трафика. Для этого выполните следующие действия:

1 В программе ViPNet Монитор выберите раздел **Блокированные IP-пакеты.**

2 На правой панели щелкните правой кнопкой мыши заблокированное соединение, которое должно быть разблокировано для обеспечения комфортной работы с открытыми ресурсами, и в контекстном меню выберите пункт **Создать правило.**

Если выбрать в списке IP-адрес, принадлежащий отправителю или получателю заблокированных IP-пакетов, то далее при добавлении фильтра по умолчанию будет предложено создать фильтр для всех типов протоколов без учета номеров портов и направления соединения. Такое правило разрешает любой обмен трафиком с выбранным IP-адресом.

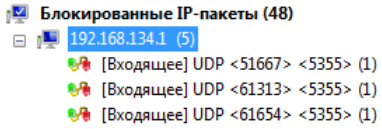


Рисунок 99: Выбран IP-адрес

Если выбрать запись соединения, то далее при добавлении фильтра будет предложено создать фильтр для конкретного протокола, направления соединения, портов источника и назначения (эти данные будут автоматически получены из выбранной записи).

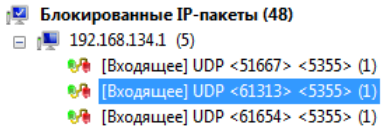


Рисунок 100: Выбрано конкретное соединение

3 В зависимости от типа заблокированного соединения, в окне **Локальное правило** или **Широковещательное правило** проверьте, устраивает ли вас информация, полученная автоматически из заблокированного соединения. Если необходимо, внесите соответствующие изменения.

4 Нажмите кнопку **OK**, чтобы автоматически добавить фильтр к созданному правилу.

Нажмите кнопку **Отмена**, чтобы добавить фильтр позже.

5 После нажатия кнопки **OK** проверьте параметры, установленные автоматически. Если необходимо, внесите нужные изменения.

6 По окончании нажмите кнопку **OK**. В окне ViPNet Монитор откроется раздел **Фильтры открытой сети.**

Подробнее о создании правил открытой сети см. раздел Создание правил для открытой сети(на стр. 137).

Просмотр статистики фильтрации IP-пакетов

Чтобы просмотреть статистику фильтрации IP-пакетов, в окне программы ViPNet Монитор на панели навигации выберите раздел **Статистика**.

В разделе **Статистика** представлены данные о количестве входящих и исходящих IP-пакетов, которые были пропущены или заблокированы в соответствии с заданными правилами фильтрации трафика. Эта информация может быть полезна при первоначальной настройке программы ViPNet Монитор.

Чтобы обнулить статистику IP-пакетов, нажмите кнопку **Очистить**.

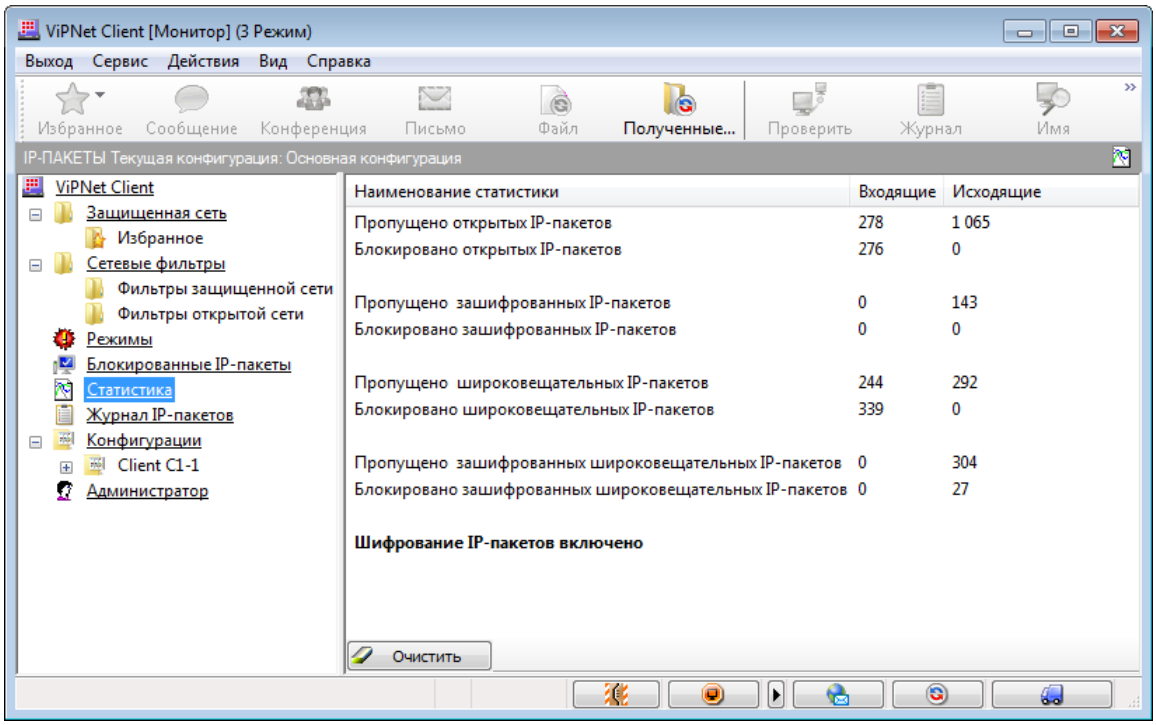


Рисунок 101: Просмотр статистики IP-пакетов

Просмотр информации о клиенте, времени работы программы и числе соединений

Чтобы получить информацию о сети ViPNet, в которой находится данный узел ViPNet, о пользователе, который произвел вход в программу, сведения о соединениях узла и другую дополнительную информацию, в окне программы ViPNet Монитор выберите раздел **ViPNet Client**.

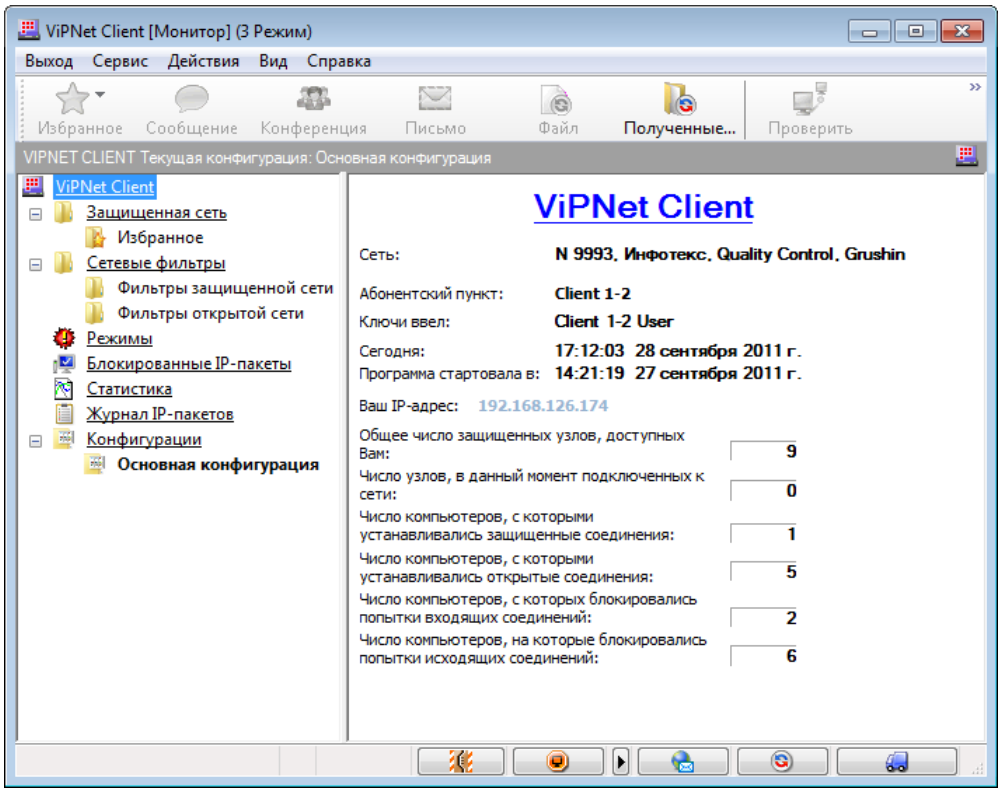


Рисунок 102: Раздел общей информации об узле ViPNet

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 сети Интернет. 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 **Конфигурация** и в контекстном меню выберите **Создать новую конфигурацию**.

   В списке конфигураций появится элемент **Новая конфигурация**.

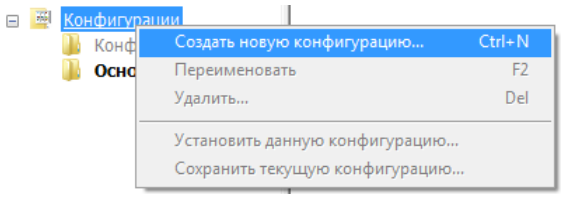
   

   Рисунок 103: Создание новой конфигурации

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 **Установить данную конфигурацию**.

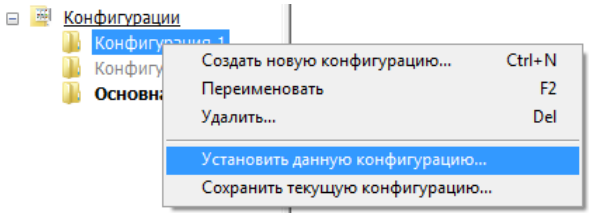


Рисунок 104: Установка конфигурации

Если на сетевом узле программа ViPNet Client интегрирована с программой ViPNet SafeDisk-V, то при смене защищенной конфигурации на незащищенную или незащищенной конфигурации на защищенную доступ к контейнерам ViPNet SafeDisk-V будет запрещен или разрешен соответственно. Подробнее об интеграции программы ViPNet Client с программой ViPNet SafeDisk-V см. в разделе Общие сведения об интеграции ViPNet Client с ViPNet SafeDisk-V(на стр. 158).

4 Выполните требуемые изменения в настройках ViPNet Монитор.

Если на сетевом узле программа ViPNet Client интегрирована с программой ViPNet SafeDisk-V, при необходимости измените настройки интеграции для работы с контейнерами ViPNet SafeDisk-V (см. «Настройка параметров работы с ViPNet SafeDisk-V для текущей конфигурации программы ViPNet Монитор» на стр. 162).

5 Чтобы сохранить изменения в настройках программы для текущей конфигурации, щелкните ее правой кнопкой мыши и в контекстном меню выберите пункт **Сохранить текущую конфигурацию**. В окне подтверждения нажмите кнопку **Да**.

Если в программе создано несколько конфигураций, то при запуске ViPNet Монитор откроется окно выбора конфигурации.

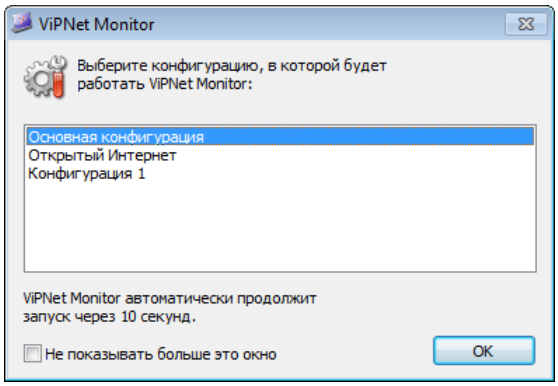


Рисунок 105: Выбор конфигурации при запуске программы

Конфигурация «Открытый Интернет»

Если абонентский пункт связан с координатором, который зарегистрирован в прикладной задаче «Сервер Открытого Интернета», в списке конфигураций программы ViPNet Монитор присутствует конфигурация «Открытый Интернет».

Если доступ абонентских пунктов в Интернет организован через сервер Открытого Интернета:

- Для работы в защищенной сети установите любую конфигурацию, кроме конфигурации «Открытый Интернет».

  В этом случае соединение с сервером Открытого Интернета установить невозможно. Следовательно, невозможно получить доступ к Интернету.

- Для работы с ресурсами Интернета установите конфигурацию «Открытый Интернет».

  В этом случае:

  - Невозможно установить соединение с какими-либо сетевыми узлами ViPNet, кроме сервера Открытого Интернета.
  - Запрещена работа с контейнерами ViPNet SafeDisk-V, если на сетевом узле программа ViPNet Client интегрирована с программой ViPNet SafeDisk-V (см. «Общие сведения об интеграции ViPNet Client с ViPNet SafeDisk-V» на стр. 158).

Примечание. При загрузке программы ViPNet Монитор в конфигурации «Открытый Интернет» автоматически устанавливаются следующие настройки:

- 2 режим безопасности;
- в разделе **Открытая сеть** фильтр, разрешающий соединение по протоколу DHCP.

При необходимости режим безопасности может быть изменен на первый.

Таким образом, абонентский пункт подключен либо только к защищенной сети ViPNet, либо только к Интернету. Это позволяет изолировать компьютер, обменивающийся потенциально опасным трафиком в Интернете, от остальных узлов сети ViPNet.

Удаленное управление сетевыми узлами ViPNet

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.

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.

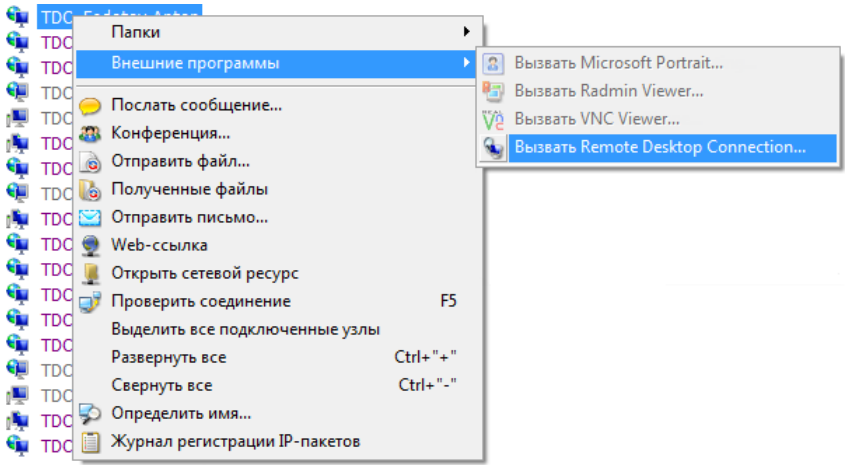


Рисунок 106: Вызов внешней программы

Команды подменю **Внешние программы** активны, только если на компьютере установлены соответствующие программы. 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 ввода пароля откроется удаленный доступ к сетевому узлу.

Примечание. Следует иметь в виду, что для успешного подключения к сетевому узлу ViPNet требуется правильно настроить используемое для удаленного доступа программное обеспечение.

Например, если используется программа 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.

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. 232).
2. В программе ViPNet Монитор:
   - Настройте параметры сохранения пароля при входе в программу. Для этого войдите в программу с правами администратора (см. «Работа в программе с правами администратора» на стр. 251). 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. 256).

Примечание. Подразумевается, что на удаленном узле используется аутентификация пользователя по паролю (см. «Способы аутентификации пользователя» на стр. 75).

- Включите опцию автоматической блокировки компьютера при запуске программы с целью предотвращения несанкционированной работы (подробнее см. раздел Параметры, влияющие на блокировку компьютера(на стр. 207)).

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**.

   При использовании ОС Windows XP/Server 2003 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).

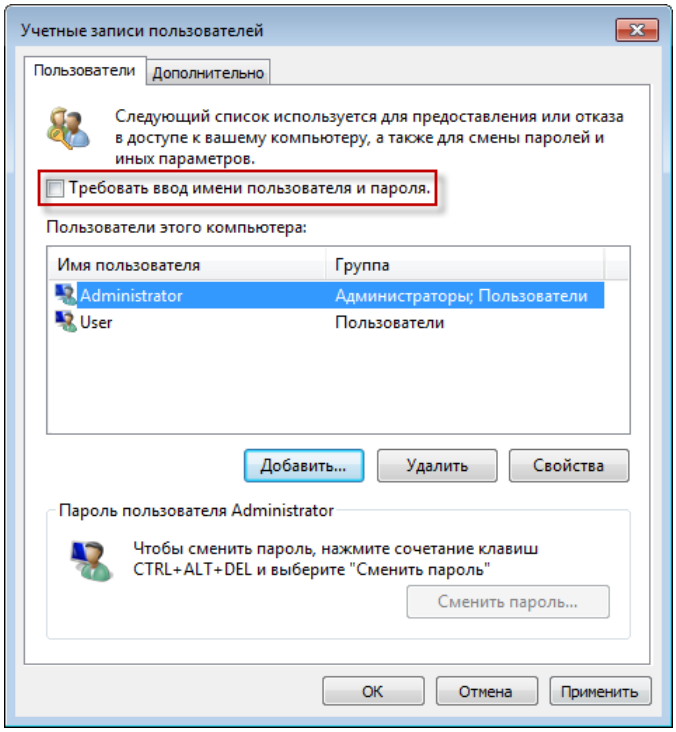


Рисунок 107: Настройка автоматического входа в ОС на вкладке Пользователи

- На вкладке **Дополнительно** (**Advanced**) снимите флажок **Требовать нажатия CTRL+ALT+DELETE** (**Require users to press Ctrl+Alt+Delete**).

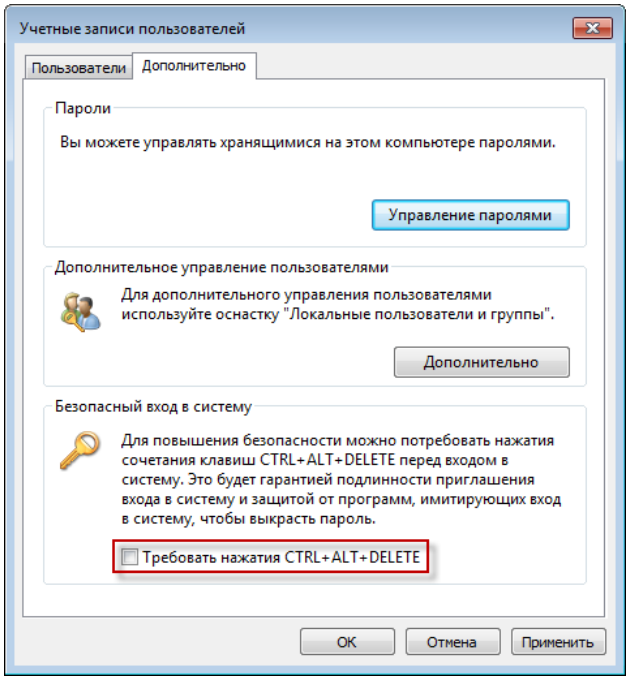


Рисунок 108: Настройка автоматического входа в ОС на вкладке Дополнительно

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 ручная правка реестра.

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 ветки 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**.

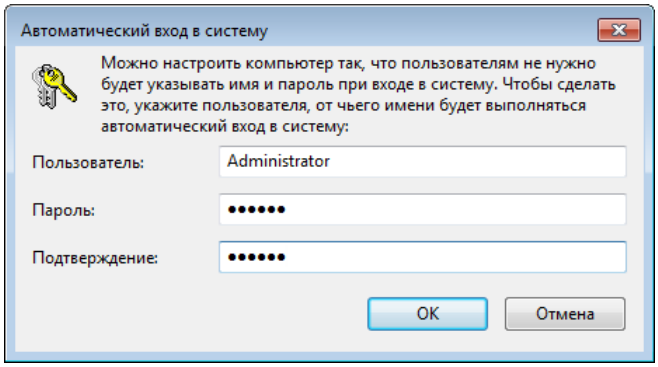


Рисунок 109: Окно ввода пароля для автоматического входа в систему

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**.

Настройка терминального сервера

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.

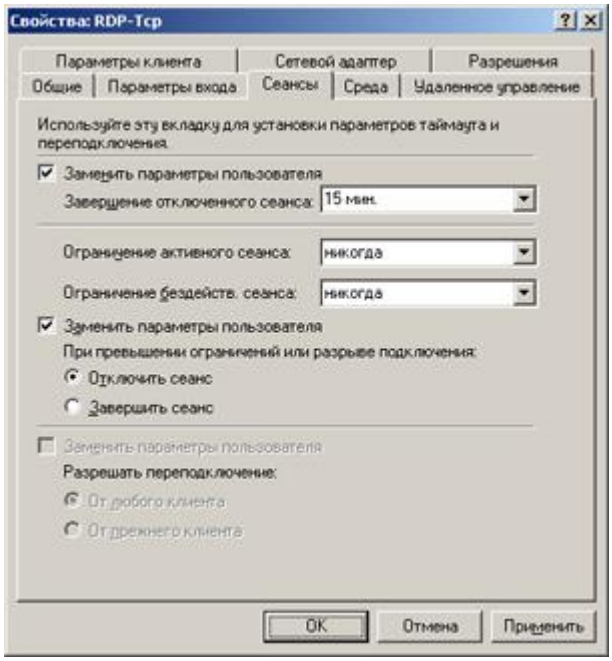


Рисунок 110: Неверные настройки терминального сервера

Для решения проблемы следует вернуть все настройки в состояние по умолчанию, сняв все флажки **Заменить параметры пользователя**.

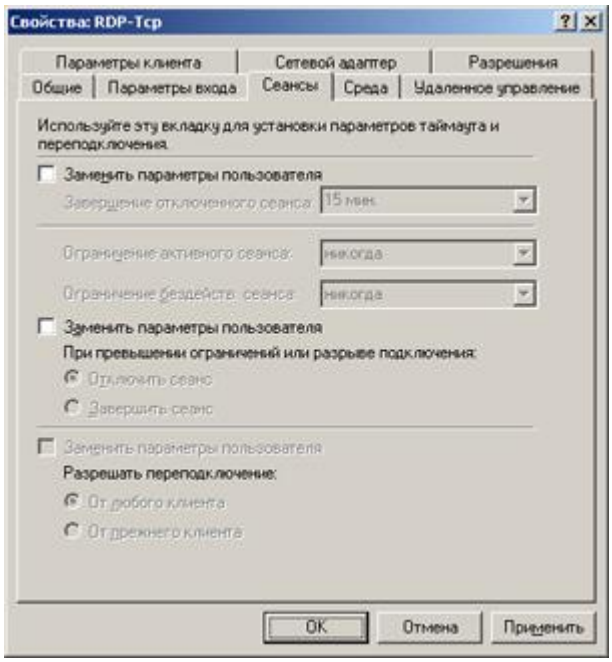


Рисунок 111: Верные настройки терминального сервера

Примечание. В операционной системе Windows Server 2008 R2 службы терминалов называются службами удаленных рабочих столов.

Установка стороннего программного обеспечения

Загрузить установочный комплект Remote Administrator можно со страницы Radmin http://www.radmin.com/download/. Пакет Remote Administrator включает клиентскую и серверную части.

Загрузить установочный комплект VNC можно со страницы RealVNC http://www.realvnc.com/download.html. Пакет VNC включает клиентскую и серверную части.

Загрузить установочный комплект Remote Desktop Connection можно с web-сайта Microsoft http://www.microsoft.com/windowsxp/downloads/tools/RDCLIENTDL.mspx. В операционных системах Windows 2k/XP/2003/Vista/2008/7 программа Remote Desktop Connection установлена по умолчанию.

Настройка параметров безопасности

Описанные в настоящем разделе функции выполняются в окне **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 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. 334), следует сменить пароль пользователя.

Кроме того, рекомендуется менять пароль пользователя после первичной инициализации, при первом входе в программу ViPNet. 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.**

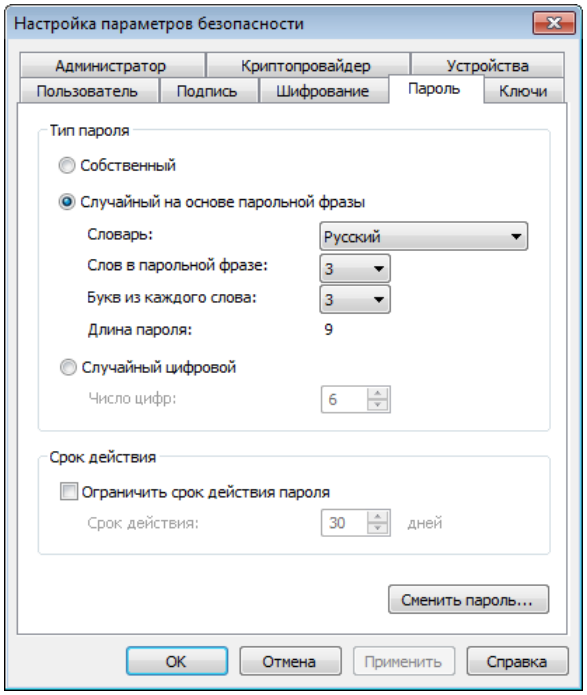


Рисунок 112: Смена текущего пароля пользователя

2 В группе **Тип пароля** выберите тот тип, которому должен соответствовать новый пароль:

- **Собственный** — пароль, определяемый пользователем (см. «Выбор собственного пароля» на стр. 240);
- **Случайный на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы, по заданным параметрам (см. «Выбор пароля на основе парольной фразы» на стр. 240);
- **Случайный цифровой** — пароль, формируемый автоматически из заданного числа цифр (см. «Выбор цифрового пароля» на стр. 241).

3 Нажмите кнопку **Сменить пароль**, после чего в зависимости от выбранного типа в появившемся окне выполните действия, необходимые для смены пароля и описанные в соответствующем подразделе.

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 112 на стр. 239) 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.

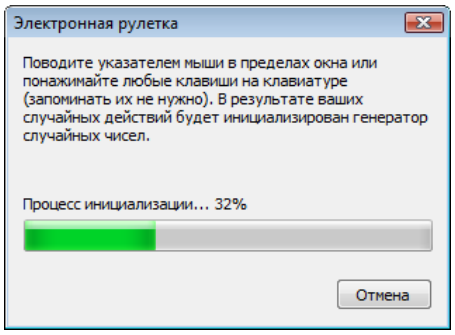


Рисунок 113: Электронная рулетка

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 112 на стр. 239) 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 и (или) парольную фразу, отображенную 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 112 на стр. 239) 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

Для настройки параметров шифрования:

1 В окне **Настройка параметров безопасности** откройте вкладку **Шифрование**.

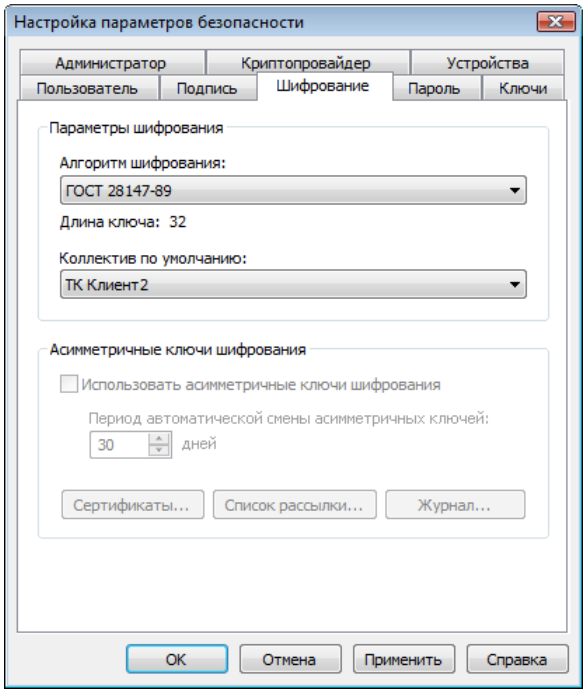


Рисунок 114: Настройка параметров шифрования

2 Если пользователь, от имени которого выполнен запуск программы ViPNet Client, зарегистрирован на данном сетевом узле более чем в одном коллективе, в разделе **Параметры шифрования** в списке **Коллектив по умолчанию** выберите тот коллектив, от имени которого необходимо осуществлять шифрование исходящих сообщений.

Внимание! В списке **Алгоритм шифрования** рекомендуется оставить значение, используемое по умолчанию.

Настройка параметров работы криптопровайдера ViPNet

В программе ViPNet Монитор используется криптопровайдер, по своей функциональности полностью соответствующий ПО ViPNet CSP. Криптопровайдер ViPNet обеспечивает вызов криптографических функций через интерфейс Microsoft

CryptoAPI 2.0. Это позволяет вызывать криптографические функции из различных приложений Microsoft и другого ПО, использующего данный интерфейс.

Для настройки параметров работы с криптопровайдером ViPNet:

1 В окне **Настройка параметров безопасности** откройте вкладку **Криптопровайдер**.

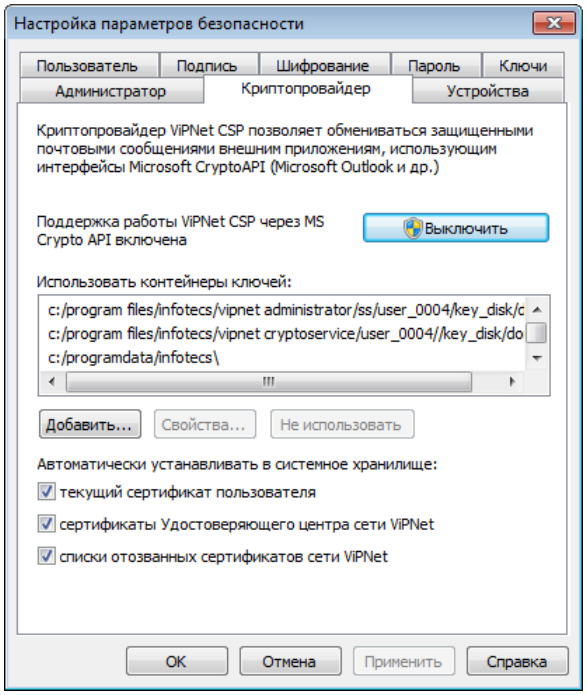


Рисунок 115: Настройка параметров работы с криптопровайдером ViPNet

2 Убедитесь в том, что криптопровайдер ViPNet включен. Об этом свидетельствует сообщение «Поддержка работы ViPNet CSP через MS Crypto API включена».

Внимание! Включение и выключение криптопровайдера ViPNet выполняется путем включения и выключения драйвера поддержки работы криптопровайдера в ОС. Поэтому для включения и выключения криптопровайдера ViPNet необходимы права администратора Windows. Если используемая учетная запись Windows не обладает правами администратора и в системе включен контроль учетных записей (UAC), при попытке включить или выключить криптопровайдер потребуется ввести пароль учетной записи администратора Windows.

После включения или выключения работы криптопровайдера через интерфейс MS Crypto API необходимо перезагрузить компьютер.

---

3 Добавьте контейнер ключей, который должен использоваться криптопровайдером, с помощью кнопки **Добавить**.

В случае, если обращение к контейнеру выполняется из приложений через интерфейс MS Crypto API, контейнер добавляется в список автоматически.

4 В окне **ViPNet CSP – инициализация контейнера ключа** укажите расположение контейнера ключей:

- папку на диске;
- внешнее устройство с указанием его параметров.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

Внимание! В случае если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.x, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

Нажмите кнопку **ОК**. Полный путь к выбранному контейнеру отобразится в списке **Использовать контейнеры ключей.**

Примечание. В списке **Использовать контейнеры ключей** отображаются пути к контейнерам ключей, в которых хранятся личные сертификаты пользователя. Имя контейнера с текущим сертификатом и путь к нему отображаются на вкладке **Ключи** (см. Рисунок 161 на стр. 333).

---

5 При дальнейшей работе с контейнером:

- Для просмотра и (или) изменения свойств контейнера ключей нажмите кнопку **Свойства** (см. «Работа с контейнером ключей» на стр. 332).
- Если сертификат, соответствующий закрытому ключу, который хранится в контейнере, больше не используется, контейнер можно удалить из списка. Для удаления контейнера из списка контейнеров, используемых криптопровайдером, нажмите кнопку **Не использовать.**

6 Установите нужные флажки, позволяющие выбрать, какие сертификаты, в случае их отсутствия в системном хранилище Windows, необходимо устанавливать в это хранилище автоматически (см. «Установка в хранилище автоматически» на стр. 307):

- **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 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 Manager в составе обновления ключей.

7 Нажмите кнопку **ОК**.

Работа с внешними устройствами хранения данных

Внешние устройства хранения данных могут использоваться в программе ViPNet Монитор в процессе аутентификации пользователя (в способах **Пароль на устройстве** и **Устройство**), а также для хранения контейнера ключей (см. «Работа с контейнером ключей» на стр. 332).

Для работы с внешним устройством:

1 Откройте вкладку **Устройства**.

2 Подключите нужные устройства.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

Наименования подключенных устройств отобразятся в списке **Подключенные устройства**, а наименования контейнеров ключей, которые хранятся на выбранном устройстве, — в списке **Контейнеры ключей на устройстве**.

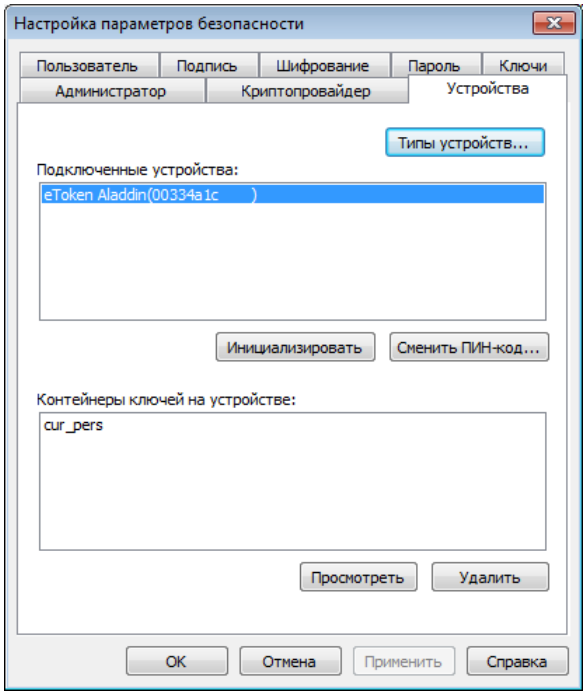


Рисунок 116: Управление внешними устройствами хранения данных

Примечание. Контейнеры, сформированные в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Manager, имеют наименование `sgn_cont`. При поступлении на сетевой узел ключей пользователя новому контейнеру присваивается наименование вида `sgn_cont<порядковый номер предыдущего контейнера + 1>` (например, `sgn_cont1`, `sgn_cont2` и так далее).

3 Задайте типы устройств, на которых необходимо выполнять поиск контейнеров ключей, с помощью кнопки **Типы устройств**.

В появившемся окне **Настройка списка опрашиваемых устройств** выберите типы устройств с помощью флажков, после чего нажмите кнопку **ОК**.

Примечание. По умолчанию все флажки в окне **Настройка списка опрашиваемых устройств** установлены. Если снять флажки, соответствующие ненужным устройствам, можно незначительно ускорить работу программы. Например, если к компьютеру подключен считыватель карт, который не должен использоваться в ПО ViPNet, снятие соответствующего флажка позволит отключить опрос этого устройства и ускорить работу функций электронной подписи.

4 При необходимости проведите инициализацию подключенного устройства (см. «Инициализация устройства» на стр. 247).

5 При необходимости измените ПИН-код администратора и (или) ПИН-код пользователя для подключенного устройства (см. «Смена ПИН-кода устройства» на стр. 249).

6 При необходимости просмотрите и (или) измените свойства контейнера ключей, который хранится на подключенном устройстве, с помощью кнопки **Просмотреть** (см. «Работа с контейнером ключей» на стр. 332).

7 Если контейнер, который хранится на подключенном устройстве, не нужно использовать для аутентификации пользователя ViPNet или электронной подписи, удалите этот контейнер с помощью кнопки **Удалить.**

Инициализация устройства

Инициализация устройства в ПО ViPNet требуется в том случае, если необходимо полностью очистить это устройство.

Для инициализации подключенного устройства:

1 Убедитесь в том, что устройство, которое необходимо инициализировать, не содержит ценной информации. При необходимости перенесите все данные, хранящиеся на устройстве, на другой съемный носитель или жесткий диск компьютера.

2 На вкладке **Устройства** (см. Рисунок 116 на стр. 246) в списке **Подключенные устройства** выберите нужное устройство.

Внимание! В случае если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.x, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

---

3 Нажмите кнопку **Инициализировать.**

4 В окне с предупреждением об удалении данных с устройства нажмите кнопку **Да.**

5 В появившемся окне **Инициализация** введите ПИН-код администратора.

6 При необходимости смены ПИН-кода пользователя введите в двух других полях окна также новый ПИН-код пользователя.

7 Нажмите кнопку **ОК**.

Внимание! Перед инициализацией устройства Rutoken или Rutoken ЭЦП в приложении ViPNet следует предварительно инициализировать устройство с помощью программы «Панель управления Рутокен», установив для параметра **Политика смены PIN-кода Пользователя** значение **Администратором**.

В случае если вы используете устройство ОКБ САПР Шипка (Shipka) и произвели инициализацию в приложении ViPNet, для корректной работы устройства вам также необходимо выполнить инициализацию с помощью утилиты ОКБ САПР «Параметры авторизации» (см. «Информация о внешних устройствах хранения данных» на стр. 45).

Программы «Панель управления Рутокен» и «Параметры авторизации» не входят в комплект поставки продуктов ViPNet.

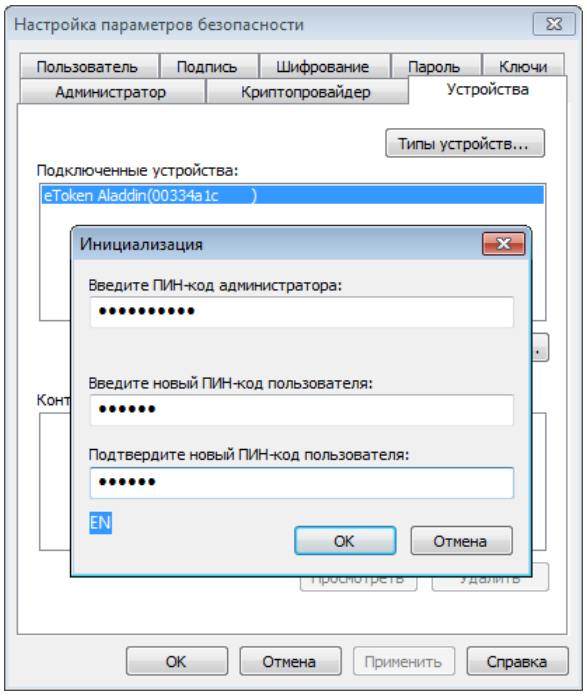


Рисунок 117: Инициализация устройства

Теперь подключенное устройство полностью отформатировано.

Смена ПИН-кода устройства

Смена ПИН-кода устройства может потребоваться в связи с истечением срока действия пароля согласно регламенту организации или по другим причинам, утвержденным регламентом.

Для того чтобы сменить ПИН-код администратора или пользователя подключенного устройства (в зависимости от уровня полномочий на доступ к устройству):

1. Нажмите кнопку **Смена ПИН-кода**.
2. В окне **Смена ПИН-кода** выберите тип изменяемого ПИН-кода.
3. В поле **Введите старый ПИН-код** укажите прежний ПИН-код, а в оставшихся двух полях — новый ПИН-код, после чего нажмите кнопку **ОК**.

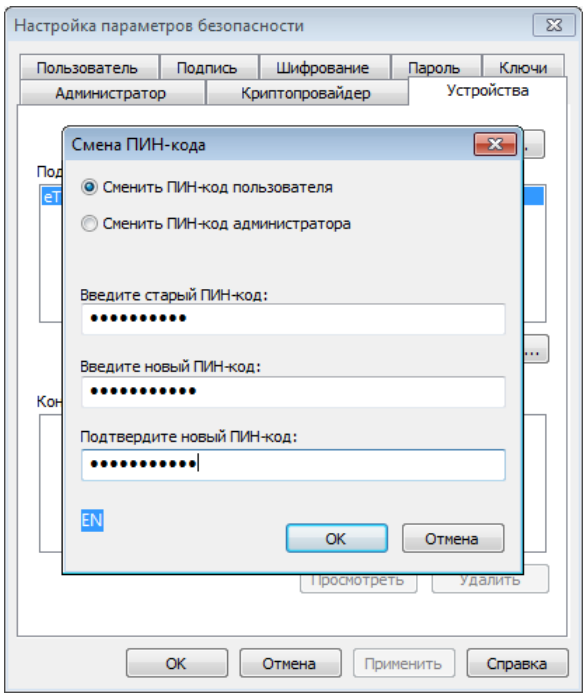


Рисунок 118: Смена ПИН-кода устройства

Теперь для доступа к устройству необходимо использовать новый ПИН-код.

Синхронизация компьютера с КПК

Чтобы обеспечить возможность синхронизации компьютера с КПК (на базе Windows Mobile 5.0/6.x) при помощи программы ActiveSync 4.x (или с помощью Центра устройств Windows Mobile на Windows Vista и Windows 7), выполните одно из следующих действий:

- В программе ViPNet Монитор включить правило **Windows Mobile-based device** (см. «Фильтры открытой сети, настроенные по умолчанию» на стр. 134).
- На КПК в меню **Настройка > Подключения > От USB к ПК** снять флажок **Включить режим расширенных сетевых возможностей**.

Если КПК был подключен к компьютеру, то для синхронизации его нужно отключить и снова подключить.

Работа в программе с правами администратора

В программе ViPNet Монитор предусмотрена возможность работы с правами администратора. В режиме администратора 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. 252).
- Журнал событий, содержащий записи о смене режима безопасности и других действиях, совершенных пользователем или администратором.
- Возможность просмотреть журнал IP-пакетов определенного сетевого узла ViPNet (см. «Работа с журналом IP-пакетов» на стр. 210).

При работе в режиме администратора все ограничения, накладываемые уровнем полномочий пользователя, снимаются.

Чтобы войти в программу в качестве администратора:

1. Выполните одно из действий:
   - В окне программы ViPNet Монитор в меню **Сервис** выберите пункт **Вход администратора**.
   - Щелкните значок программы  в области уведомлений правой кнопкой мыши и в контекстном меню выберите пункт **Вход 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 администратора**.
2. В окне **Пароль администратора** введите пароль администратора сетевого узла ViPNet.

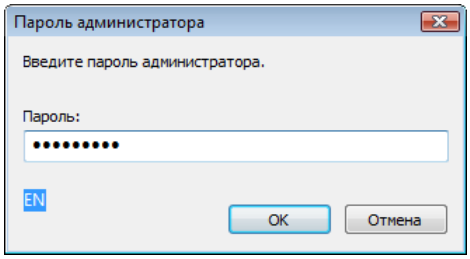


Рисунок 119: Ввод пароля администратора сетевого узла

3 Нажмите кнопку **OK**.

4 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 OFFICE пароль администратора для всех сетевых узлов хранится в файле `ViPNet_a.txt`, который находится в подпапке `\NCC\KEYS` в папке установки программы ViPNet Manager.

Дополнительные настройки программы ViPNet Монитор

После входа в ViPNet Монитор в качестве администратора 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 качестве администратора (см. «Работа в программе с правами администратора» на стр. 251).

2 В окне программы ViPNet Монитор на левой панели выберите раздел **Администратор**.

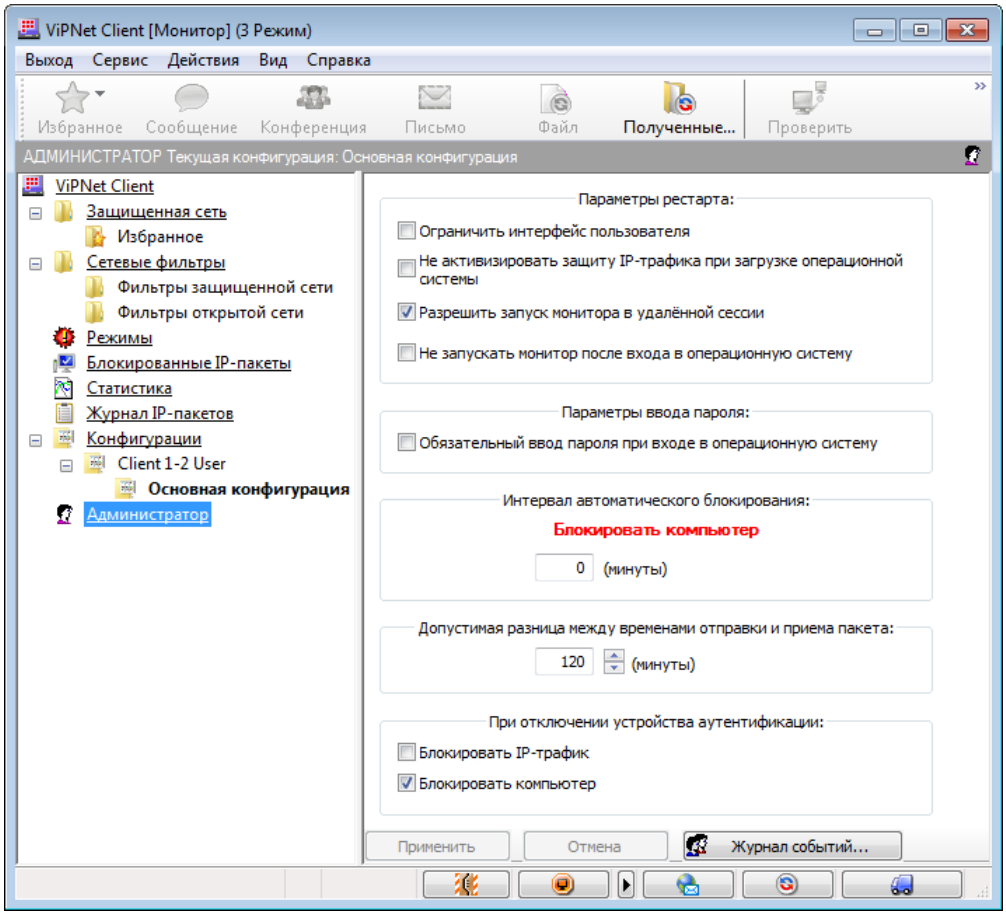


Рисунок 120: Настройка дополнительных параметров в режиме администратора

3 В разделе **Администратор**:

- Чтобы запретить пользователю создавать, изменять или удалять какие-либо правила и фильтры, установите флажок **Ограничить интерфейс пользователя**.

  В режиме ограниченного интерфейса пользователю будет доступен только раздел **Защищенная сеть**. Кроме того, в меню **Сервис** будет недоступен пункт **Импорт настроек**. В окне **Настройка** будут недоступны:

  - Флажок **Блокировать все протоколы, кроме IP, ARP, RARP** в разделе **Общие**.
  - Флажок **Блокировать компьютер** в подразделе **Общие > Запуск и аварийное завершение**.
  - Все параметры в подразделе **Защищенная сеть > Дополнительные параметры**.
  - Параметры обработки прикладных протоколов в разделе **Прикладные протоколы**.

- Все флажки в разделе **Обнаружение атак**.
- Все параметры в разделе **Журнал IP-пакетов**.
- Флажок **Разрешить использование контейнеров SafeDisk-V** в разделе **SafeDisk-V**.

В окне **Настройка параметров безопасности** будут отключены элементы управления на вкладках **Шифрование**, **Пароль**, **Ключи**, **Криптопровайдер**. Пользователь не сможет создавать, изменять или удалять никакие правила и фильтры.

Примечание. В режиме ограниченного интерфейса, щелкнув правой кнопкой мыши значок  в области уведомлений, пользователь может:

- Изменить режим безопасности (доступны только 1, 2 и 3 режимы).
- Установить одну из ранее созданных конфигураций.
- Заблокировать компьютер.

- Чтобы отключить защиту компьютера с помощью программного обеспечения ViPNet, 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, будет включен пятый режим безопасности, соответственно, компьютер не будет защищен. Однако для включения защиты IP-трафика можно будет вручную запустить программу ViPNet Монитор и пройти аутентификацию.

Примечание. Не рекомендуется устанавливать этот флажок на координаторах, а также на абонентских пунктах, которые имеют динамический IP-адрес или должны взаимодействовать узлами, имеющими динамический IP-адрес.

- Чтобы запретить другим пользователям (имеющим учетные записи на данном компьютере) запускать ViPNet Монитор на данном сетевом узле во время сеанса удаленной работы (например, с помощью Remote Desktop), снимите флажок **Разрешить запуск монитора в удаленной сессии** (по умолчанию 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.

- Чтобы после загрузки Windows защита трафика была включена, но программа «Монитор» не запускалась, установите флажок **Не запускать монитор после входа в операционную систему**. В этом случае после загрузки Windows будет включен последний использовавшийся режим безопасности, защита компьютера будет активна.
- Чтобы при загрузке Windows пользователь не мог отказаться от запуска ViPNet Монитор, установите флажок **Обязательный ввод пароля при входе в операционную систему**. В этом случае в окне ввода пароля пользователя ViPNet 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.

- В поле **Интервал автоматического блокирования** введите продолжительность интервала в минутах. Если в течение указанного времени не будут использоваться клавиатура и мышь, программа автоматически включит текущий (последний использовавшийся) режим блокировки компьютера (см. «Блокировка компьютера и IP-трафика» на стр. 206). Если значение интервала блокирования равно 0 (установлено по умолчанию), то автоматическая блокировка компьютера отключена.
- В поле **Допустимая разница между временами отправки и приема пакета** можно ввести интервал времени в минутах. Если разница между временем отправки входящего пакета и временем его приема больше указанного интервала, пакет будет заблокирован.

  Действие данной функции распространяется на сетевые узлы ViPNet, с которыми у данного узла есть связь (эти узлы отображаются в разделе **Защищенная сеть**). При включении данной функции следует учитывать время на сетевых узлах ViPNet, с которыми осуществляется взаимодействие. Если эти узлы находятся в другом часовом поясе (или время на этих узлах установлено неправильно), IP-пакеты от этих узлов могут быть заблокированы.
- Чтобы при отключении внешнего устройства, которое было использовано для аутентификации пользователя, IP-трафик не блокировался, снимите флажок **Блокировать IP-трафик** (по умолчанию флажок установлен). Если флажок

установлен, то при отключении устройства программа автоматически включит режим блокировки IP-трафика или режим блокировки компьютера и IP-трафика (в зависимости от того, снят или установлен флажок **Блокировать компьютер**).

- Чтобы при отключении внешнего устройства, которое было использовано для аутентификации пользователя, компьютер не блокировался, снимите флажок **Блокировать компьютер** (по умолчанию флажок установлен). Если флажок установлен, то при отключении устройства программа автоматически включит режим блокировки компьютера или режим блокировки компьютера и IP-трафика (в зависимости от того, снят или установлен флажок **Блокировать IP-трафик**).

Примечание. Настройки, заданные с помощью флажков из группы **При отключении устройства аутентификации**, учитываются только в способах аутентификации **Пароль на устройстве** и **Устройство** (см. «Способы аутентификации пользователя» на стр. 75). Эти настройки определяют режим блокировки, который будет использоваться при отключении внешнего устройства (см. «Особенности блокировки компьютера при использовании внешнего устройства для аутентификации пользователя» на стр. 208).

4 Чтобы сохранить настройки, нажмите кнопку **Применить**. Чтобы отказаться от изменений, нажмите кнопку **Отменить.**

Дополнительные настройки параметров безопасности

Помимо дополнительных параметров настройки в разделе **Администратор**, во время работы с правами администратора (см. «Работа в программе с правами администратора» на стр. 251) сетевого узла 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 Client.

Примечание. Если для управления сетью ViPNet используется программа ViPNet Manager, изменить состояние флажка **Разрешить сохранение пароля в реестре** невозможно, если в программе ViPNet Manager на вкладке **Полномочия** для данного сетевого узла задан параметр **Разрешить сохранять пароль** или **Запретить сохранять пароль**. 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 спискам сертификатов из ЦУС** — 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 (см. «Способы аутентификации пользователя» на стр. 75) 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 качестве администратора (см. «Работа в программе с правами администратора» на стр. 251).
2. В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите кнопку **Изменить**.
3. В окне **Способ аутентификации** выберите в списке один из способов:
   - **Пароль**. Для входа в программу ViPNet Монитор требуется ввести пароль пользователя. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к персональной ключевой информации пользователя.
   - **Пароль на устройстве**. При выборе этого способа аутентификации необходимо подключить внешнее устройство, на котором будет сохранен парольный ключ пользователя.

     Для входа в программу ViPNet Монитор пользователь должен обеспечить контакт устройства со считывателем и ввести ПИН-код.

     Внимание! Использовать способ аутентификации **Пароль на устройстве** для входа в ПО ViPNet Client крайне не рекомендуется.

   - **Устройство**. При выборе этого способа аутентификации необходимо подключить внешнее устройство для сохранения ключей защиты, принадлежащих пользователю, то есть парольного и персонального ключей (см. «Симметричные ключи в ПО ViPNet» на стр. 270).

     Для входа в программу ViPNet Монитор пользователь должен обеспечить контакт устройства со считывателем и ввести ПИН-код (и в некоторых случаях пароль пользователя).

     При выборе способа аутентификации **Устройство** ключ защиты сохраняется на внешнем устройстве. Если вы используете процедуры подписи и шифрования внутри сторонних приложений (например, в MS Office), то в этом случае настоятельно рекомендуется контейнер ключей 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! В случае если при использовании способов аутентификации **Пароль на устройстве** и **Устройство** внешнее устройство будет отключено, компьютер будет автоматически заблокирован. Для продолжения работы необходимо вновь подключить это внешнее устройство. При необходимости параметры автоматической блокировки компьютера и IP-трафика могут быть изменены (см. «Особенности блокировки компьютера при использовании внешнего устройства для аутентификации пользователя» на стр. 208).

4 Выбрав способ аутентификации, нажмите кнопку **OK**.

5 На вкладке **Ключи** в группе **Аутентификация** значения полей **Способ аутентификации** и **Тип носителя** изменятся в соответствии с выбранным режимом.

Просмотр журнала событий

В журнале событий регистрируются действия пользователей и администратора по изменению настроек программы ViPNet Монитор:

- Изменение правил фильтрации IP-пакетов.
- Вход пользователя в программу и его выход.
- Вход в режиме администратора.
- Смена режимов безопасности.
- Смена конфигурации и другие события.

Данная информация позволяет администратору контролировать соблюдение принятой политики безопасности.

Для просмотра журнала событий:

1 Выполните вход в программу в качестве администратора (см. «Работа в программе с правами администратора» на стр. 251).

2 В окне программы ViPNet Монитор на панели навигации выберите раздел **Администратор**.

3 В разделе **Администратор** нажмите кнопку **Журнал событий**.

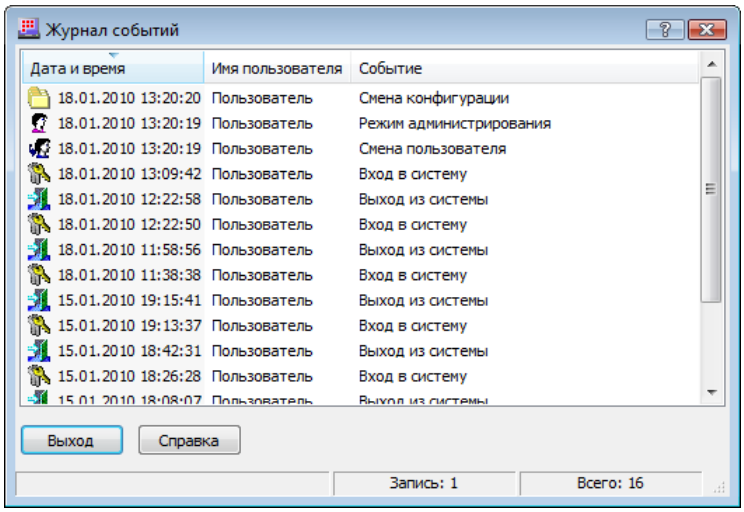


Рисунок 121: Просмотр журнала событий

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:

Таблица 5. Фиксируемые в журнале события

Столбец	Описание
Дата и время	Когда произошло событие.
Имя пользователя	Кто являлся инициатором события.
Событие	Расшифровка событий: • Вход в систему. • Выход из системы. • Режим администрирования — при входе в программу с паролем 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

Столбец	Описание
	неверного ввода пароля Администратора. •  Технологический перезапуск — перезагрузка программы после принятия файлов обновления или после нажатия на кнопку блокировки (при использовании кнопки в режиме блокировки **Блокировать IP-трафик** или **Блокировать компьютер и IP-трафик**) на нижней панели основного окна программы. •  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 правил фильтрации трафика. •  Смена режима безопасности. •  Включение или выключение функции «Блокировать все протоколы кроме IP, ARP, RARP» — установка или снятие флажка **Блокировать все протоколы, кроме IP, ARP, RARP** в окне **Сервис** > **Настройка**> **Общие**. •  Включение или выключение функции «Блокировать компьютер» — установка или снятие флажка **Блокировать компьютер** в окне **Настройка > Общие > Запуск и аварийное завершение**.

10

Справочники и ключи

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.

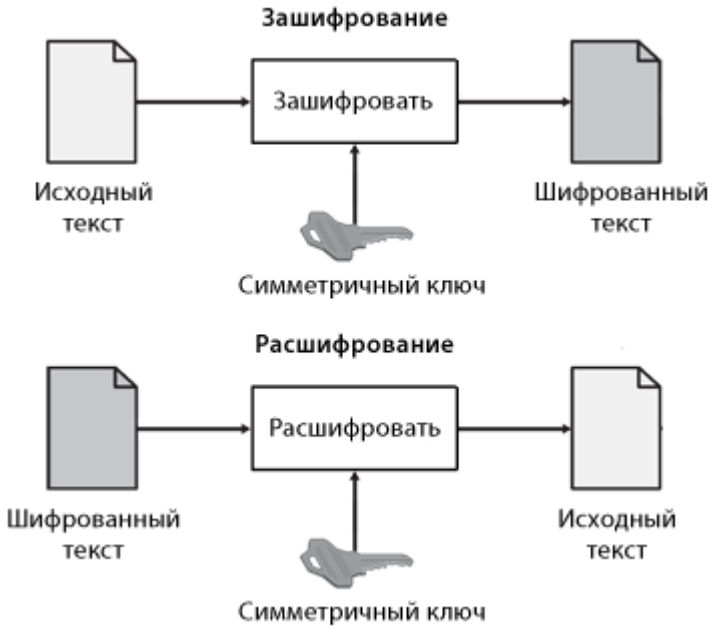


Рисунок 122: Зашифрование и расшифрование на симметричном ключе

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.

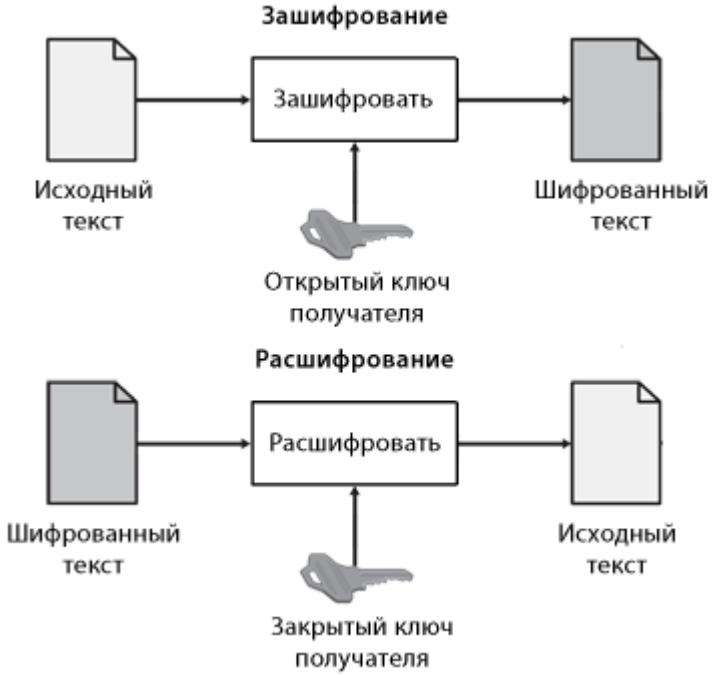


Рисунок 123: Зашифрование и расшифрование на асимметричном ключе

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. 266).

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.

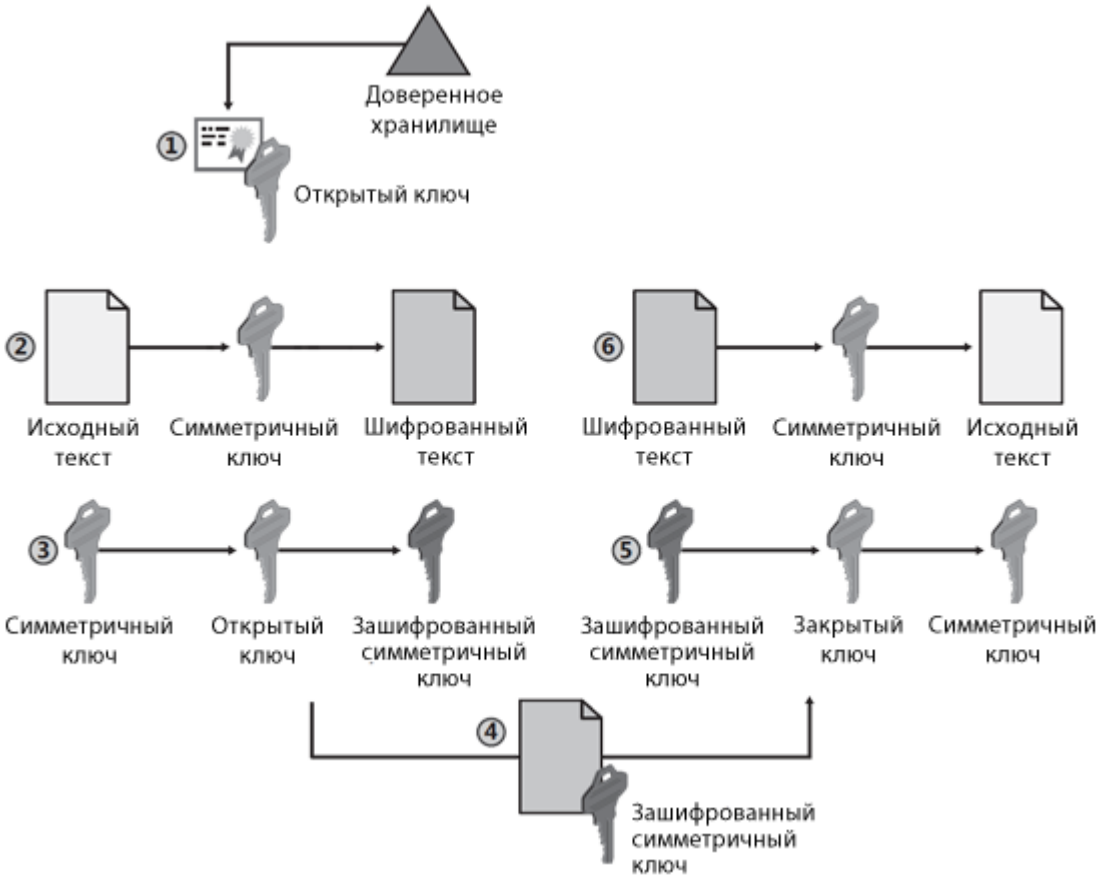


Рисунок 124: Шифрование с помощью комбинированного алгоритма

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.

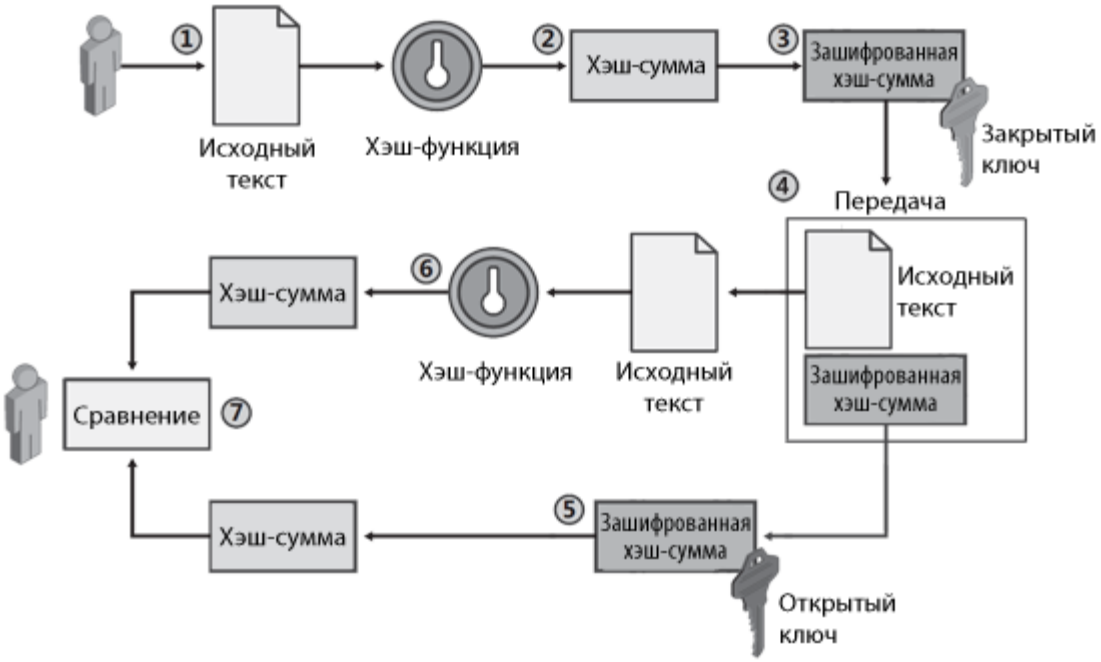


Рисунок 125: Применение хэш-функции и асимметричного алгоритма в электронной цифровой подписи

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.

Ключевая система ViPNet

В технологии ViPNet для шифрования применяется комбинация криптографических алгоритмов с симметричными и асимметричными ключами.

Таблица 6. Применение криптографических алгоритмов в ПО ViPNet

Криптографические алгоритмы	
С симметричными ключами	**С асимметричными ключами**
• шифрование IP-трафика • шифрование сообщений программы «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 Administrator или ViPNet 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 Administrator или ViPNet Manager. Симметричные ключи обмена следует передавать по защищенным каналам (для первоначальной инициализации ПО ViPNet дистрибутивы 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 126: Применение ключей обмена

Для защиты ключей обмена применяется три уровня шифрования:

- ключи обмена зашифрованы на ключах защиты коллективов;
- ключи защиты коллективов зашифрованы на персональных ключах;
- в свою очередь, персональные ключи зашифрованы на парольных ключах.

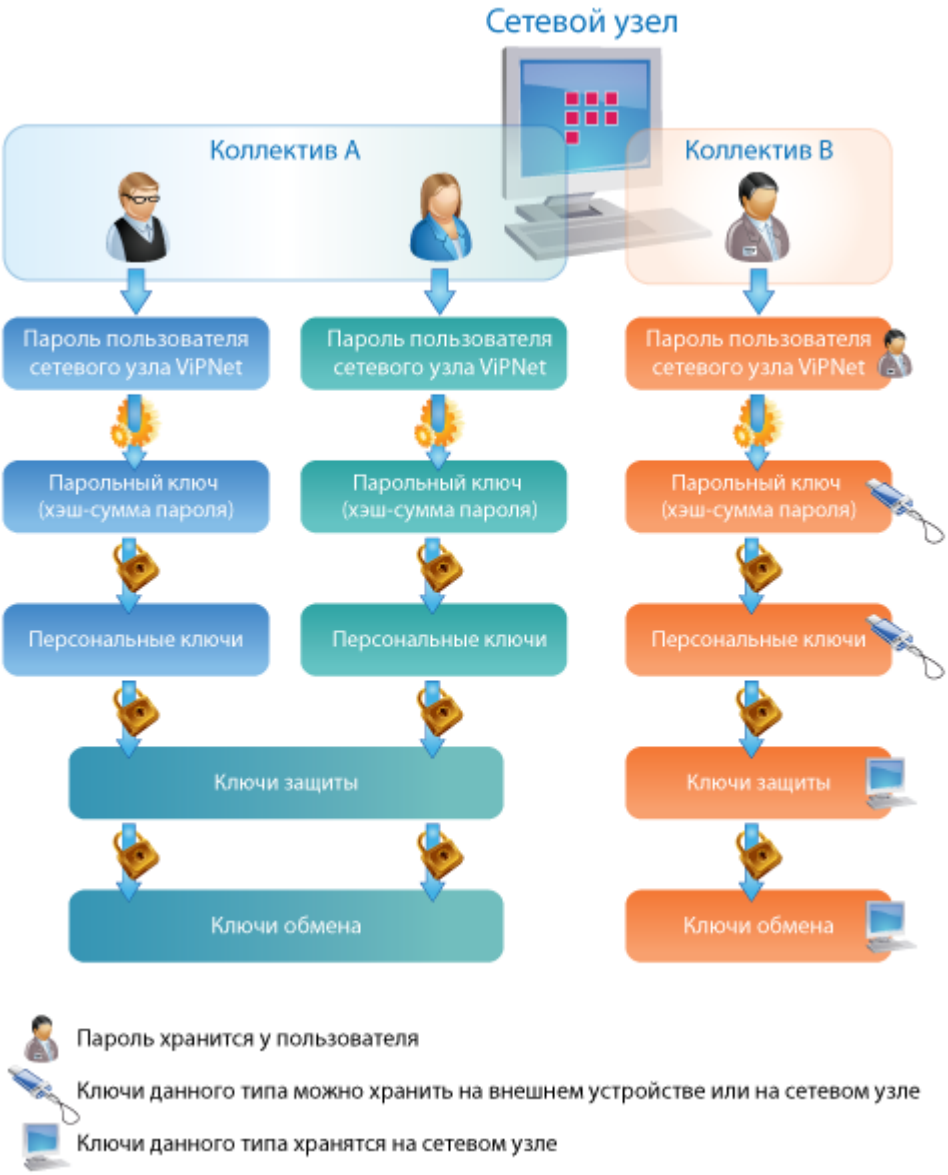


Рисунок 127: Иерархия защиты ключей обмена на сетевом узле

При создании структуры сети ViPNet администратор создает в программе ViPNet Administrator или ViPNet Manager файл дистрибутива ключей (*.dst) для каждого пользователя сетевого узла ViPNet. Файлы дистрибутивов необходимы для первичной инициализации ПО ViPNet 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 ключевой информации 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.

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. 268). Если на компьютере установлено ПО ViPNet, в состав которого входит криптопровайдер, асимметричные ключи можно использовать для шифрования (см. «Асимметричное шифрование» на стр. 265). 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 (например, администратором сети ViPNet), 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 следует хранить в тайне от других пользователей: рекомендуется использование съемных носителей или внешних устройств (см. «Информация о внешних устройствах хранения данных» на стр. 45). На жестком диске закрытый ключ хранится в зашифрованном виде в файле, который называется контейнером ключей. Схема защиты закрытого ключа электронной подписи изображена на следующем рисунке.

Рисунок 128: Схема защиты закрытого ключа подписи

Если закрытый ключ подписи хранится на внешнем устройстве, ключом защиты (см. «Ключ защиты») 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 «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 Manager адрес электронной почты указать невозможно.

Следует понимать, что технология асимметричного шифрования основана на стандартном использовании интерфейса Microsoft Crypto API. Следовательно, при использовании данной технологии пользователи ViPNet могут быть не связаны между собой в смысле топологии сети ViPNet (их сети могут не являться доверенными). Кроме того, получатель сообщения может вообще не являться пользователем программы ViPNet Client. Для расшифрования сообщения получателю достаточно закрытого ключа, сертификата и установленного на компьютере ПО, в состав которого входит криптопровайдер ViPNet.

Обновление справочников и ключей

Общие сведения о справочниках и ключах

Если администратор сети ViPNet вносит какие-либо изменения в структуру сети или настройки отдельных сетевых узлов, например, создает новые связи между сетевыми узлами, также изменяется справочники и ключи для сетевых узлов. Обновления справочников и ключей создаются администратором сети в программе ViPNet Administrator или ViPNet Manager и могут быть автоматически отправлены на сетевые узлы, которых коснулись изменения.

Обновление справочников и ключей на сетевом узле происходит в автоматическом режиме, если не открыт сеанс обмена защищенными сообщениями. Если в окне **Настройка** в подразделе **Предупреждения** установлен флажок **Выдавать предупреждения перед ViPNet-обновлениями**, при поступлении обновления программа выдает соответствующее сообщение. В противном случае обновление принимается автоматически.

Если по каким-либо причинам обновление справочников и ключей из ViPNet Administrator или ViPNet Manager не может быть принято по сети, существует возможность выполнить обновление вручную с помощью файла `*.dst` (см. «Обновление справочников и ключей с помощью файла *.dst» на стр. 276).

Обновление справочников и ключей с помощью файла *.dst

Обновление справочно-ключевой информации с помощью файла `*.dst` можно выполнить двумя способами:

1. Выполнить процедуру первичной инициализации (см. «Установка и удаление программы» на стр. 53), указав в мастере первичной инициализации путь к файлу `*.dst` с новой справочно-ключевой информацией.
2. Использовать мастер **Установка ключей сети ViPNet**, который запускается двойным щелчком по файлу `*.dst`.

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.

Чтобы обновить справочно-ключевую информацию с помощью мастера **Установка ключей сети ViPNet**, выполните следующие действия:

1. Перед обновлением выгрузите из памяти компьютера все запущенные модули ПО ViPNet, воспользовавшись командой **Выход** в главном меню или в области уведомлений.

2. Дважды щелкните файл дистрибутива ключей `*.dst` с новой справочно-ключевой информацией, полученный от администратора сети ViPNet. Будет запущен мастер **Установка ключей сети ViPNet**.

   Если при запуске мастера будут обнаружены работающие приложения ViPNet, будет выведено сообщение о необходимости завершить их работу. Выйдите из указанных приложений и нажмите кнопку **Повтор**.

3. 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 нажмите кнопку **Обзор**, чтобы указать дистрибутив ключей.

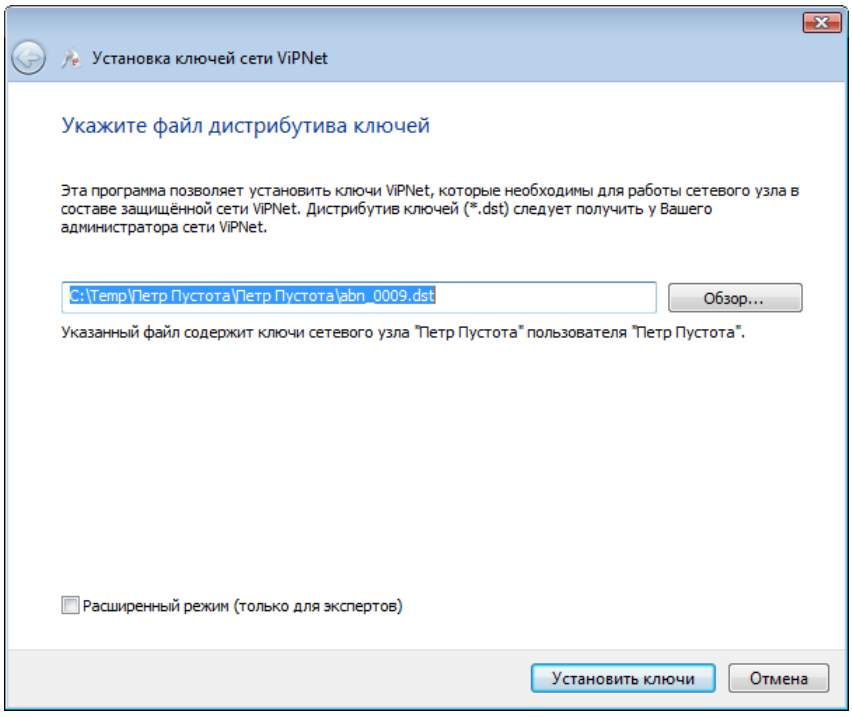


*Рисунок 129: Обновление справочно-ключевой информации с помощью файла *.dst*

4 Если выбран дистрибутив, который содержит новую версию справочников и ключей текущего узла, для установки ключей ViPNet в папки по умолчанию нажмите кнопку **Установить ключи**.

Примечание. Перед началом обновления ключей в папке установки программы ViPNet Монитор, в подпапке `\ccc\backup` создается резервная копия существующих ключей сетевого узла. При необходимости можно восстановить справочно-ключевую информацию из резервной копии (см. «Резервное копирование и восстановление ключей» на стр. 282).

5 Если пути к папке ключей узла или к папке ключей пользователя отличаются от путей по умолчанию, выполните следующие действия:

- Установите флажок **Расширенный режим (только для экспертов)**, затем нажмите кнопку **Далее**.

Внимание! Использование расширенного режима мастера установки ключей рекомендуется только для администратора сети ViPNet.

- С помощью кнопок **Обзор** укажите в соответствующих полях папку ключей сетевого узла и папку ключей пользователя.

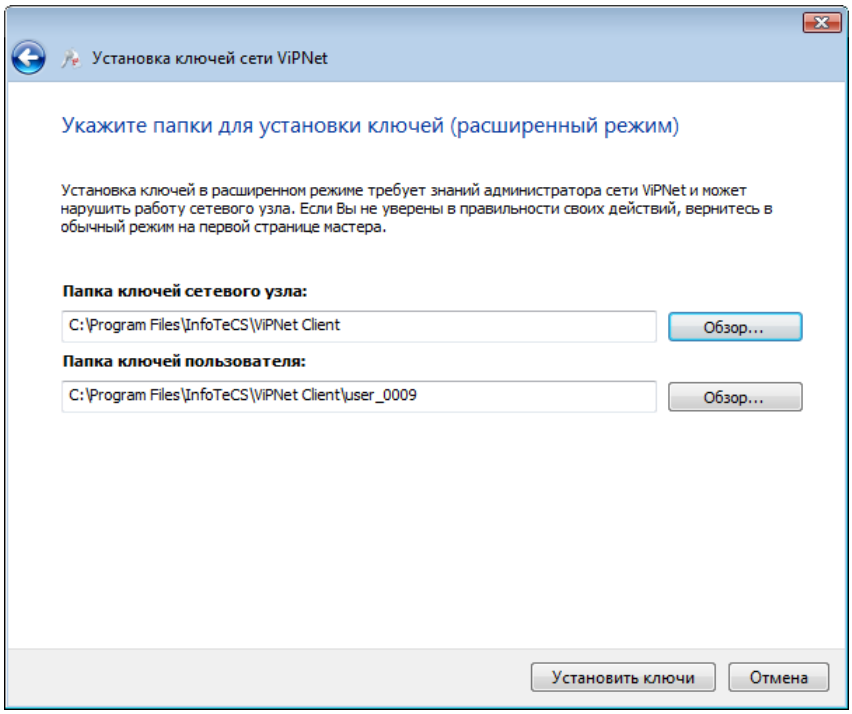


Рисунок 130: Указание папок для установки ключей узла и ключей пользователя

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

6 Если обнаружены какие-либо несоответствия между выбранным дистрибутивом ключей и текущими ключами на узле, кнопка **Установить ключи** будет недоступна. Для продолжения установки нажмите кнопку **Далее**:

- Если выбранный дистрибутив содержит более старую версию ключей и справочников, чем имеющаяся на узле, будет выведено соответствующее сообщение.

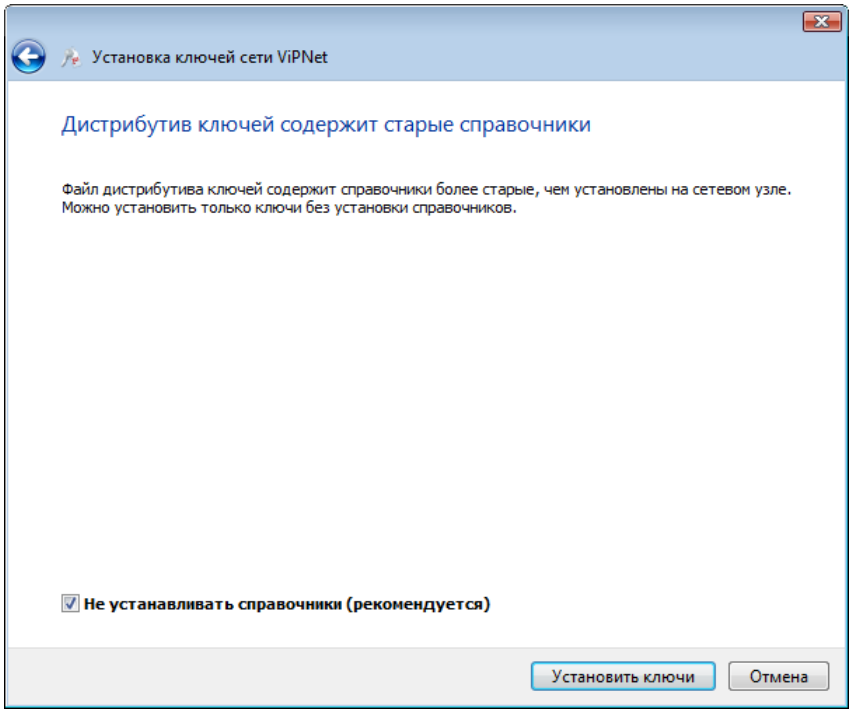


Рисунок 131: Дистрибутив содержит старые справочники

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

Если вы хотите продолжить установку, рекомендуется установить только ключи, но не устанавливать справочники. Для этого убедитесь, что установлен флажок **Не устанавливать справочники (рекомендуется)**, и нажмите кнопку **Установить ключи**.

- Если выбранный дистрибутив содержит ключи другого сетевого узла, был изменен мастер-ключ сетевого узла, формат дистрибутива отличается от формата текущих ключей или способ аутентификации, заданный в дистрибутиве, отличается от текущего, будет выведено предупреждение.

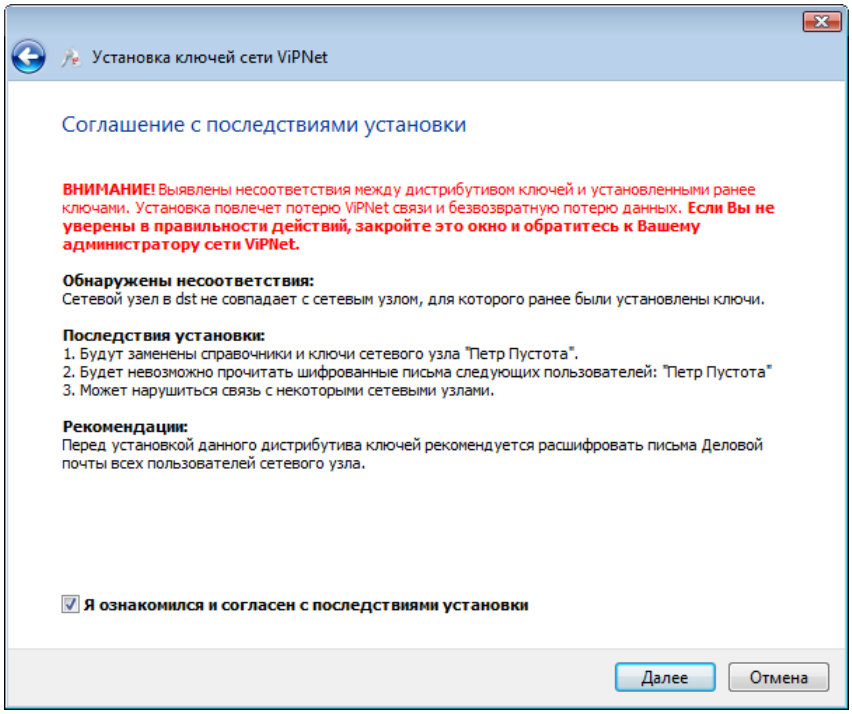


Рисунок 132: Обнаружено несоответствие между дистрибутивом и текущими ключами на узле

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. Перед продолжением установки рекомендуется завершить работу мастера, расшифровать письма программы «Деловая почта», затем повторно запустить мастер установки ключей.

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

7 Если обновление ключей прошло успешно, мастер установки выведет соответствующее сообщение. Для просмотра информации о выполненной установке ключей, щелкните ссылку **Подробнее о произведенных действиях**. Для завершения работы мастера нажмите кнопку **Закрыть**.

Если выполнить установку ключей не удалось, программа сообщит о возникших ошибках. Для устранения ошибок обратитесь к администратору сети ViPNet.

8 После успешной установки ключей можно запустить ПО ViPNet.

Резервное копирование и восстановление ключей

Резервная копия включает набор ключей пользователя и адресные справочники. Адресные справочники хранятся в транспортном каталоге (транспортный каталог можно выбрать во время первичной инициализации ключевой информации). Ключи пользователя хранятся в подпапке `\key_disk` или `\user_AAAA\key_disk` (где AAAA – шестнадцатеричный идентификатор пользователя сетевого узла).

Перед обновлением ключей сетевого узла с помощью мастера **Установка ключей сети ViPNet** (см. «Обновление справочников и ключей с помощью файла *.dst» на стр. 276) резервная копия существующей ключевой информации сохраняется в подпапку `\CCC\backup\[<год>,<число>,<время - ЧЧ.ММ.СС>]` папки установки ПО ViPNet.

При необходимости всегда можно восстановить ключевую информацию из резервной копии. Для этого:

1 Скопируйте файлы из папки резервной копии в транспортный каталог (по умолчанию транспортный каталог совпадает с папкой установки ПО ViPNet).

2 Если ключи пользователя хранятся на внешнем носителе, скопируйте папку `\key_disk` с содержимым ключевого диска на этот внешний носитель

3 На вопросы о замене файлов отвечайте утвердительно.

Компрометация 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 мог стать доступным съемный носитель 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 ключевой информации, хранящейся на компьютере
5. На компьютере, подключенном к сети, не установлена программа ViPNet Монитор или программа работала в 4 или 5 режиме безопасности, при этом:
   - в локальной сети возможно присутствие посторонних лиц или
   - на границе локальной сети отсутствует (отключен) межсетевой экран.
6. Увольнение сотрудников, имевших доступ к ключевой информации
7. Входящий документ подписан сертификатом, находящимся в списке отозванных сертификатов.
8. Случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (например, ключевой носитель вышел из строя, и существует возможность того, что это произошло в результате несанкционированных действий злоумышленника).

К событиям, требующим проведения расследования и принятия решения на предмет происшествия компрометации, относится возникновение подозрений, что произошла утечка 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 РНПК (AAAA.pk, где AAAA — идентификатор пользователя в сети ViPNet) входит в состав первоначального дистрибутива ключей.

Если текущий персональный ключ пользователя оказался скомпрометирован, администратор УКЦ высылает пользователю новые ключи, защищенные с помощью очередного варианта персонального ключа, который не нужно передавать по сети, так как он уже содержится в РНПК. Если при обновлении файл РНПК 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 УКЦ за новым файлом РНПК.

11

Работа с сертификатами

Общие сведения о сертификатах открытых ключей

Определение и назначение

Сертификат открытого ключа является одним из объектов криптографии с открытым ключом — системы шифрования, в которой для прямого и обратного преобразований используются разные ключи:

- Закрытый ключ — для формирования электронной подписи (см. «Электронная подпись») 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 при отправке 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 специальные 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. 289).

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 — самоподписанный сертификат администратора УЦ, изданный для администратора другого УЦ. В зависимости от модели доверительных отношений, установленной между УЦ (см. «Роль PKI для криптографии с открытым ключом» на стр. 292), может использоваться либо как сертификат издателя (в иерархической модели), либо для проверки сертификатов пользователей другой сети (в распределенной модели).

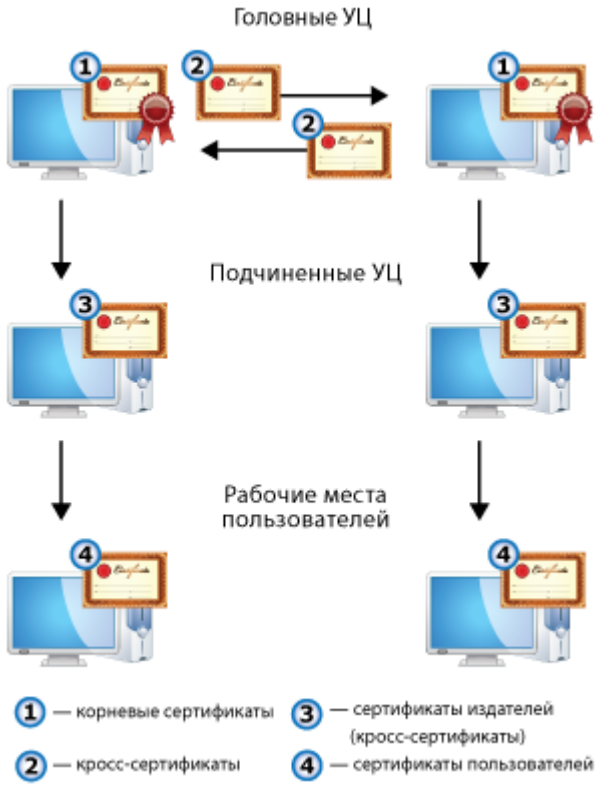


Рисунок 133: Типы сертификатов

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. 292) 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 — информация защищена от несанкционированной модификации как при хранении, так и при передаче.
- Неотрекаемость — отправитель не может 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,

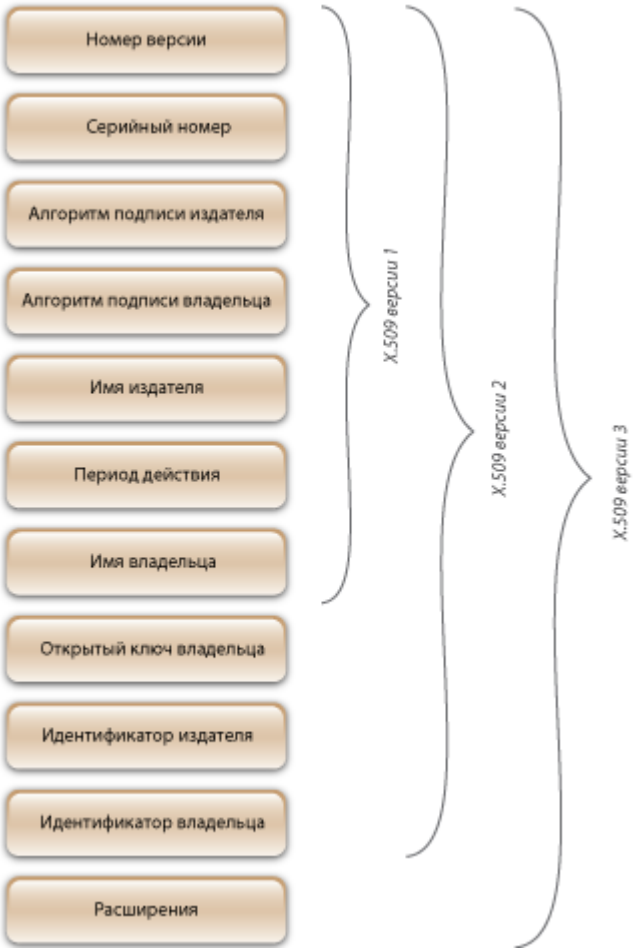


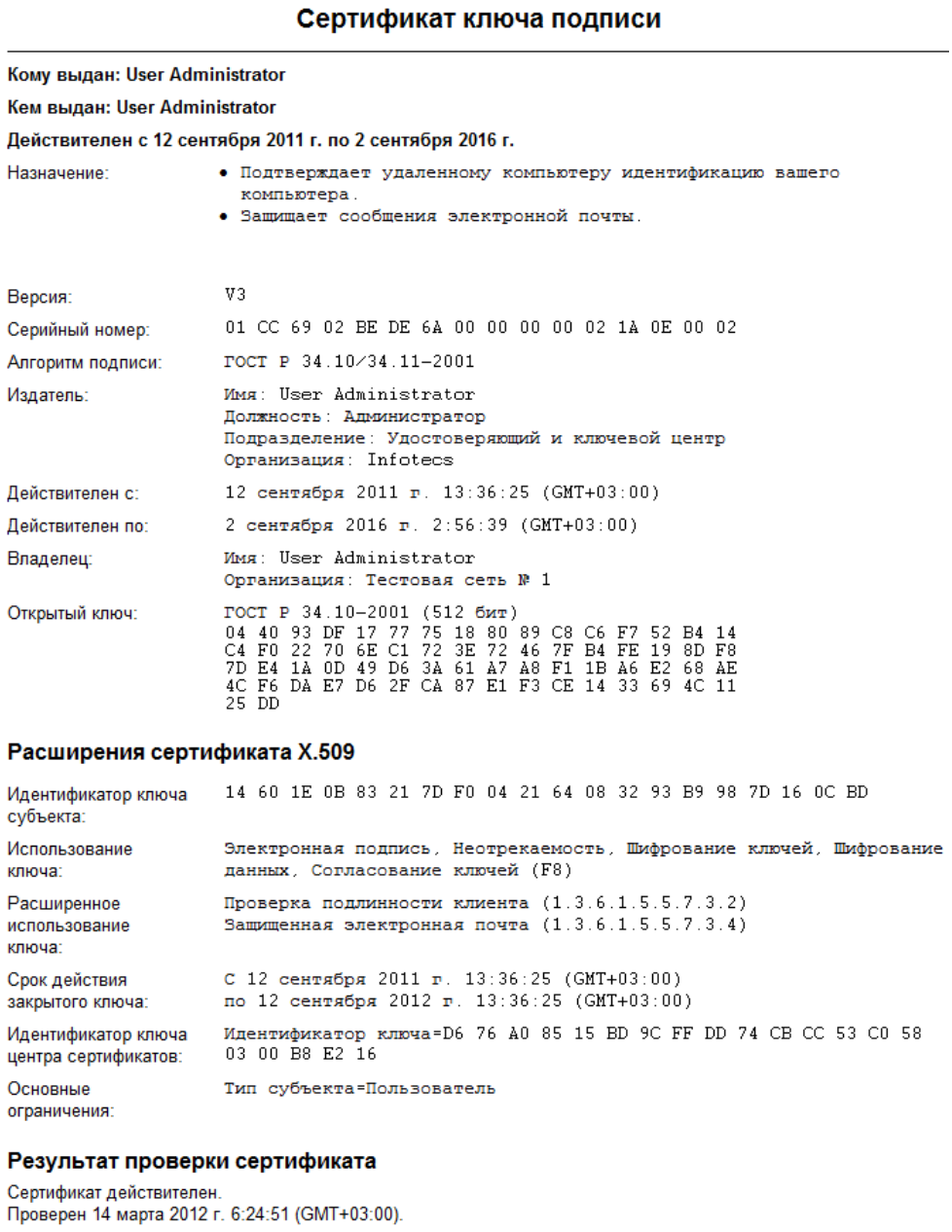
Рисунок 134: Структура сертификата, соответствующего стандарту X.509 версий 1, 2 и 3

- 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.



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 135: 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 (УЦ). УЦ предназначен для регистрации пользователей, выпуска сертификатов, их хранения, выпуска СОС и поддержания его в актуальном состоянии. В сетях ViPNet УЦ 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 УЦ. Доверительные отношения между этими УЦ могут выстраиваться по распределенной или иерархической модели.

- В иерархической модели доверительных отношений УЦ объединяются в древовидную структуру, в основании которой находится главный (корневой) УЦ, который выдает кросс-сертификаты подчиненным ему центрам, там самым обеспечивая доверие к открытым ключам этих центров. Каждый УЦ вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчиненным ему центрам. В результате доверие сертификату открытого ключа каждого УЦ основано на заверении его ключом вышестоящего центра. Сертификат главного УЦ (корневой сертификат) является самоподписанным. В остальных УЦ администраторы не имеют собственных корневых сертификатов и для установления доверительных отношений формируют запросы на кросс-сертификат к своим вышестоящим УЦ.

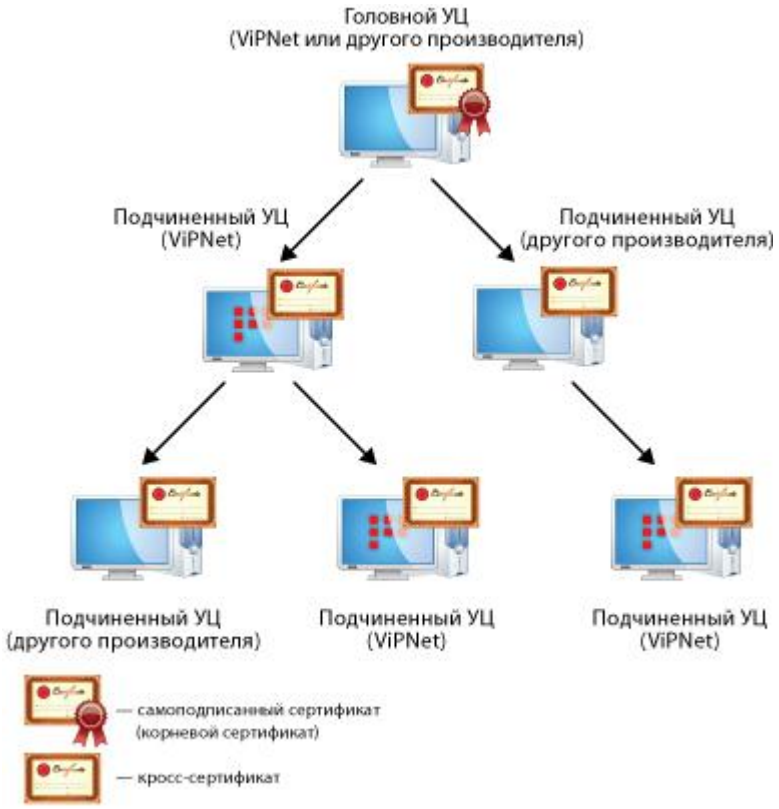


Рисунок 136: Иерархическая модель доверительных отношений

- В распределенной модели доверительных отношений все УЦ равнозначны: в каждом УЦ администратор имеет свой корневой (самоподписанный) сертификат. Доверительные отношения между УЦ в этой модели устанавливаются путем двусторонней кросс-сертификации, когда два УЦ издают кросс-сертификаты друг для друга. Взаимная кросс-сертификация проводится попарно между всеми УЦ. В результате в каждом УЦ в дополнение к корневому сертификату имеются кросс-сертификаты, изданные для администраторов других УЦ.

  Для подписания сертификатов пользователей каждый УЦ продолжает пользоваться своим корневым сертификатом, а изданный кросс-сертификат другого УЦ использует для проверки сертификатов пользователей другой сети. Это возможно в силу того, что кросс-сертификат создается на базе существующего корневого сертификата доверенного УЦ и содержит сведения о том же открытом ключе. Поэтому нет необходимости переиздавать сертификаты пользователей своей сети.

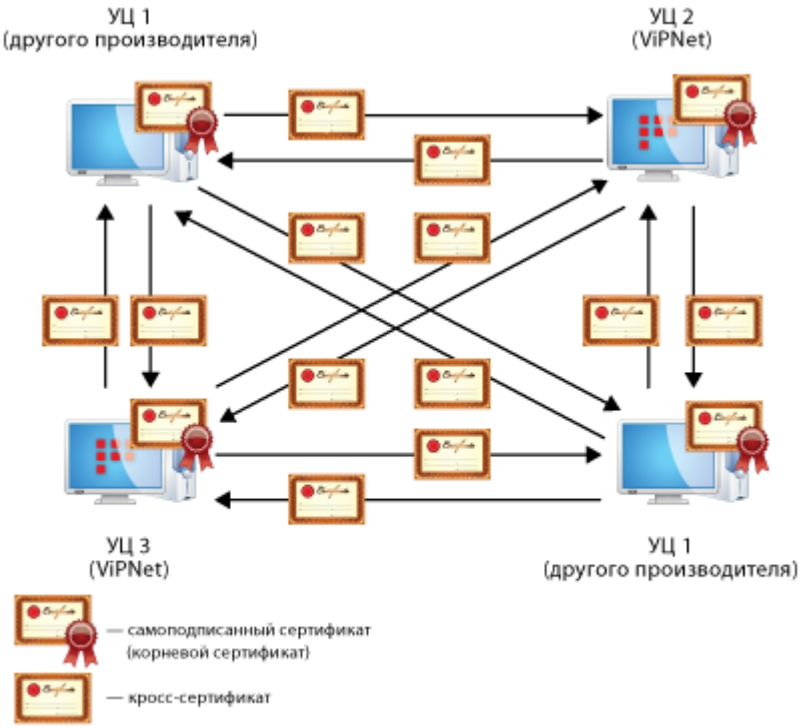


Рисунок 137: Распределенная модель доверительных отношений

Зная иерархию и подчиненность УЦ 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, 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 с использованием открытого ключа получателя.

6 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

7 Документ отправляется.

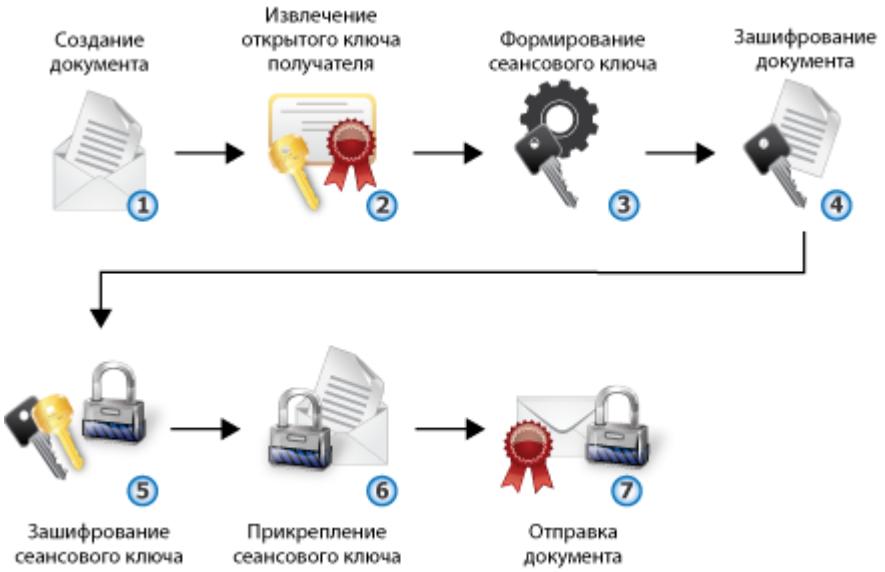


Рисунок 138: Процесс зашифрования электронных документов

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 139: 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») 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 140: 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 141: 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, 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 с использованием открытого ключа получателя.

10 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

11 Документ отправляется.

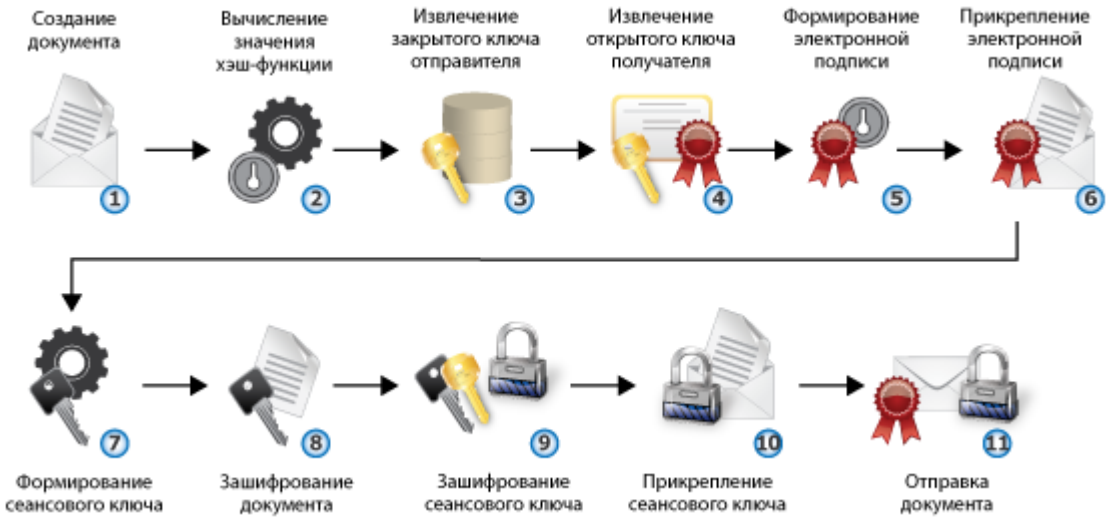


Рисунок 142: Процесс подписания и зашифрования электронных документов

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.

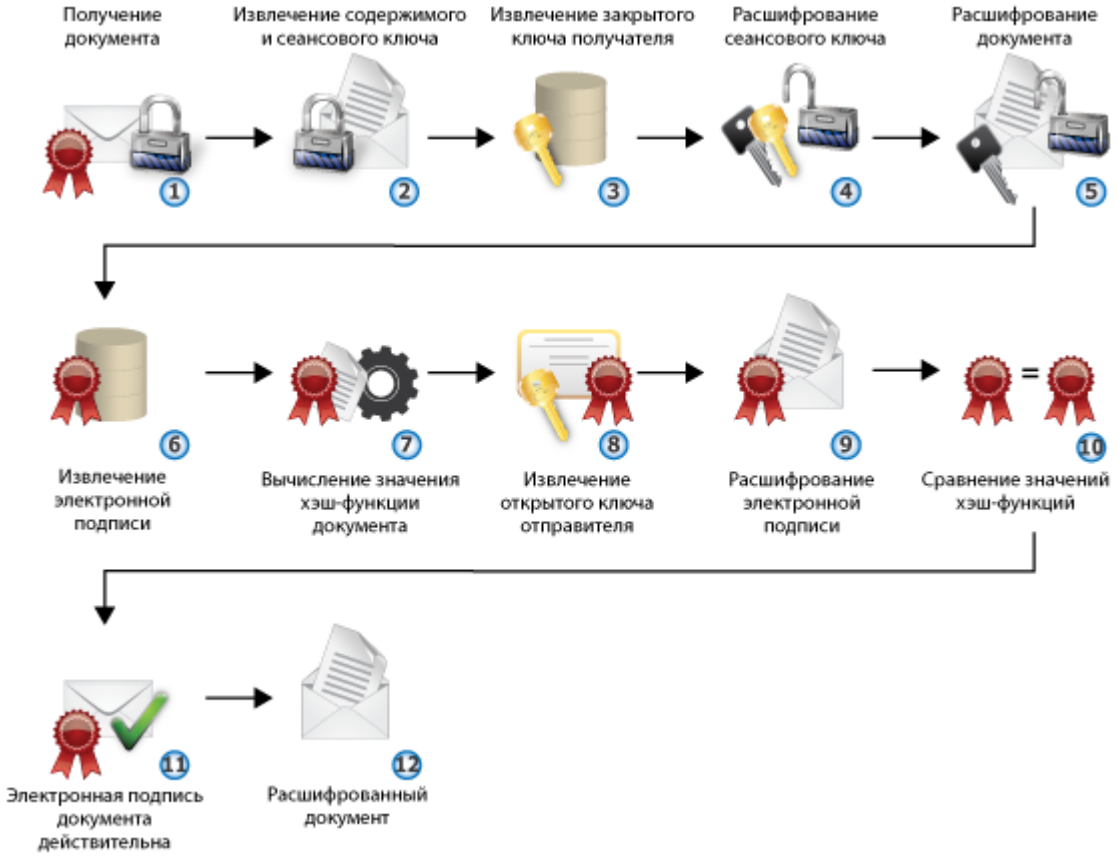


Рисунок 143: Процесс расшифрования и проверки электронного документа

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 т. д.

В программе ViPNet Client можно просматривать следующие типы сертификатов:

- текущий сертификат пользователя (см. «Просмотр текущего сертификата пользователя» на стр. 302),
- личные сертификаты пользователя (см. «Просмотр личных сертификатов пользователя» на стр. 302),
- доверенные корневые сертификаты (см. «Просмотр доверенных корневых сертификатов» на стр. 303),
- изданные сертификаты (см. «Просмотр изданных сертификатов» на стр. 303).

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;
- 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 Administrator УКЦ.

В сертификате пользователя сети ViPNet OFFICE кнопка **Заявление издателя**

всегда недоступна.

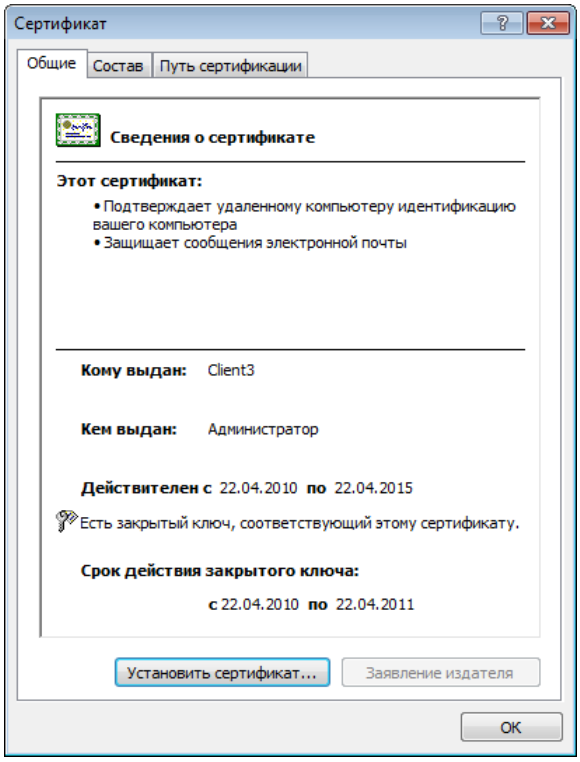


Рисунок 144: Просмотр основной информации о сертификате

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 о 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. 256).

---

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 или ViPNet Manager по запросам пользователей или по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, 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. «Определение и назначение» на стр. 286) 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 Client 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. 307) Установка в хранилище вручную(на стр. 309)
Установка сертификата в контейнер. Если требуется использовать сертификат, который хранится отдельно от закрытого ключа, этот сертификат необходимо сопоставить закрытому ключу. Для этого следует установить сертификат в контейнер, в котором хранится соответствующий закрытый ключ.	Установка сертификата в контейнер(на стр. 312)
Смена текущего сертификата. Можно выбрать другой сертификат (из числа действительных личных сертификатов пользователя) в качестве текущего.	Смена текущего сертификата(на стр. 313)
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. 315) Процедура обновления закрытого ключа и сертификата(на стр. 316)
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 сертификатов в действие(на стр. 324) Ввод в действие автоматически(на стр. 324) Ввод в действие вручную(на стр. 325)

Функциональная возможность	Ссылка
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. 326) Просмотр запроса на сертификат(на стр. 326) Удаление запроса на сертификат(на стр. 327)
Экспорт сертификата. В зависимости от целей использования сертификата за пределами ПО ViPNet, сертификат может быть экспортирован в файлы различных форматов.	Экспорт сертификата(на стр. 328)

Установка сертификатов в хранилище

Установка сертификатов в хранилище позволяет использовать сертификаты во внешних приложениях (таких как Windows Live Mail, MS Outlook, MS Word и др.). Можно установить сертификат в хранилище операционной системы или хранилище программы ViPNet Client (в папку `D_STATION` транспортного каталога).

Установку можно выполнить автоматически или вручную.

Внимание! При установке сертификата в хранилище ОС Windows Vista или Windows Server 2008 следует запускать программу ViPNet Client 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.

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.

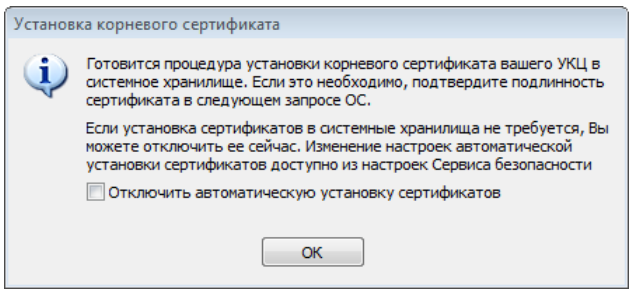


Рисунок 145: Установка корневого сертификата

2 Если автоматическая установка сертификатов не была прервана, в окне запроса на добавление сертификата в хранилище проверьте подлинность сертификата, после чего нажмите кнопку **Да**.

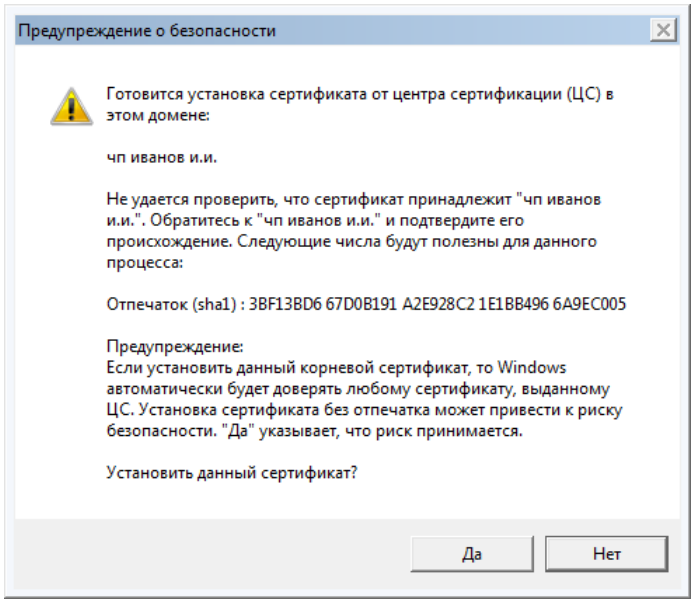


Рисунок 146: Подтверждение подлинности корневого сертификата

Корневой сертификат установлен в хранилище сертификатов текущего пользователя.

Установка в хранилище вручную

Для работы с защищенными документами и соединениями 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, кроме сертификата пользователя, необходимо 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. 301).

2. Нажмите кнопку **Установить сертификат**.

3. На странице приветствия мастера установки сертификатов нажмите кнопку **Далее**.

4. На странице **Выбор хранилища сертификатов** укажите, в какое хранилище будет установлен ваш сертификат, и нажмите кнопку **Далее**.

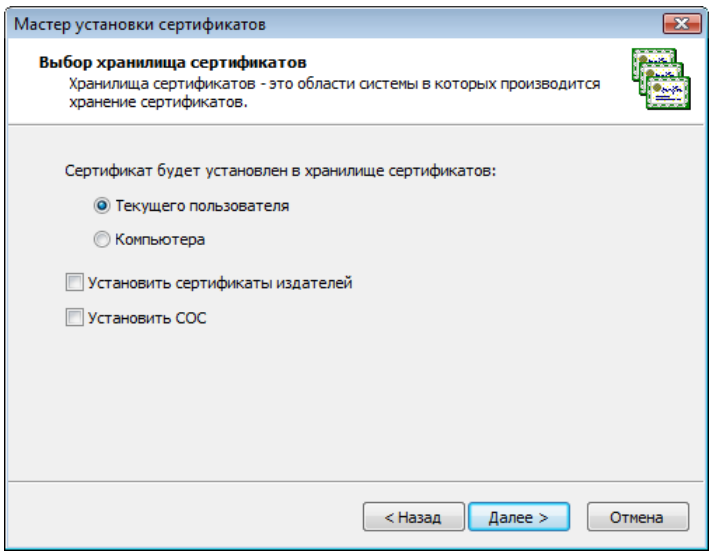


Рисунок 147: Выбор хранилища сертификатов

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.

Для продукта ViPNet CSP сертификат следует устанавливать в хранилище компьютера при использовании ViPNet CSP 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.

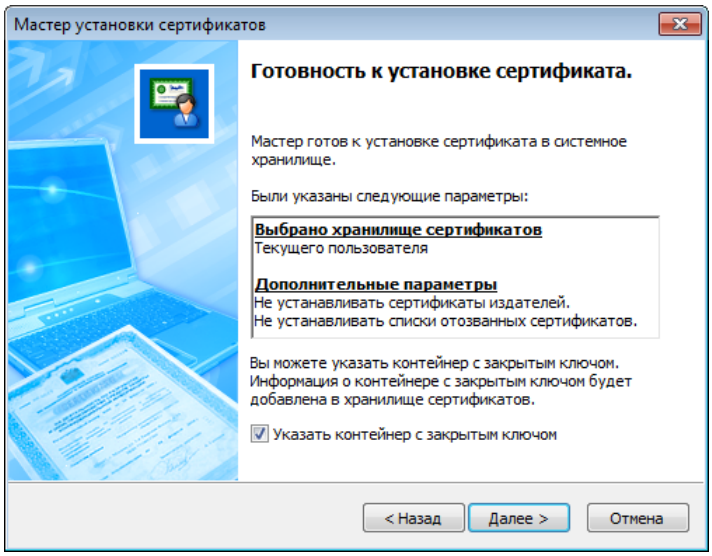


Рисунок 148: Страница Готовность к установке сертификата

- Если сертификат хранится в файле отдельно от закрытого ключа, установите флажок **Указать контейнер с закрытым ключом**.

Примечание. Флажок **Указать контейнер с закрытым ключом** 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 с закрытым ключом** установлен и контейнер не найден либо недоступен, в появившемся окне **ViPNet CSP – инициализация контейнера ключа** укажите расположение контейнера ключей:

- папку на диске;
- устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

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 с закрытым ключом** установлен и контейнер доступен, в появившемся окне **ViPNet CSP – пароль контейнера ключа** в поле **Пароль** введите пароль доступа к контейнеру, после чего нажмите кнопку **OK**.

Примечание. Окно **ViPNet CSP – пароль контейнера ключа** 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. 339).

Установка сертификата в контейнер

Установка сертификата в контейнер ключей требуется в том случае, если для подписи и шифрования необходимо использовать сертификат, который хранится отдельно от контейнера и не сопоставлен соответствующему закрытому ключу.

Для того чтобы установить сертификат в контейнер ключей:

1 Вызовите окно **Свойства контейнера ключей** (см. Рисунок 162 на стр. 335) для контейнера, в котором хранится закрытый ключ, соответствующий сертификату.

2 В окне **Свойства контейнера ключей** нажмите кнопку **Добавить**.

Примечание. Кнопка **Добавить** активна в том случае, если в контейнере хранится хотя бы один закрытый ключ, не сопоставленный сертификату (в таблице **Закрытые ключи** столбец **Сертификат** для строки с информацией о закрытом ключе является пустым).

3 В появившемся окне **Открыть** выберите формат файла сертификата (`*.cer` или `*.p7b`), после чего выберите сертификат, соответствующий закрытому ключу.

Если указанный сертификат не соответствует закрытому ключу, появится окно с сообщением «Ключ не найден».

Если указанный сертификат соответствует закрытому ключу, в таблице **Закрытые ключи** в столбце **Сертификат** для строки с информацией о закрытом ключе появится значок  . После этого сертификат может быть использован криптопровайдером ViPNet CSP для подписи и шифрования.

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. 256).

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 сертификатов в действие» на стр. 324), а затем назначить текущим.

При успешном выполнении описанных действий выбранный сертификат назначается текущим. При этом на вкладке **Ключи** (см. Рисунок 161 на стр. 333) 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 закрытый ключ также обновляется.

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, содержащий дополнительные атрибуты. Например, для использования сертификата в системах документооборота могут быть добавлены назначения сертификата, могут быть изменены данные о владельце сертификата (должность, подразделение и другие), добавлены расширения либо политики применения сертификата.

Таким образом, требуется обновлять сертификат открытого ключа и закрытый ключ не реже, чем 1 раз в год.

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.

Настройка оповещения об истечении срока действия закрытого ключа и сертификата

По умолчанию программа ViPNet Client 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.

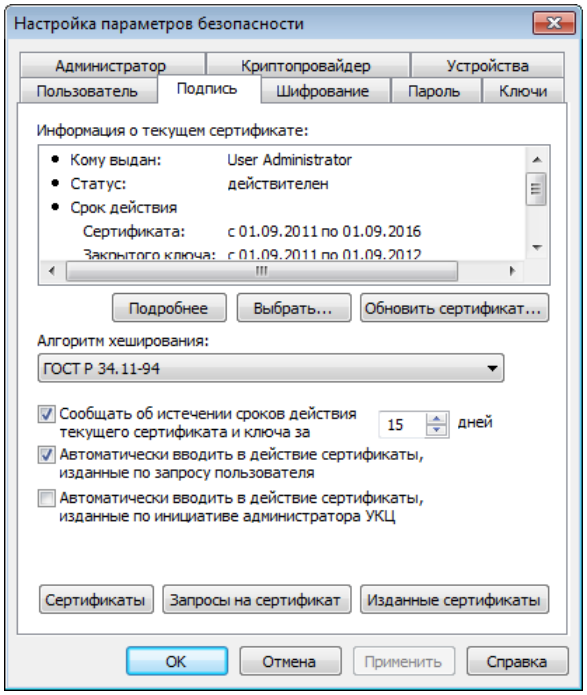


Рисунок 149: Просмотр информации о текущем сертификате и настройка параметров оповещения об истечении сроков действия закрытого ключа и сертификата

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 Client выдаст соответствующее сообщение.

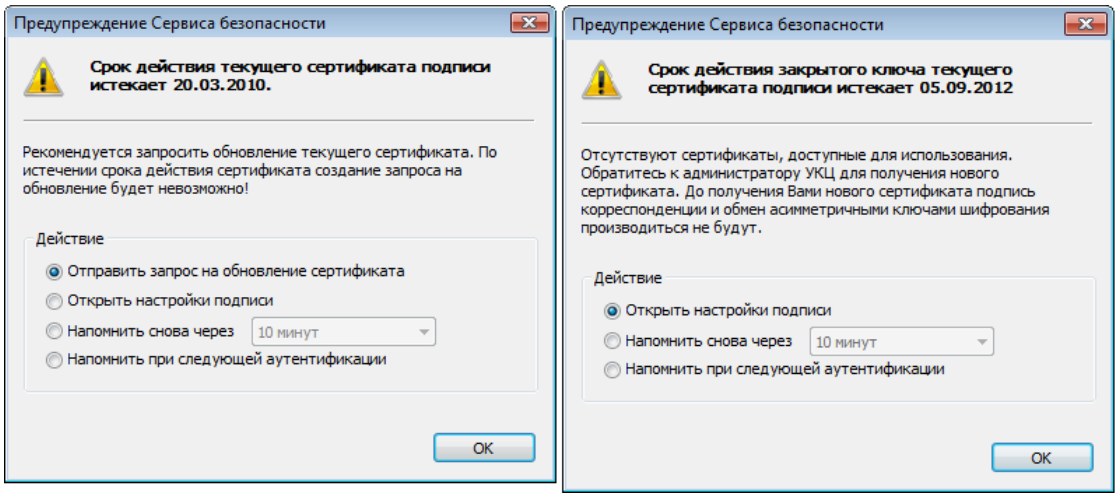


Рисунок 150: Предупреждения о скором истечении срока действия сертификата и закрытого ключа

- 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 149 на стр. 316) 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 стартовой странице мастера обновления сертификата нажмите кнопку **Далее**.

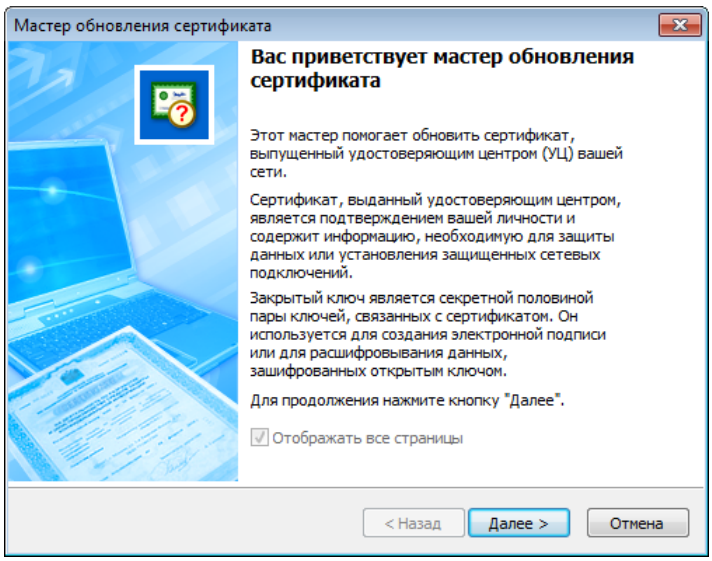


Рисунок 151: Стартовая страница мастера обновления сертификата

2 На странице **Открытый ключ**:

- Укажите параметры открытого ключа в соответствии с приведенной ниже таблицей:

Таблица 7. Характеристики алгоритма ГОСТ Р 34.10-2001

Алгоритм подписи	Описание	Параметры алгоритма	Описание параметров	Длина ключа
ГОСТ Р 34.10-2001	Новый стандарт электронной подписи, основанный на арифметике эллиптических кривых. OID «1.2.643.2.2.19»	ГОСТ Р 34.10-2001	Параметры по умолчанию (рекомендуется). OID «1.2.643.2.2. 35.1»	512
		ГОСТ Р 34.10-2001	Параметры подписи 3 (в соответствии с RFC 4357 http://www.ietf.org/rfc/rfc4357.txt). OID «1.2.643.2.2. 35.3»	

Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью

вычисления и проверки подписи.

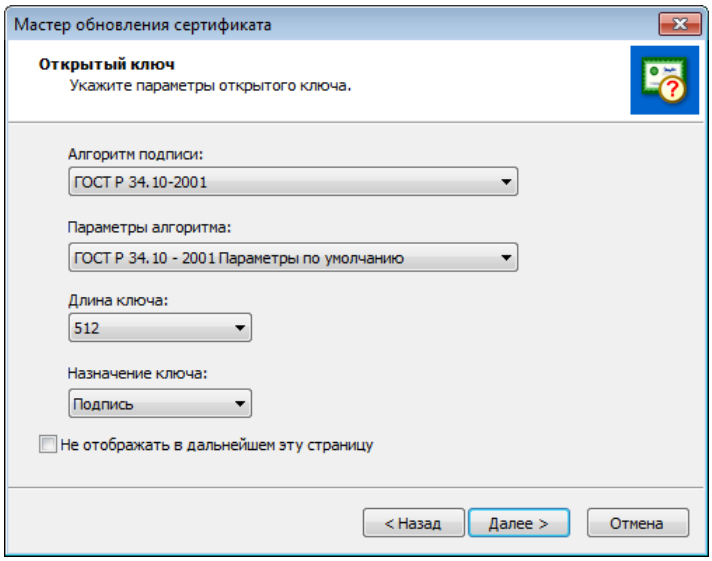


Рисунок 152: Выбор параметров открытого ключа

- В списке **Назначение ключа** выберите нужное значение:
  - если сертификат предполагается использовать в рамках ПО ViPNet — значение **Подпись**;
  - если сертификат предполагается использовать как в рамках ПО ViPNet, так и во внешних программах (например, в MS Outlook), — значение **Подпись и шифрование**.
- 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 и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

После этого нажмите кнопку **Далее**.

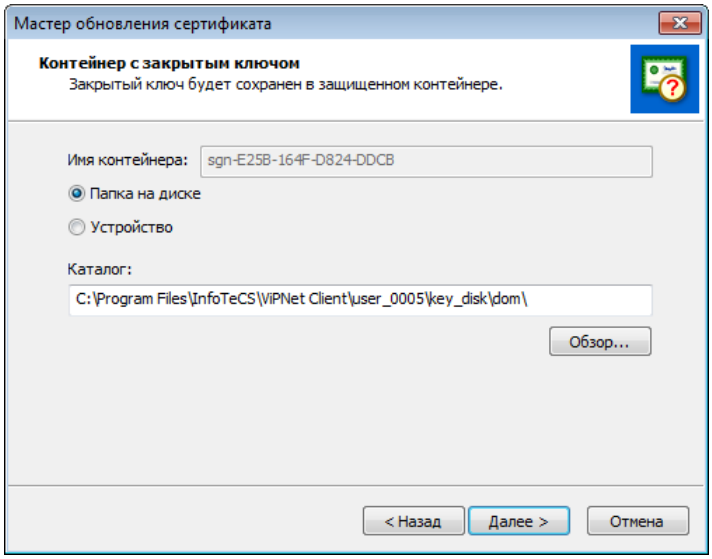


Рисунок 153: Указание места хранения контейнера ключей

4 На странице **Срок действия сертификата** задайте желаемый срок действия обновляемого сертификата удобным для вас способом, после чего нажмите кнопку **Далее**.

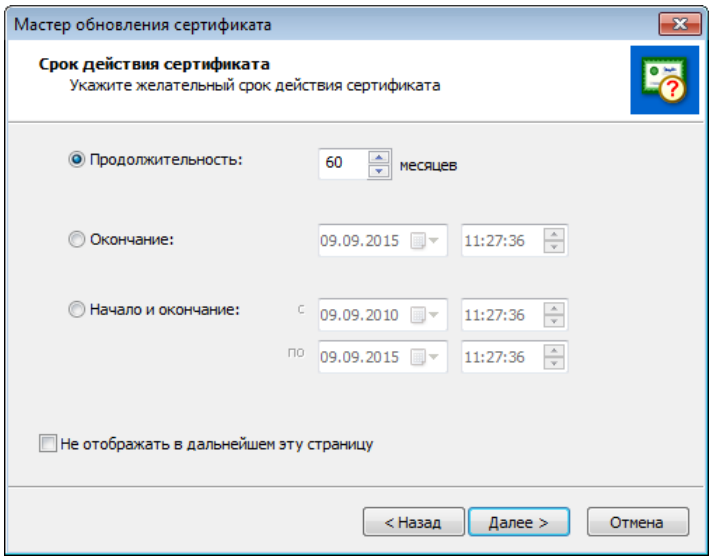


Рисунок 154: Указание желаемого срока действия сертификата

5 На странице **Способ передачи сертификата** выберите, каким образом запрос на обновление сертификата будет передан в программу ViPNet Удостоверяющий и ключевой центр или ViPNet Manager:

- **Передать через транспортный модуль** — отправка запроса через транспортный модуль ViPNet MFTP.

- **Передать через файл** — сохранение запроса в файл формата *.sok по пути, указанному с помощью кнопки **Обзор**. По завершении работы мастера обновления этот файл необходимо передать администратору вашей сети ViPNet.

После этого нажмите кнопку **Далее**.

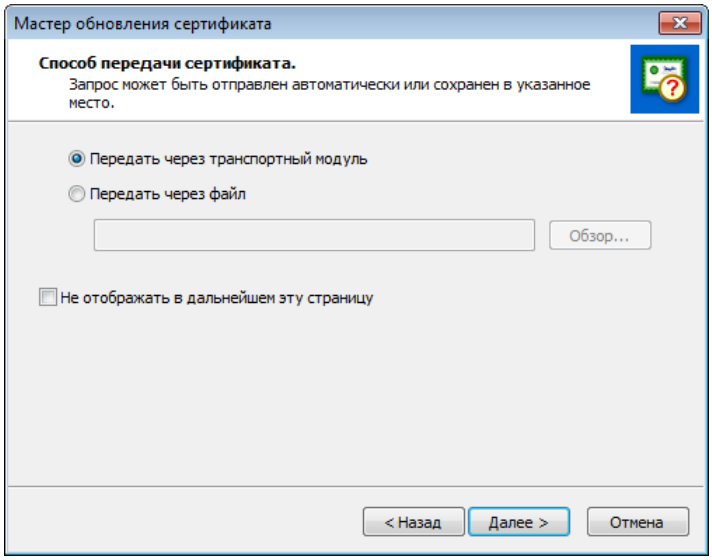


Рисунок 155: Выбор способа передачи сертификата в программу ViPNet Удостоверяющий и ключевой центр или ViPNet Manager

6 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**.

7 При появлении электронной рулетки (см. Рисунок 113 на стр. 240) следуйте указаниям окна.

Примечание. В случае если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

8 На странице **Завершение работы мастера обновления сертификата**:

- В случае если ранее на странице **Способ передачи сертификата** выбран способ **Передать через файл**, нажмите кнопку **Готово**. Работа мастера обновления сертификата завершена. Созданный файл необходимо передать администратору вашей сети ViPNet.
- В случае если ранее на странице **Способ передачи сертификата** выбран способ **Передать через транспортный модуль**, задайте значения следующих параметров:
  - **Ожидать ответа на запрос** — для входа в режим ожидания ответа от программы ViPNet Удостоверяющий и ключевой центр или ViPNet Manager.

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 мин. Если обработка запросов в программе ViPNet Удостоверяющий и ключевой центр осуществляется вручную, время ожидания ответа не ограничено. Подробнее см. документ «ViPNet Administrator Удостоверяющий и ключевой центр. Руководство администратора».

  - **Ввести изданный сертификат в действие** — для ввода изданного сертификата в действие и назначения его текущим сразу после получения.

Примечание. Флажок **Ввести изданный сертификат в действие** можно не устанавливать, если в окне **Настройка параметров безопасности** на вкладке **Подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**.

Нажмите кнопку **Готово.**

9 Если при выборе передачи сертификата через транспортный модуль был установлен флажок **Ожидать ответа на запрос**, при появлении сообщения «Ожидание ответа удостоверяющего центра» дождитесь отображения ответа от программы ViPNet Удостоверяющий и ключевой центр или ViPNet Manager:

- **Запрос на сертификат удовлетворен** — обновленный сертификат получен.
- **Запрос на сертификат отклонен** — сертификат не был обновлен. Обратитесь к администратору вашей сети ViPNet для уточнения причин отклонения запроса.

Примечание. Запрос, переданный программе ViPNet Manager, обрабатывается автоматически и не может быть отклонен.

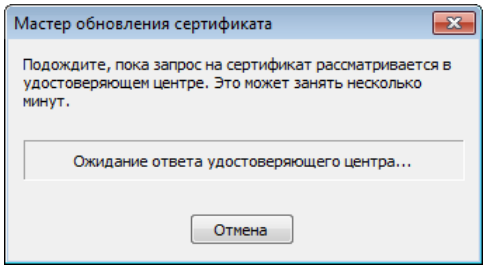


Рисунок 156: Ожидание ответа от программы ViPNet Удостоверяющий и ключевой центр или ViPNet Manager

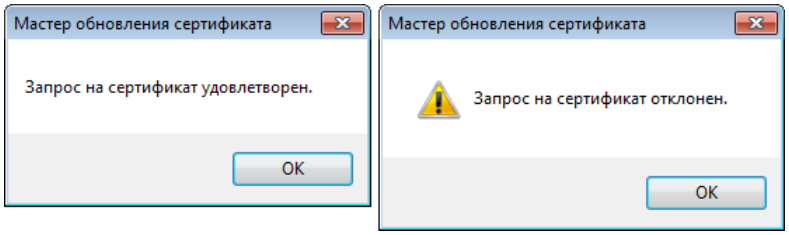


Рисунок 157: Возможные ответы от программы ViPNet Удостоверяющий и ключевой центр

10 Убедитесь в том, что изданный сертификат введен в действие.

- Вызовите окно **Настройка параметров безопасности**, после чего откройте вкладку **Подпись**.
- Нажмите кнопку **Запросы на сертификат**.

- Убедитесь в том, что для отправленного запроса отображается статус **сертификат введен в действие**.

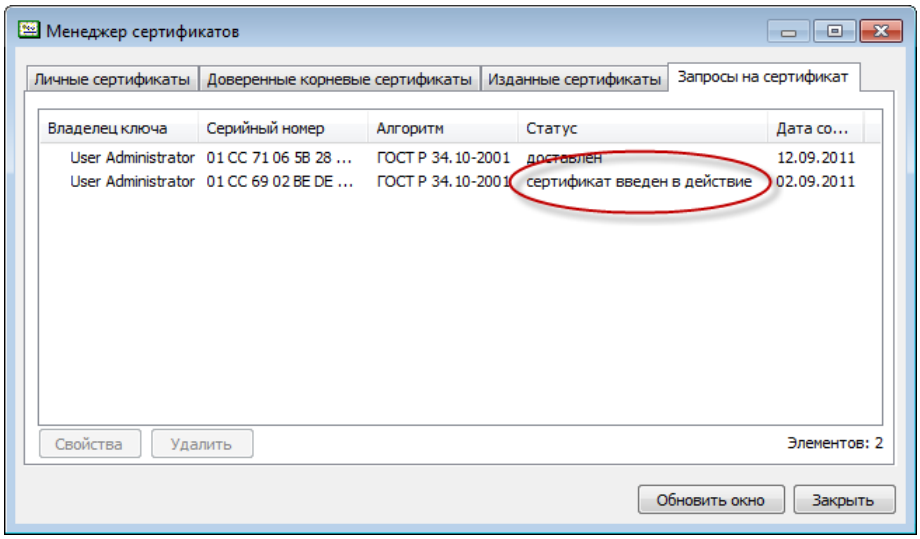


Рисунок 158: Статус запроса в случае ввода сертификата в действие

Если сертификат издан, но не введен в действие автоматически (статус запроса **удовлетворен**), выполните ввод сертификата в действие вручную (см. «Ввод в действие вручную» на стр. 325).

Ввод сертификатов в действие

Для того чтобы использовать сертификат, полученный из ViPNet Удостоверяющий и ключевой центр или ViPNet Manager в результате обновления либо переданный на используемый сетевой узел в виде файла, 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 или ViPNet Manager, выполнялся автоматически, убедитесь в том, что установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**, а также флажок **Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ**, после чего нажмите кнопку **Применить** или **ОК**.

Сертификаты будут введены в действие автоматически в течение часа с момента их получения.

Примечание. Если введен в действие сертификат, изданный 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. 356).

Ввод в действие вручную

Способ ввода сертификата в действие вручную зависит от того, каким образом сертификат был передан на используемый сетевой узел:

- Если сертификат был передан на сетевой узел в составе обновления (издан по запросу пользователя или по инициативе администратора) и при этом не была произведена настройка, позволяющая выполнить ввод этого сертификата в действие автоматически:
  - В окне **Настройка параметров безопасности** откройте вкладку **Подпись,** после чего нажмите кнопку **Изданные сертификаты**.
  - В окне **Менеджер сертификатов** на вкладке **Изданные сертификаты** выберите полученный сертификат, который необходимо ввести в действие, после чего нажмите кнопку **Ввести в действие**.
- Если сертификат был издан в программе ViPNet Удостоверяющий и ключевой центр и передан на сетевой узел в виде файла:
  - В окне **Настройка параметров безопасности** откройте вкладку **Подпись**, после чего нажмите кнопку **Изданные сертификаты**.
  - В окне **Менеджер сертификатов** нажмите кнопку **Импорт**.
  - В окне **Открыть** (**Open**) выберите файл формата *.sok, полученный от администратора вашей сети ViPNet.

    Выбранный файл будет помещен в каталог установки программы ViPNet Client, в папку `\ccc\From_KC`. При этом информация об изданном сертификате отобразится на вкладке **Изданные сертификаты**.
  - Выберите сертификат, который необходимо ввести в действие, после чего нажмите кнопку **Ввести в действие**.

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. 313).

Работа с запросами на сертификаты

Работа с запросами на сертификаты (см. «Запрос на сертификат») 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 выполните двойной щелчок мыши 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.**

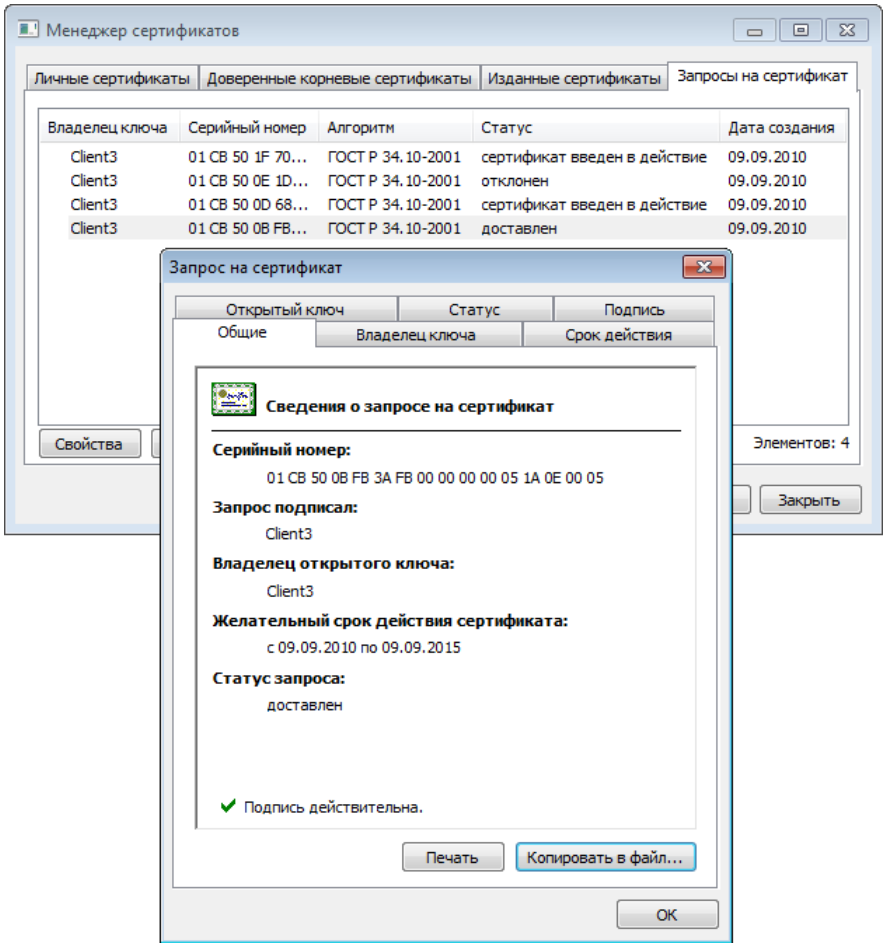


Рисунок 159: Просмотр подробной информации о запросе на сертификат

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 установления процесса обмена защищенными сообщениями;
- вывод сертификата на печать.

Для экспорта сертификата в файл определенного формата:

1. Вызовите окно **Сертификат** для того сертификата, который необходимо экспортировать (см. «Просмотр сертификатов» на стр. 301).
2. Откройте вкладку **Состав**, после чего нажмите кнопку **Копировать в файл**.
3. На стартовой странице мастера экспорта сертификатов нажмите кнопку **Далее**.

Совет. Если при последующих запусках мастера желательно пропускать те или иные страницы, на этих страницах следует устанавливать флажок **Не отображать в дальнейшем эту страницу**.

4. На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. «Форматы экспорта сертификатов» на стр. 329), после чего нажмите кнопку **Далее**.

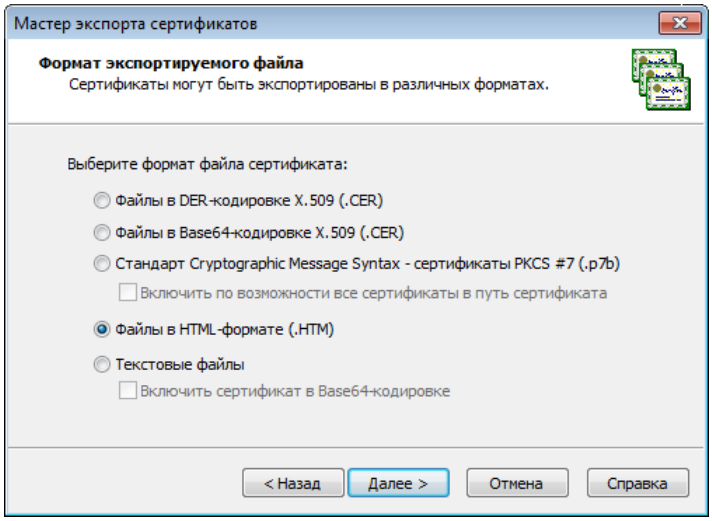


Рисунок 160: Выбор формата файла

5 На странице **Имя файла экспорта** 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 «Экспорт успешно выполнен» 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, или 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 находится подробная информация о каждом из форматов экспорта сертификатов, поддерживаемыми 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) спецификации (RFC 1341 and successors) 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 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 и сертификат (см. «Сертификат открытого ключа подписи пользователя»), соответствующий закрытому ключу.

В программе ViPNet Client доступны следующие операции с контейнером ключей:

- Установка (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 339).

  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. 307), так и отдельно (см. «Установка нового контейнера ключей и смена контейнера ключей с текущим сертификатом» на стр. 339) (например, в случае, если закрытый ключ хранится в контейнере, а сертификат сформирован по запросу пользователя в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Manager).
  - 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. 334).

  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 и (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. 338).

  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. 340).

  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. 258).

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»):

1 Откройте вкладку **Ключи**.

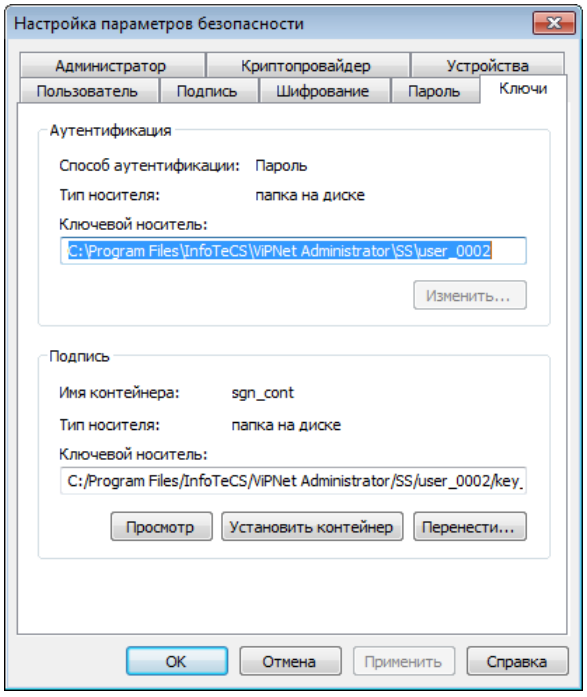


Рисунок 161: Работа с контейнером ключей

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. 334);
  - удаления пароля (см. «Удаление сохраненного на компьютере пароля к контейнеру ключей» на стр. 336);
  - проверки соответствия закрытого ключа сертификату (см. «Проверка контейнера ключей» на стр. 337);
  - удаления закрытого ключа (см. «Удаление закрытого ключа» на стр. 338).
- **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. 339).
- **Перенести** — для изменения расположения контейнера ключей (см. «Перенос контейнера ключей» на стр. 340).

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. 339) 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 161 на стр. 333) нажмите кнопку **Просмотр**.
2. В окне **Свойства контейнера ключей** нажмите кнопку **Сменить пароль**.

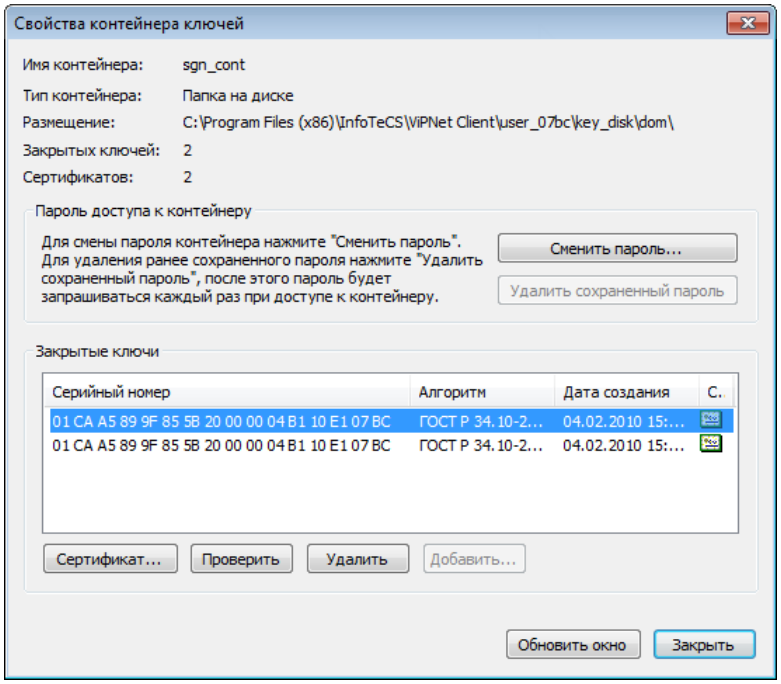


Рисунок 162: Информация о контейнере ключей

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. 238).

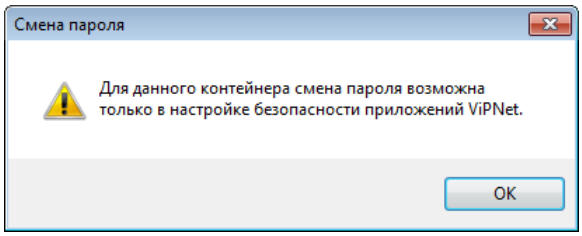


Рисунок 163: Сообщение о невозможности смены пароля для доступа к контейнеру

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 персональный ключ пользователя создан в программе ViPNet Registration Point либо был перенесен (см. «Перенос контейнера ключей» на стр. 340) из папки

ключей пользователя (по умолчанию `C:\Program Files (x86)\InfoTeCS\ViPNet Client\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 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 новый пароль в полях **Введите пароль** и **Подтверждение**. Нажмите кнопку **OK**.

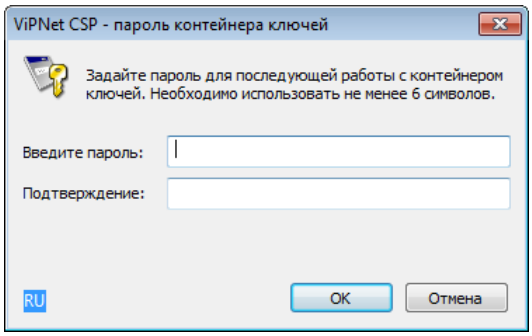


Рисунок 164: Смена пароля доступа к контейнеру ключей

Пароль доступа к контейнеру 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 и (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 161 на стр. 333) нажмите кнопку **Просмотр.**

2 В окне **Свойства контейнера ключей** (см. Рисунок 162 на стр. 335) 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, выполните следующие действия:

1. В окне **Свойства контейнера ключей** (см. Рисунок 162 на стр. 335) в списке **Закрытые ключи** выберите строку закрытого ключа.
2. Нажмите кнопку **Проверить**.
3. В окне **ViPNet CSP - пароль контейнера ключей** введите пароль доступа к контейнеру и нажмите кнопку **OK**.

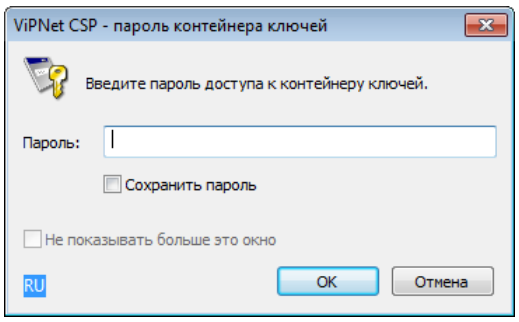


Рисунок 165: Ввод пароля доступа к контейнеру ключей

После этого 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 совместимость с сертификатом, хранящимся 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.

При успешной проверке закрытого ключа отобразится сообщение «Сертификат успешно проверен».

Удаление закрытого ключа

Удаление закрытого ключа (и сертификата, при его наличии) 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.

Чтобы удалить закрытый ключ и сертификат из контейнера:

1. В окне **Свойства контейнера ключей** (см. Рисунок 162 на стр. 335) в списке **Закрытые ключи** выберите строку закрытого ключа или несколько строк, удерживая клавишу **Shift**.
2. Нажмите кнопку **Удалить**. Появится предупреждение о том, что удаленные закрытые ключи невозможно восстановить.
3. В окне предупреждения нажмите кнопку **Да.**

Выбранный закрытый ключ и соответствующий ему сертификат будут удалены из контейнера. 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 Client (см. «Установка сертификатов в хранилище» на стр. 307) 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.

Для установки нового или смены текущего контейнера ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 161 на стр. 333) 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.

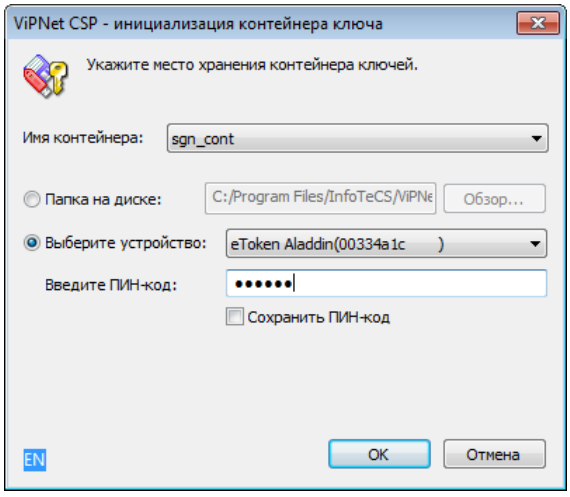


Рисунок 166: Инициализация контейнера ключей с внешнего устройства

Внимание! В случае если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.x, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый

формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

Нажмите кнопку **ОК**.

3 В случае если целостность контейнера нарушена (отсутствует закрытый ключ), в окне с сообщением об ошибке 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 требуется в следующих случаях:

- для изменения расположения контейнера, например, если 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. 258).

Примечание. Не поддерживается перенос контейнера ключей на устройства eToken ГОСТ, ruToken, Shipka, Kaztoken (см. «Информация о внешних устройствах хранения данных» на стр. 45).

Для того чтобы поменять расположение контейнера ключей:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** (см. Рисунок 161 на стр. 333) 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 и установить драйверы этого устройства. Перечень доступных устройств хранения данных и полезная информация об использовании устройств содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

Внимание! В случае если на выбранном устройстве хранятся ключи, сформированные в ПО ViPNet версии ниже 3.1.x, появится окно программы **Конвертер ключей ViPNet** с предложением конвертировать ключи в новый формат. Подробная информация о работе с программой **Конвертер ключей ViPNet** содержится в разделе Информация о внешних устройствах хранения данных(на стр. 45).

Контейнер ключей будет перенесен по указанному пути.

Возможные неполадки и способы их устранения

Возможные неполадки

Нет ключевой дискеты или неверный пароль

В этом случае программа выдает следующее сообщение:

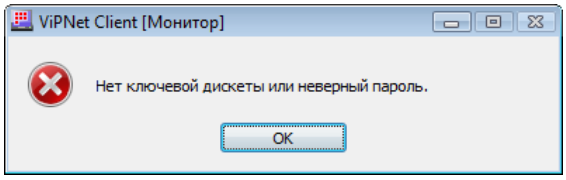


Рисунок 167: Сообщение о неверном пароле

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, путь к ключевой дискете указан неверно.

  В этом случае в окне ввода пароля щелкните значок справа от кнопки **Настройка**, в меню выберите пункт **Каталог 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.

Невозможно подключиться к ресурсам в Интернете

Возможно, установлен первый или второй режим безопасности. Для безопасной работы в Интернете установите третий режим (см. «Изменение режима безопасности» на стр. 129). Для работы во втором режиме безопасности необходимо настроить правила фильтрации трафика, разрешающие соединение с требуемыми адресами.

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 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 фильтры по умолчанию в разделе **Открытая сеть** включены и настроены, как описано в разделе Фильтры, настроенные по умолчанию (см. «Фильтры открытой сети, настроенные по умолчанию» на стр. 134).
- Установлен первый или второй режим безопасности и не заданы разрешающие сетевые фильтры. Установите третий режим безопасности (см. «Изменение режима безопасности» на стр. 129).

Невозможно запустить службу MSSQLSERVER

Возможно, причиной неполадки является сбой одного из компонентов программы ViPNet Client. 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 установить соединение по протоколу SSL

Возможно, причиной неполадки является сбой одного из компонентов программы ViPNet Client. Для решения данной проблемы выполните действия, описанные в разделе Невозможно запустить службу MSSQLSERVER(на стр. 344).

Невозможно установить соединение по протоколу PPPoE

В операционных системах Windows Vista и Windows 7 соединение по протоколу PPPoE может блокироваться программой ViPNet Монитор.

Для решения данной проблемы выполните следующие действия:

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

2 В окне **Настройка** откройте раздел **Общие**.

3 Снимите флажок **Блокировать все протоколы, кроме IP, ARP, RARP**.

4 Нажмите кнопку **OK**.

Невозможно запустить программу

Вероятно, программа ViPNet Монитор была деинсталлирована или удалена с компьютера вручную. Убедитесь в том, что программа ViPNet Монитор установлена и в случае необходимости переустановите ее либо обратитесь за помощью к администратору сети ViPNet.

Невозможно изменить настройки в программе ViPNet Монитор

На сетевом узле ограничены полномочия пользователя. Изменить настройки программы ViPNet Монитор может только администратор сетевого узла (см. «Работа в программе с правами администратора» на стр. 251). Обратитесь к нему за помощью либо попросите повысить уровень полномочий.

Невозможно сохранить пароль

Возможность сохранения пароля может предоставить администратор сетевого узла. Для этого необходимо войти в программу ViPNet Монитор в режиме администратора (см. «Работа в программе с правами администратора» на стр. 251).

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, создайте папку `C:\ProgramData\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:
   - `bio` — электронная рулетка (используется в программном обеспечении ViPNet по умолчанию).
   - `accord` — Аккорд-АМДЗ.
   - `sobol` — электронный замок «Соболь».
   - `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. Нажмите сочетание клавиш **Win+R**.
2. В поле **Открыть** введите `regedit` и нажмите кнопку **OK**. Откроется окно **Редактор реестра**.
3. В ключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Infotecs\PatchEngine` присвойте параметру `Flags` значение 0.

Внимание! Не изменяйте никакие параметры системного реестра, кроме `Flags`. Неправильное изменение параметров реестра может привести к неисправности компьютера.

4. Перезагрузите компьютер.

   Если после выполнения указанных действий проблема не будет решена, обратитесь в службу технической поддержки компании «ИнфоТеКС».

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 112 на стр. 239) 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. 238).

Примечание. В программе ViPNet Manager невозможно изменить пароль пользователя функционирующего сетевого узла.

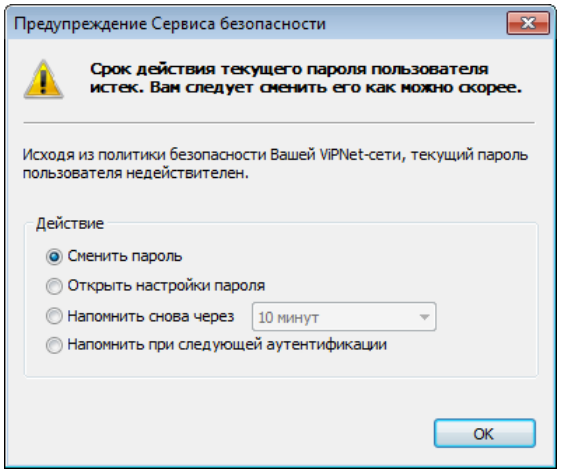


Рисунок 168: Предупреждение об истечении срока действия пароля пользователя

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 112 на стр. 239);
   - **Открыть настройки пароля** — для вызова окна **Настройка параметров безопасности** на вкладке **Пароль** (см. Рисунок 112 на стр. 239), 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 Client.
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.

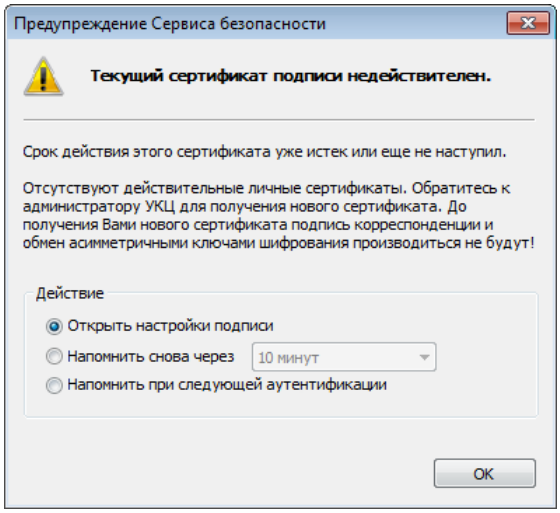


Рисунок 169: Предупреждение о том, что текущий сертификат недействителен

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 Client.

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. 316). 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 или ViPNet Manager.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

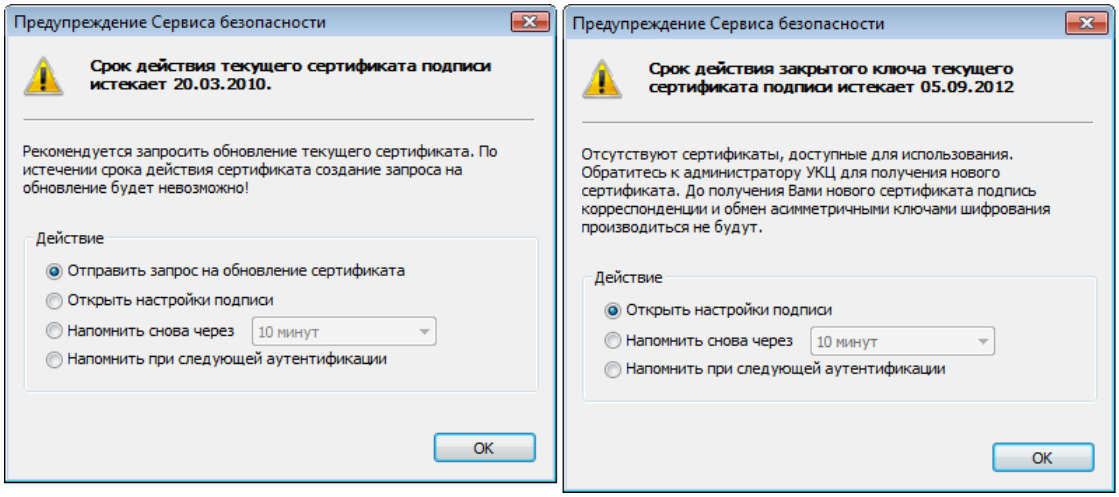


Рисунок 170: Предупреждения о скором истечении срока действия сертификата и закрытого ключа

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. 316).
   - **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 Client.
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. 316). 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. 326).

- 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 или ViPNet Manager.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте еще один запрос на обновление текущего сертификата.

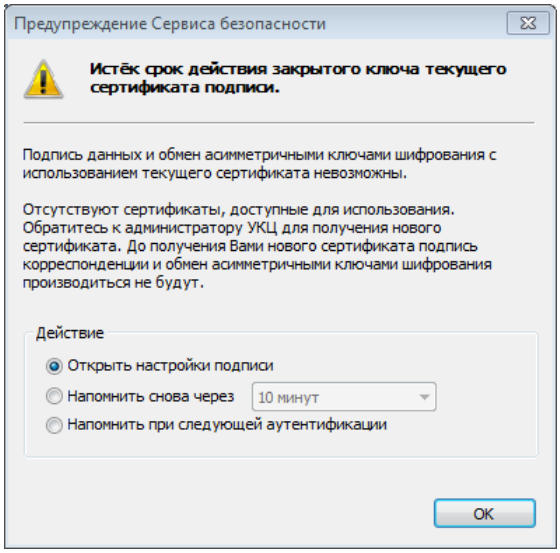


Рисунок 171: Предупреждение о том, что истек срок действия закрытого ключа

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 Client.
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. 256).

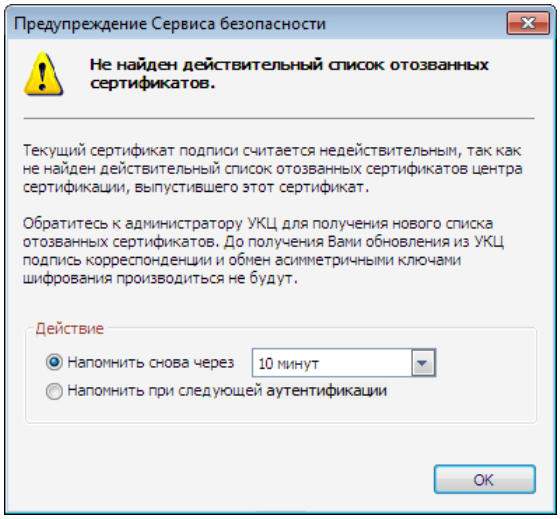


Рисунок 172: Предупреждение о том, что действительный список отозванных сертификатов не найден

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 Client.

  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 149 на стр. 316) 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 149 на стр. 316), 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. 316).

     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**.

B

События, отслеживаемые ПО ViPNet

Все события разделены на группы и подгруппы. Иерархическая схема этих групп изображена на следующем рисунке:

Рисунок 173: Классификация событий в Журнале IP-пакетов

Блокированные IP-пакеты

*Таблица 8. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные правилами 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

№ события	Название события	Описание события
17	**Неверный IP-адрес**	Это событие регистрируется только на координаторе, осуществляющем туннелирование. На координатор поступил зашифрованный пакет, предназначенный для туннелируемого ресурса данного координатора, но IP-адрес ресурса отсутствует в списке туннелируемых адресов данного координатора.
18	**Неизвестный IP-адрес получателя**	Это событие регистрируется только на координаторе. Появляется в случае, если координатор не знает, на какой адрес перенаправить входящий пакет
70	**Пакет заблокирован транзитным фильтром для защищенного узла**	Это событие регистрируется только на координаторе с операционной системой Linux. Пакет заблокирован правилом фильтрации для транзитного зашифрованного трафика

*Таблица 9. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные правилами открытой сети***

№ события	Название события	Описание события
22	**Незашифрованный IP-пакет от сетевого узла**	От защищённого адресата пришёл открытый пакет
23	**Незашифрованный широковещательный IP-пакет от сетевого узла**	От защищённого адресата пришёл открытый широковещательный пакет
30	**Локальный IP-пакет блокирован фильтром открытой сети**	Пакет блокируется правилом фильтрации открытой сети из группы локальных правил или для пакета не удалось найти подходящее правило
31	**Транзитный IP-пакет блокирован фильтром открытой сети**	Это событие регистрируется только на координаторе. Пакет блокируется правилом фильтрации открытой сети из группы транзитных правил или для пакета не удалось найти подходящее правило
32	**Широковещательный IP-пакет блокирован фильтром открытой сети**	Пакет блокируется правилом фильтрации открытой сети из группы широковещательных правил или для пакета не удалось найти подходящее правило
33	**IP-пакет блокирован фильтром антиспуфинга**	Это событие регистрируется только на координаторе. Найдено соответствующее правило в таблице антиспуфинга

№ события	Название события	Описание события
34	**Неподдерживаемый тип ICMP-сообщения**	ICMP-пакет не принадлежит ни одному из существующих соединений и при этом его тип отличен от типа 8, кода 0
37	**Пакет блокирован фильтром для туннелируемых узлов**	Это событие регистрируется только на координаторе. Пакет блокируется правилом фильтрации для туннелируемых узлов или для пакета не удалось найти подходящее правило
38	**Пакет блокирован правилом 1 режима**	Пакет блокируется 1 режимом безопасности, установленным на сетевых интерфейсах
39	**IP-пакет блокирован фильтрами по умолчанию при загрузке компьютера**	Пакет заблокирован фильтрами по умолчанию при загрузке компьютера

*Таблица 10. 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.

№ события	Название события	Описание события
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 «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**	Поступили пакеты с одинаковыми идентификационными номерами СУ, но разными IP-адресами
97	**IP-пакет блокирован фильтром SQL**	Соединение заблокировано Microsoft SQL фильтром
100	**Недопустимые флаги TCP**	Блокируются новые соединения с установленными одновременно флагами SYN+FIN/RST. Также блокируются новые (с точки зрения ПО ViPNet) соединения без флага SYN. То есть если до загрузки ПО ViPNet были установлены какие-либо TCP-соединения, то после загрузки все пакеты, касающиеся этих соединений, будут блокироваться. Блокируется «некорректный» пакет в уже установленном TCP-соединении.
101	**Не найден маршрут для транзитного IP-пакета**	Это событие регистрируется только на координаторе. Не найдено правило для транзитного пакета в таблице маршрутов

№ события	Название события	Описание события
102	**Модуль прикладной обработки не загружен**	Не загружен соответствующий модуль прикладной обработки
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 адаптер
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

Пропущенные IP-пакеты и служебные события

*Таблица 11. 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 12. Группа **Все IP-пакеты\Все пропущенные IP-пакеты\Пропущенные незашифрованные IP-пакеты***

№ события	Название события	Описание события
60	**Пропущен незашифрованный локальный IP-пакет**	Найдено разрешающее правило фильтрации открытой сети в группе локальных правил
61	**Пропущен незашифрованный широковещательный IP-пакет**	Найдено разрешающее правило фильтрации открытой сети в группе широковещательных правил
62	**Пропущен незашифрованный транзитный IP-пакет**	Это событие регистрируется только на координаторе. Найдено разрешающее правило фильтрации открытой сети в группе транзитных правил

№ события	Название события	Описание события
63	**Пакет пропущен фильтром для туннелируемых узлов**	Это событие регистрируется только на координаторе. Найдено разрешающее правило фильтрации для туннелируемых узлов
64	**IP-пакет пропущен фильтрами по умолчанию при загрузке компьютера**	Пакет пропущен фильтрами по умолчанию при загрузке компьютера

*Таблица 13. 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 МЭ 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 МЭ 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**

№ события	Название события	Описание события
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

События системы обнаружения атак

Таблица 14. Атаки, основанные на особенностях протокола IP

№ события	Название события	Описание события
1001	**Атака Land**	Попытка злоумышленника замедлить работу компьютера. Атака использует уязвимость стека TCP/IP, заключающуюся в том, что путем передачи фальшивого TCP-пакета можно заставить атакуемый компьютер попытаться установить соединение самому с собой, путем отправки SYN-пакета с адресом отправителя, идентичным адресу атакуемого компьютера
1002	**IP-опции нулевой длины**	Попытка злоумышленника вывести из строя внешний сетевой экран путем посылки пакета с IP-опциями нулевой длины
1003	**Пустой IP-фрагмент**	Обнаружен пустой IP-фрагмент
1020	**Атака Jolt2**	Обнаружен пакет с некорректным смещением фрагмента, соответствующим атаке Jolt2. Атака заключается в посылке в течение короткого промежутка времени большого числа специально сформированных пакетов с целью замедлить атакуемую систему

Таблица 15. Атаки, основанные на особенностях протокола ICMP

№ события	Название события	Описание события
1101	**Возможная атака Smurf**	Обнаружен ICMP-запрос, отправленный на адрес подсети (x.x.x.0 или x.x.x.255); такой запрос способен инициировать множественные эхо-ответы, которые могут перегрузить сеть или атакуемую систему
1104	**ICMP-запрос маски подсети**	Обнаружен запрос на получение значения маски подсети. Такая информация может помочь хакеру собрать данные о конфигурации сети
1106	**Фрагментация ICMP-заголовка**	ICMP-заголовок был разбит на несколько фрагментов в попытке обойти сетевые экраны или системы обнаружения вторжений

Таблица 16. Атаки, основанные на особенностях протокола UDP

№ события	Название события	Описание события
1203	**Урезанный UDP-заголовок**	Обнаружен UDP-пакет с аномально коротким заголовком
1204	**Возможная атака Fraggle**	Обнаружен UDP-пакет, отправленный на адрес подсети (x.x.x.0 или x.x.x.255) и предназначенный для одного из «отражающих» портов; такой пакет способен инициировать множество ответов, которые могут перегрузить сеть или атакуемую систему
1205	**Зацикливание портов UDP**	Обнаружен UDP-пакет, зацикленный между двумя «отражающими» портами. Такие пакеты могут отражаться бесконечное число раз, перегружая сеть и ресурсы вовлеченных систем
1206	**Атака Snork**	Попытка вызова отказа в обслуживании

Таблица 17. Атаки, основанные на особенностях протокола TCP

№ события	Название события	Описание события
1302	**Фрагментация TCP-заголовка**	TCP-заголовок был разбит на несколько фрагментов в попытке обойти сетевые экраны или системы обнаружения вторжений
1303	**Урезанный TCP-заголовок**	Обнаружен TCP-пакет с аномально коротким TCP-заголовком
1304	**Неправильное смещение Urgent в TCP-заголовке**	Множество таких пакетов могут вызвать «зависание» у некоторых реализаций TCP/IP
1305	**Атака WinNuke**	Попытка привести Вашу систему к перезагрузке. Атака использует ошибку реализации стека TCP/IP при посылке пакета Out of Band
1306	**TCP-опции нулевой длины**	Попытка злоумышленника вывести из строя Ваш внешний сетевой экран с помощью посылки пакета с TCP-опциями нулевой длины
1307	**Сканирование TCP XMAS**	Обнаружен TCP-пакет с установленными битами FIN, URG и PUSH. Злоумышленник пытается определить наличие доступных служб на Вашей системе, посылая такие специально сформированные пакеты

№ события	Название события	Описание события
1308	**Сканирование TCP null**	Обнаружен TCP-пакет со сброшенными всеми управляющими битами. Злоумышленник пытается определить наличие доступных служб на Вашей системе, посылая такие специально сформированные пакеты

Глоссарий

D

DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса серверов DNS, IP-адреса серверов WINS.

P

PKI (инфраструктура открытых ключей)

PKI (инфраструктура открытых ключей) — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам в распределенных системах через создание сертификатов открытых ключей и поддержание их жизненного цикла.

См. также: Открытый ключ.

V

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя ЦУС и УКЦ.

См. также: Сеть ViPNet, Удостоверяющий и ключевой центр (УКЦ), Центр управления сетью (ЦУС).

ViPNet Manager

Приложение, которое входит в состав линейки программных продуктов ViPNet OFFICE, предназначено для создания, конфигурирования и управления малыми и средними сетями ViPNet. Также выполняет функции удостоверяющего и ключевого центров.

ViPNet SafeDisk-V

Программное обеспечение ViPNet SafeDisk-V входит в состав программного комплекса ViPNet CUSTOM. ViPNet SafeDisk-V предназначено для защиты конфиденциальной информации. Для хранения конфиденциальной информации в программе ViPNet SafeDisk-V создается контейнер, который представляет собой зашифрованный файл на жестком диске или на съемном носителе.

Работа с программой ViPNet SafeDisk-V возможна только совместно с программой ViPNet Client.

А

Абонентский пункт (АП)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора абонентский пункт не выполняет функции маршрутизации трафика и служебной информации.

См. также: Координатор (ViPNet-координатор), Маршрутизация, Сетевой узел ViPNet (СУ).

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности). Аутентификация осуществляется на основании того или иного секретного элемента (аутентификатора), которым располагает субъект.

В

Виртуальный IP-адрес

Виртуальный IP-адрес назначается непосредственно на данном узле (А) для узла (Б) и привязывается к идентификатору сетевого узла (Б). Использование виртуальных адресов позволяет устранить конфликт, если узлы работают в локальных сетях с пересекающимся адресным пространством, и скрыть реальную топологию сети.

См. также: Реальный IP-адрес, IP-адрес.

Внешние IP-адреса

Адреса внешней сети.

См. также: Внешняя сеть.

Внешняя сеть

Сеть, имеющая другое адресное пространство по отношению к внутренней сети. Как правило, этот термин используется для обозначения глобальной сети Интернет.

См. также: Внутренняя сеть.

Д

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Manager для каждого пользователя сетевого узла ViPNet. В этом файле помещены адресные справочники, ключевая информация 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: Адресные справочники, Сетевой узел ViPNet (СУ), Удостоверяющий и ключевой центр (УКЦ), Файл лицензии.

Допустимые в Интернете IP-адреса

Все IP-адреса, кроме зарезервированных для использования в локальных сетях частных IP-адресов.

См. также: Локальная сеть (LAN), Частный адрес.

З

Запрос на сертификат

Файл, содержащий имя пользователя в формате X.500, открытый ключ и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

Запрос может быть сформирован как на издание нового, так и на обновление уже имеющегося сертификата.

См. также: Сертификат открытого ключа подписи пользователя, Открытый ключ, Закрытый ключ.

Защищенное соединение

Соединение между узлами, зашифрованное с помощью ПО ViPNet.

Защищенные прикладные серверы

Прикладные серверы (web-сервер, почтовый сервер, FTP-сервер и т.д.), размещенные на защищенных узлах.

См. также: Защищенный узел.

Защищенный DNS или WINS сервер

Сервер DNS или WINS, размещенный на защищенном узле.

См. также: Защищенный узел.

Защищенный узел

Сетевой узел, на котором установлено ПО ViPNet с функцией шифрования трафика на сетевом уровне.

К

Клиент (ViPNet-клиент)

Сетевой узел, на котором установлена программа ViPNet Client.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Коллектив

Совокупность пользователей одного сетевого узла ViPNet, имеющих одни и те же ключи для шифрования конфиденциальной информации.

См. также: Сетевой узел ViPNet (СУ).

Контейнер ключей

Файл, в котором хранятся закрытый ключ и соответствующий ему сертификат открытого ключа.

При формировании запроса на обновление сертификата имя контейнера, в котором будет храниться новая пара ключей подписи (закрытый и сертификат), задается автоматически и имеет вид `sgn-<случайное число 16-ричного формата>`.

См. также: Сертификат открытого ключа подписи пользователя.

Координатор (ViPNet-координатор)

Сетевой узел с установленным программным обеспечением ViPNet Coordinator, выполняющий в рамках сети ViPNet серверные функции, маршрутизацию трафика и служебной информации.

См. также: Маршрутизация, Сеть ViPNet.

О

Обновление справочно-ключевой информации

При различных изменениях в сети ViPNet (добавление, удаление сетевого узла ViPNet, добавление пользователя, издание нового сертификата и т.д.), производимых администратором в ЦУС, УКЦ, ViPNet Manager, может изменяться справочно-ключевая информация для сетевых узлов ViPNet. В этом случае администратор сети ViPNet централизованно высылает на СУ сформированные обновления из ЦУС или ViPNet Manager (возможно обновление как одного из совершенных изменений, так и всех одновременно).

См. также: Администратор сети ViPNet, Сетевой узел ViPNet (СУ), Сеть ViPNet, Справочно-ключевая информация, Удостоверяющий и ключевой центр (УКЦ), Центр управления сетью (ЦУС), ViPNet Manager.

Общий коллектив

Коллектив, который автоматически регистрируется на сетевом узле и включает всех пользователей данного сетевого узла.

Ключи для обмена между общими коллективами сетевых узлов используются в программах:

- ViPNet Монитор для защиты трафика,
- ViPNet Деловая почта при зашифровании писем (если не нужно разграничивать доступ между пользователями сетевого узла ViPNet),
- ViPNet MFTP при обмене служебными конвертами.

См. также: Коллектив.

Открытый Интернет

Технология, реализованная в ПО ViPNet, которая позволяет подключить группу компьютеров локальной сети, которым разрешена работа в Интернете, к открытым интернет-ресурсам, обеспечивая их изолированность от возможных атак извне без физического отключения от локальной сети.

См. также: Локальная сеть (LAN), Сетевая атака.

Открытый сервер DNS или WINS

Сервер DNS или WINS на открытом узле.

См. также: Открытый узел.

Открытый узел

Узел, с которым обмен информацией происходит в незашифрованном виде.

П

Папка справочно-ключевой информации

Папка, в которую устанавливается дистрибутив ключей. Несколько программ ViPNet могут использовать одну и ту же папку справочно-ключевой информации.

См. также: Дистрибутив ключей.

Пароль администратора сетевого узла ViPNet

Пароль для временного включения на сетевом узле ViPNet режима администратора, в рамках которого появляются дополнительные возможности настройки приложений

ViPNet. Пароль администратора СУ может быть создан в УКЦ или ViPNet Manager администратором сети ViPNet.

См. также: Администратор сети ViPNet, Сетевой узел ViPNet (СУ), Удостоверяющий и ключевой центр (УКЦ), ViPNet Manager.

Пароль пользователя на основе парольной фразы

Пароль пользователя необходим для входа в любую программу ViPNet. Случайный пароль создается на основе парольной фразы, которую можно использовать для запоминания пароля. Парольные фразы могут быть созданы на русском, английском и немецком языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объему словаря (русского, немецкого или английского). Парольная фраза может содержать 3 или 4 слова, при желании пароль может быть создан из двух парольных фраз.

Чтобы получить пароль из парольной фразы, достаточно набрать без пробелов в английской раскладке первые X букв из каждого слова парольной фразы, содержащей Y слов. Пользователь сам задает параметры X и Y, а также язык парольной фразы.

Например, при использовании трех первых букв из каждого слова парольной фразы «Затейливый ювелир утащил сдобу» получим пароль «pfn.dtenfclj».

См. также: Пароль пользователя, Парольная фраза.

Полномочия пользователя

Права, определяющие допустимость различных действий пользователей на сетевом узле ViPNet по изменению настроек установленного на нем ПО ViPNet.

Администратор ЦУС выставляет полномочия пользователей одного сетевого узла ViPNet в рамках прикладной задачи. Если полномочия пользователя ограничены, ввод пароля администратора сетевого узла ViPNet снимет эти ограничения, предоставив максимальные полномочия в приложениях.

См. также: Администратор ЦУС, Пароль администратора сетевого узла ViPNet, Прикладная задача, Сетевой узел ViPNet (СУ).

С

Сертификат открытого ключа подписи пользователя

Электронный документ заранее 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 сети ViPNet сертификат создается программой УКЦ и заверяется электронной подписью администратора УКЦ.

Электронная подпись Удостоверяющего центра (администратора УКЦ), заверяющая содержимое каждого сертификата, обеспечивает подлинность и целостность указанной в нем информации, включая описание владельца и его открытый ключ. Спецификация содержимого и формат сертификата в сети ViPNet соответствует стандарту X.509 версии 3 и Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года.

См. также: Администратор УКЦ, Открытый ключ, Электронная подпись.

Сетевой узел ViPNet (СУ)

Узел с установленным ПО ViPNet, с помощью которого защищают информацию приложений ViPNet, хранимую локально на компьютере, и (или) трафик посредством шифрования, имитозащиты и электронной подписи.

См. также: Сеть ViPNet, Электронная подпись.

Сеть ViPNet

Логическая сеть, организованная с помощью ПО 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 (СУ).

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны администратором Удостоверяющего центра и на данный момент недействительны.

См. также: Уполномоченное лицо (администратор) Удостоверяющего центра.

Структура сети ViPNet

Для обеспечения безопасности корпоративной сети необходима установка программного обеспечения ViPNet, которое позволяет защитить весь сетевой трафик, а также информацию, хранящуюся на компьютерах. При этом доступ к защищенному компьютеру с открытых или других защищенных компьютеров может быть в той или иной степени ограничен.

Для организации такой защиты необходимо развернуть сеть ViPNet, базовыми компонентами которой являются:

- рабочее место администратора сети ViPNet с установленным ПО ViPNet Administrator и ViPNet Client или ViPNet CryptoService (для сети ViPNet CUSTOM) или ViPNet Manager и ViPNet Client (для сети ViPNet OFFICE) для организации обмена служебной информацией с другими узлами сети ViPNet;
- координаторы — серверы с установленным ПО ViPNet Coordinator, размещенные на границах сетей или сегментов сети;
- компьютеры пользователей с установленным клиентским ПО ViPNet Client (для сетей ViPNet CUSTOM и ViPNet OFFICE) или ViPNet CryptoService (только для сетей ViPNet CUSTOM).

Каждый клиентский узел должен быть зарегистрирован на координаторе. Каналы 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: «ViPNet Administrator», «Координатор (ViPNet-координатор)», «Защищенный узел», «Открытый узел», «Сеть ViPNet», «ViPNet Manager».

Т

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса, использующиеся в одной сети, в адреса, использующиеся в другой. При этом одна сеть будет называться внутренней сетью, другая — внешней.

Например, NAT служит для преобразования адресов, зарезервированных для использования в локальных сетях, в адреса Интернета.

См. также: Внешняя сеть, Внутренняя сеть, Динамическая трансляция сетевых адресов, Статическая трансляция сетевых адресов.

Туннелируемый узел

Узел, на котором не установлено ПО 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: За координатором (узел, стоящий за координатором), Клиент (ViPNet-клиент), Координатор (ViPNet-координатор), Туннелирование.

У

Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет справочники и ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками отозванных сертификатов.

См. также: Администратор УКЦ, Корневой сертификат, Пользователь ViPNet, Список отозванных сертификатов (СОС), ViPNet Administrator.

Ц

Центр управления сетью (ЦУС)

Программа, входящая в ПО ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение конфигурации виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка защищенных адресных справочников;
- формирование информации о связях пользователей для УКЦ;
- определений полномочий пользователей сетевых узлов ViPNet.

См. также: Адресные справочники, Полномочия пользователя, Сетевой объект, Удостоверяющий и ключевой центр (УКЦ), ViPNet Administrator.

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 применяются в Интернете. Если вы имеете адрес из такого диапазона и хотите выйти в Интернет, используйте межсетевой экран с NAT.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

См. также: Межсетевой экран (МЭ), Трансляция сетевых адресов (NAT).

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 ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Указатель