ViPNet Client 4

Руководство пользователя

Версия продукта: 4.5.5 hotfix 9

infotecs

ФРКЕ.00116-05 34 01

Версия продукта 4.5.5 hotfix 9

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

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

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

Данное руководство предназначено для пользователей программного обеспечения ViPNet Client® for Windows (далее — ViPNet Client). В нем содержится информация о назначении и составе программы ViPNet® Client, а также рекомендации по настройке и использованию возможностей программы ViPNet Client.

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

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

Соглашения документа

Обозначение	Описание
	**Внимание!** Содержит критически важную информацию
	**Примечание.** Содержит рекомендательную информацию
	**Совет.** Содержит полезные приёмы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
`Код`	Имя файла, путь, фрагмент кода или команда в командной строке

Примечание. В документе могут присутствовать снимки интерфейса из предыдущих версий продукта. Поэтому некоторые элементы интерфейса, которые не влияют на понимание текста, могут выглядеть не так, как в продукте.

О программе

Назначение ПО ViPNet Client

Программное обеспечение ViPNet Client предназначено для использования в сетях ViPNet, управляемых с помощью ПО ViPNet Administrator. 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, удалённый, мобильный компьютер или сервер.

Состав ПО ViPNet Client

Программное обеспечение ViPNet Client состоит из следующих компонентов:

- Низкоуровневый драйвер сетевой защиты ViPNet-драйвер.
- Сервис управления драйвером защиты.
- Программа ViPNet Client.
- Транспортный модуль ViPNet MFTP.
- Программа ViPNet Контроль приложений.
- Программа ViPNet Деловая почта.
- Криптопровайдер ViPNet CSP.
- Модуль расширенной фильтрации.
- Система обновления ViPNet.

Низкоуровневый ViPNet-драйвер сетевой защиты

ViPNet-драйвер (см. Принцип работы ViPNet-драйвера) выполняет шифрование и фильтрацию IP-трафика. Он взаимодействует с драйверами сетевых интерфейсов компьютера (реальных и виртуальных), что обеспечивает независимость программы от операционной системы. ViPNet-драйвер перехватывает и контролирует весь входящий и исходящий IP-трафик компьютера.

Сервис управления драйвером защиты ViPNet

Сервис управления — это служба Windows, которая обеспечивает:

- загрузку в ViPNet-драйвер справочной информации о структуре сети, правил фильтрации и ключей шифрования;
- приём и передачу на другие сетевые узлы информации о состоянии узла и параметрах доступа;
- ведение журнала IP-пакетов (см. Работа с журналом IP-пакетов) и журнала событий (см. Просмотр журнала событий).

Программа ViPNet Client

Программа ViPNet Client предоставляет пользовательский интерфейс для изменения настроек ViPNet-драйвера, а также прикладные и административные возможности.

Для работы узла ViPNet и обеспечения безопасности компьютера запуск программы ViPNet Client не требуется.

Транспортный модуль ViPNet MFTP

Транспортный модуль — это служба Windows и графический интерфейс для её настройки. Функции ViPNet MFTP зависят от назначения программы, в которую он входит. На клиентском узле транспортный модуль обеспечивает обмен управляющими конвертами, конвертами программы ViPNet Деловая почта и файлами с другими сетевыми узлами ViPNet. Подробнее см. документ «ViPNet MFTP. Руководство администратора».

Программа ViPNet Контроль приложений

Программа ViPNet Контроль приложений — необязательный модуль ViPNet Client, ее наличие определяется лицензией на сеть ViPNet в вашей организации.

Программа ViPNet Контроль приложений позволяет:

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

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

Программа ViPNet Деловая почта

Программа ViPNet Деловая почта — необязательный модуль ViPNet Client, предназначена для обмена электронной почтой между пользователями сети ViPNet. С её помощью можно безопасно 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).

Подробнее см. документ «ViPNet Деловая почта. Руководство пользователя».

Криптопровайдер ViPNet CSP

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

С помощью криптопровайдера ViPNet CSP вы можете выполнять следующие операции:

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

Внимание! При установке ViPNet CSP в составе ViPNet Client поддержка протокола TLS/SSL отключена. Чтобы её включить:

1. В меню **Пуск** выберите **ViPNet** > **Настройка компонентов ViPNet Client** > **Изменить состав**.
2. В список **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** добавьте компонент **Поддержка протокола TLS/SSL**.

Не включайте поддержку протокола TLS/SSL, если планируется обновление ОС до Windows 10.

Подробнее см. документ «ViPNet CSP. Руководство пользователя».

Модуль расширенной фильтрации

Модуль расширенной фильтрации — система обнаружения вторжений. Он позволяет:

- создавать фильтры прикладного уровня;
- взаимодействовать с антивирусным программным обеспечением.

Система обновления ViPNet

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

Принцип работы ViPNet-драйвера

Ядром программного обеспечения ViPNet является ViPNet-драйвер, его основная функция — фильтрация, шифрование и расшифрование входящих и исходящих IP-пакетов.

Инициализация ViPNet-драйвера и ключей шифрования ViPNet выполняется перед входом пользователя в Windows, то есть до запуска остальных служб и драйверов операционной системы. 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-драйвер первым получает контроль над стеком протоколов TCP/IP. К моменту инициализации драйверов сетевых интерфейсов он подготовлен к шифрованию и фильтрации трафика. Это обеспечивает защищённое соединение с контроллером домена, контроль сетевой активности запущенных на компьютере приложений и блокирование нежелательных пакетов извне.

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

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

Каждый входящий пакет обрабатывается следующим образом:

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

ViPNet-драйвер работает между канальным и сетевым уровнем модели OSI, что позволяет обрабатывать входящие IP-пакеты до их обработки стеком протоколов TCP/IP и передачи на прикладной уровень. Таким образом, ViPNet-драйвер защищает IP-трафик всех приложений, не нарушая привычный порядок работы пользователей.

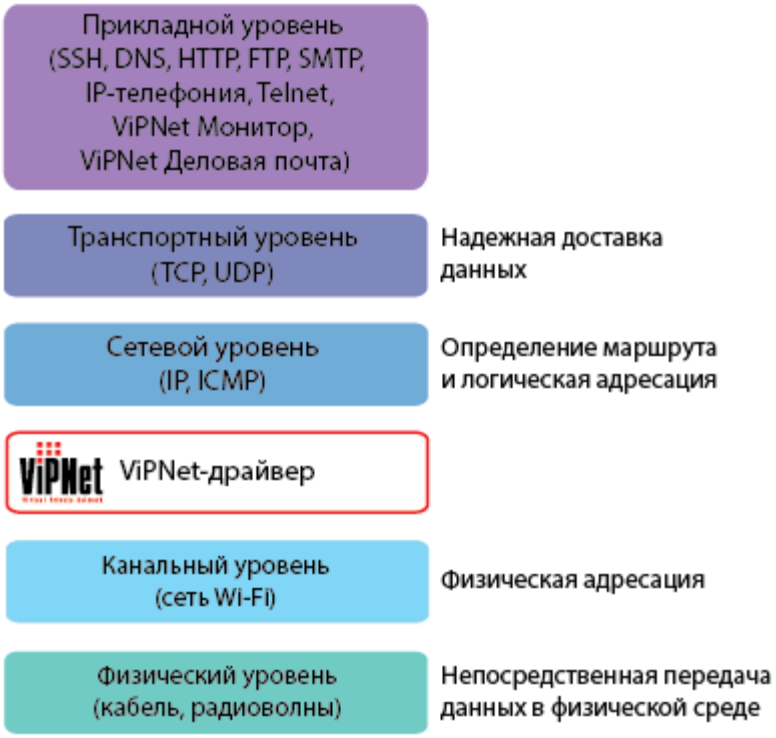


Рисунок 1. ViPNet-драйвер в модели OSI

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

Примечание. На приведённой схеме модели OSI есть 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.

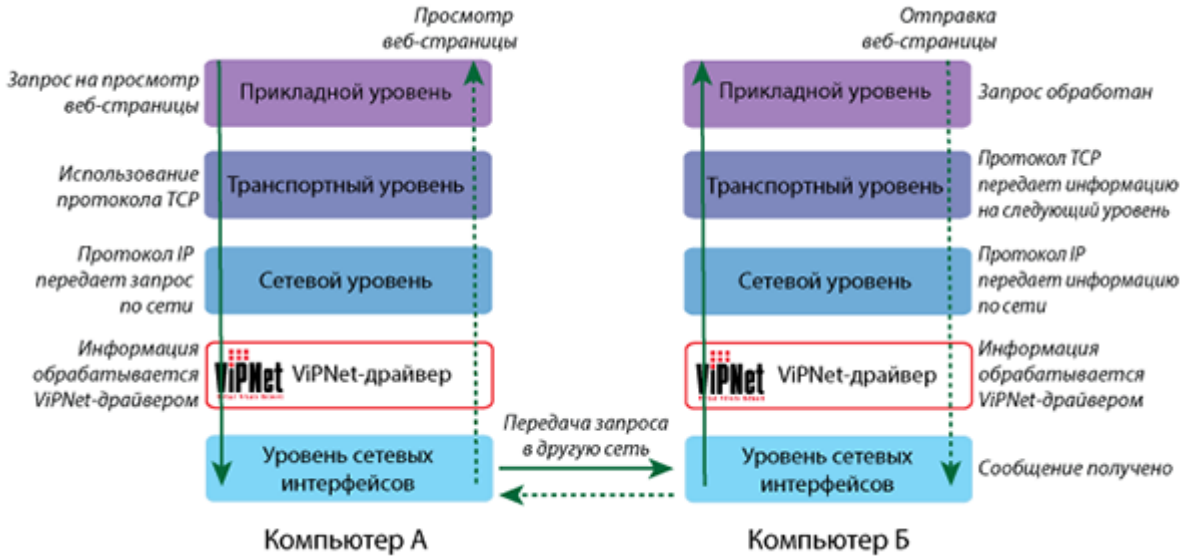


Рисунок 2. Схема работы сети TCP/IP, защищённой ПО ViPNet

Компьютер А отправляет на компьютер Б запрос по протоколу HTTP. Запрос передаётся 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 Б, принимает запрос и удаляет из него служебную информацию ViPNet. Затем ViPNet-драйвер расшифровывает запрос и передаёт по стеку TCP/IP на прикладной уровень для обработки.

Внимание! ViPNet-драйвер не работает с loopback-интерфейсом.

Что нового в версии 4.5.5 hotfix 9

Информацию о предыдущих версиях см. в приложении История версий.

- **Поддержка новых версий Windows**
  - Windows 11, версия 24H2, сборка 26100, редакции Enterprise и Pro;
  - Windows Server 2025, сборка 26100.
- **Окончание поддержки операционных систем**
  - Windows 10, версия 21H2, сборка 19044, редакция Enterprise;
  - Windows 11, версия 21H2, сборка 22000;
  - Windows 11, версия 22H2, сборка 22621, редакция Pro.

  Список совместимых ОС см. в разделе Системные требования.

Внимание! После обновления ViPNet Client на узле с ViPNet ЦУС перестанет работать обмен межсетевой информацией с сетями, в которых на узлах с ViPNet ЦУС или с центром управления ViPNet Prime установлены прошлые версии ViPNet Client.

Чтобы обмен межсетевой информацией работал, в доверенных сетях на узлах с ViPNet ЦУС и с центром управления ViPNet Prime должен быть установлен один из клиентов:

- ViPNet Client for Windows 4.5.3 hotfix 7 и выше
  или ViPNet Client for Windows 4.5.5 hotfix 9 и выше,
- ViPNet Client 5 for Windows 5.1 и выше,
- ViPNet Client 5 for Linux 5.0.0 или 5.1.3 и выше.

Системные требования

Требования к компьютеру для установки программы ViPNet Client:

- Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт.

Примечание. При большом количестве узлов и связей в сети ViPNet программа ViPNet Client запускается медленнее:

- при 10000 связей — 3-5 минут;
- при 20000 связей — 5-10 минут;
- при 30000 связей — 15-20 минут;
- при 60000 связей — 30-40 минут.

- Свободное место на жёстком диске — не менее 500 Мбайт (рекомендуется 1 Гбайт).
- Сетевой интерфейс (не более 10 IP-адресов на одном сетевом интерфейсе) или модем.
- Операционная система:
  - Windows 10 (32/64-разрядная) следующих версий и сборок:
    - версия 1507 (RTM), сборка 10240, редакция LTSB;
    - версия 1607, сборка 14393, редакция LTSB;
    - версия 1809, сборка 17763, редакция LTSC;
    - версия 21H2, сборка 19044, редакция LTSC;
    - версия 22H2, сборка 19045, все редакции.
  - Windows 11 следующих версий и сборок:
    - версия 22H2, сборка 22621, редакция Enterprise;
    - версия 23H2, сборка 22631, редакции Enterprise и Pro;
    - версия 24H2, сборка 26100, редакции Enterprise и Pro.
  - Windows Server 2016, сборка 14393;
  - Windows Server 2019, сборка 17763;
  - Windows Server 2022, сборка 20348;
  - Windows Server 2025, сборка 26100.

Внимание! Поскольку программа ViPNet Client предназначена для защиты трафика на рабочем месте пользователя, то стабильная работа всех сервисов серверных ОС не гарантируется. Для защиты трафика сервера воспользуйтесь технологией туннелирования ПО ViPNet Coordinator.

На терминальном сервере с ViPNet Client при одновременной работе более 10 пользователей могут не приходить обновления из ЦУСа. Для стабильной доставки обновлений выполните рекомендации раздела На терминальный сервер не приходят обновления.

- Для операционной системы должен быть установлен самый последний накопительный пакет обновлений.

Внимание! Если планируется обновление до Windows 10, перед обновлением убедитесь, что в программе ViPNet CSP отключена поддержка протокола TLS/SSL. Для этого:

1. В меню **Пуск** выберите **ViPNet** > **Настройка компонентов ViPNet Client**.
2. В окне **Управление составом ViPNet Client** выберите **Изменить состав**.
3. В списке **Поддержка работы ViPNet CSP через Microsoft CryptoAPI** снимите флажок у компонента **Поддержка протокола TLS/SSL** и нажмите **Далее**.
4. Перезагрузите компьютер, чтобы изменения вступили в силу.

- При использовании Internet Explorer — версия 11.
- На компьютере не должны быть установлены другие сетевые экраны (брандмауэры), программные NAT-устройства, ПО HP Velocity и ViPNet CSP версии ниже 4.4.0. Встроенным брандмауэром Windows на вашем компьютере управляет администратор сети ViPNet.
- На компьютере не должно быть установлено ПО и драйверы, которые работают на канальном уровне модели OSI, так как они могут отправлять и принимать трафик в обход драйвера ViPNet. Поэтому такой трафик не будет зашифровываться и блокироваться правилами межсетевого экрана (см. Принцип работы ViPNet-драйвера).

Драйверы канального уровня используют программы — анализаторы трафика (Wireshark), виртуальные платформы (Oracle VM VirtualBox, VMware Workstation) и другие. Если ПО необходимо, отключите работу таких драйверов. Например, если используются платформы виртуализации, то для всех сетевых интерфейсов компьютера отключите драйвер сетевого моста виртуальной платформы.

- Данная версия программы имеет ограниченную совместимость с ViPNet Administrator УКЦ версии 4.6.6 и ниже. Поэтому прежде чем установить ViPNet Client, обратитесь в службу поддержки ИнфоТеКС за новой версией ViPNet Administrator.

Совместная работа с другими программами ViPNet

ViPNet Client не поддерживает совместную работу со следующими программами:

- ViPNet CSP версии ниже 4.4.0;
- ViPNet Administrator УКЦ версии 4.6.6 и ниже;
- ViPNet SafeDisk-V, ViPNet Dispatcher, ViPNet CryptoService, ViPNet Registration Point, ViPNet Personal Firewall любых версий.

Комплект поставки

- Установочный файл программы.
- MSI-пакет агента (32- и 64-разрядная версии) для установки ПО через групповые политики.
- Файлы настроек для установки ПО через групповые политики: `parameters.xml`, `commands.xml`.
- Документация в формате PDF:
  - «ViPNet Client 4. Руководство пользователя».
  - «ViPNet Client 4. Быстрый старт».
  - «Работа с защищёнными DST. Быстрый старт».
  - «ViPNet Деловая почта 4. Руководство пользователя».
  - «ViPNet MFTP 4. Руководство администратора».
  - «ViPNet Контроль приложений 4. Руководство пользователя».
  - «ViPNet CSP 4.4. Руководство пользователя».
  - «Классификация полномочий. Приложение к документации ViPNet».
  - «ViPNet Client 4. Лицензионные соглашения на компоненты сторонних производителей».
  - «ViPNet CSP 4.4. Лицензионные соглашения на компоненты сторонних производителей».

Варианты исполнения ViPNet Client

Программное обеспечение ViPNet Client может поставляться в трёх вариантах исполнения в зависимости от требуемого класса защиты:

- Вариант исполнения 1, соответствующий классу защищённости КС1.
- Вариант исполнения 2, соответствующий классу защищённости КС2 при совместном использовании со средством защиты от НСД типа «электронный замок».
- Вариант исполнения 3, соответствующий классу защищённости КС3 при совместном использовании со средством защиты от НСД типа «электронный замок» и установленной и настроенной программой ViPNet Syslocker.

Соответствие классам защиты достигается за счёт выполнения настроек согласно документу «Правила пользования». Подробное описание перечисленных вариантов поставки ПО ViPNet Client приведено в формуляре.

Обработка персональных данных

Программное обеспечение ViPNet Client содержит несколько компонентов, которые работают с информацией о компьютере пользователя:

- Утилита Lumpdiag — запускается вручную пользователем, собирает и сохраняет в папке информацию о компьютере. Используется в случае неполадок в работе программы ViPNet для отправки сведений о системе в службу поддержки ИнфоТеКС.

  Утилита Lumpdiag собирает следующую информацию:

  - сведения об операционной системе;
  - сетевые настройки компьютера;
  - информация о сертификатах и ключах;
  - описание и настройки установленного на компьютере ПО ViPNet;
  - журналы событий и ошибок Windows и ПО ViPNet.

  Подробнее о работе и параметрах запуска Lumpdiag см. Сбор диагностической информации при возникновении неполадок.

- Агент для взаимодействия с ПО ViPNet StateWatcher — запускается автоматически и работает в фоновом режиме. Работает с информацией только при наличии в вашей сети комплекса мониторинга ViPNet StateWatcher. Собирает и отправляет администратору ViPNet StateWatcher следующую информацию:

  - текущее состояние компьютера и операционной системы;
  - описание и настройки установленного на компьютере ПО ViPNet;
  - сетевые настройки компьютера;
  - журналы событий и ошибок Windows и ПО ViPNet.

  Подробнее об информации, которая передаётся в ViPNet StateWatcher, см. в документе «Программный комплекс мониторинга защищённых сетей ViPNet StateWatcher. АРМ мониторинга. Руководство пользователя», приложение D «Контролируемые параметры».

  Подробнее о ViPNet StateWatcher см. документ «Программный комплекс мониторинга защищённых сетей ViPNet StateWatcher. Общее описание».

- Программа ViPNet Client — работает постоянно, в фоновом режиме. Собирает и передаёт на другие узлы ViPNet следующую информацию: время последней активности пользователя на компьютере, имя компьютера, название и версию ОС, версию установленного ПО ViPNet Client.

Обратная связь

Дополнительная информация

Сведения о продуктах ViPNet, частые вопросы и полезная информация на сайте ИнфоТеКС:

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:

+7 (495) 737-6192,

8 (800) 250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба поддержки: hotline@infotecs.ru.

Форма для обращения в службу поддержки через сайт.

Канал поддержки в Telegram: t.me/vhd21

Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов компании ИнфоТеКС регулируется политикой ответственного разглашения.

1

Установка, обновление и удаление ПО ViPNet Client

Установка ViPNet Client

Внимание! На компьютере, где устанавливается 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 ViPNet Client:

- Убедитесь, что на компьютере выполнены стандартные сетевые настройки и правильно заданы часовой пояс, дата и время.
- Отключите использование Юникода (см. Отключение Юникода (UTF-8) для поддержки языка во всем мире) и не включайте после установки программы.
- Если локализация Windows не русская, то для правильного отображения кириллицы в интерфейсе ViPNet Client измените региональные настройки Windows (см. Региональные настройки).

Для установки ViPNet Client требуются:

- Установочный `EXE`-файл программы.
- Дистрибутив ключей для сетевого узла — файл с расширением *.`dst` или *.`enc`. Если на узле планируется работа нескольких пользователей, для каждого из них нужен отдельный дистрибутив ключей.
- Пароль пользователя сетевого узла или внешнее устройство аутентификации (см. Внешние устройства).

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

Для установки ViPNet Client:

1. Запустите установочный файл  от имени администратора.
2. Примите лицензионное соглашение.
3. Чтобы установить все компоненты программы ViPNet Client с параметрами по умолчанию, нажмите **Установить**.
4. Чтобы изменить набор компонентов программы, нажмите **Компоненты и параметры** и укажите:
   - Компоненты ViPNet Client, которые необходимо установить.
     - Если вам требуются фильтры прикладного уровня или взаимодействие с антивирусной программой, установите компонент **ViPNet IDS HS Agent**.

- Если требуется аутентификация с помощью сертификата, установите компонент **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.

- Путь к папке установки программы на компьютере.

Нажмите **Далее** и укажите дополнительные параметры установки:

- **Создать ярлыки компонентов на рабочем столе**;
- **Автоматически перезагрузить компьютер при необходимости**.

Нажмите **Установить**.

5 Если появилось окно **Обнаружены проблемы совместимости**, выполните рекомендации, предложенные в этом окне.

6 Если после установки потребуется перезагрузить компьютер, появится соответствующее сообщение.

7 Выполните одно из действий:

- Если справочники и ключи ещё не установлены на компьютере, установите их (см. Установка справочников и ключей.
- Если на компьютере уже имеется ПО ViPNet, для которого ранее были установлены справочники и ключи, то при запуске программы укажите путь к папке ключей пользователя и папке ключей сетевого узла (см. Использование справочников и ключей, установленных ранее).

При первом запуске программы стандартный сетевой экран Windows может быть отключён в зависимости от настроек, заданных администратором сети ViPNet. Не включайте сетевой экран Windows во время использования ViPNet Client, так как эти программы могут конфликтовать.

Внимание! При установке ViPNet Client на виртуальной машине не используйте режим сетевых интерфейсов Bridged.

Установка в неинтерактивном режиме

В неинтерактивном режиме процесс установки программы ViPNet Client не отображается на экране компьютера. Установку в данном режиме можно выполнить с помощью командной строки Windows, запущенной от имени администратора. Параметры, которые обычно могут быть заданы в процессе установки (см. Установка ViPNet Client), в неинтерактивном режиме укажите заранее в командной строке.

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

Например, вы можете создать сценарий входа в систему (logon script), который запустит автоматическую установку ПО после загрузки системы. Информацию о создании сценариев входа в систему можно найти на сайте компании Microsoft. При установке ПО может потребоваться подтверждение в окне контроля учётных записей пользователей Windows.

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

```
<путь к установочному файлу> -q
```

Если программа ViPNet Client не была установлена в неинтерактивном режиме:

- Убедитесь, что компьютер соответствует системным требованиям.
- Запустите установку программы в интерактивном режиме. Если при установке будут обнаружены проблемы совместимости, выполните предложенные рекомендации для всех компьютеров, на которые устанавливается ViPNet Client.
- Обратитесь в службу поддержки ИнфоТеКС (см. Сбор диагностической информации при возникновении неполадок).

Дополнительные параметры установки в неинтерактивном режиме

При необходимости задайте дополнительные параметры установки:

- `-autorestart` — автоматически перезагрузить компьютер после завершения установки.
- `-SkipStartingMonitorAfterInstall="yes"` — не выводить предложение об установке ключей. Работает, если не задан параметр `-autorestart`.
- `-installfolder="<путь к папке установки>"` — изменить путь к папке установки компонентов программы ViPNet Client.

  В конце пути к папке установки не должно быть наклонной черты:

  `-installfolder="d:\program\vipnet"`
- `-x:"<путь к папке распаковки>"` — распаковать установщик программы.

После начала установки нельзя изменить параметры установки.

По умолчанию в неинтерактивном режиме ViPNet Client устанавливается в следующие папки:

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

Пример команды для установки ViPNet Client в неинтерактивном режиме с перезагрузкой:

```
<путь к установочному файлу> -q -autorestart
```

Чтобы получить помощь по параметрам установки, выполните команду:

```
<путь к установочному файлу> -q -help
```

Чтобы изменить набор компонентов программы:

Внимание! Выбор компонентов для установки с помощью параметров `-pc` и `-f` возможен, если ранее на компьютере не устанавливалась программа ViPNet Client.

---

1. Выполните команду `<путь к установочному файлу> -q -help`
2. В окне подсказки снимите флажки с компонентов, которые не нужны пользователю.

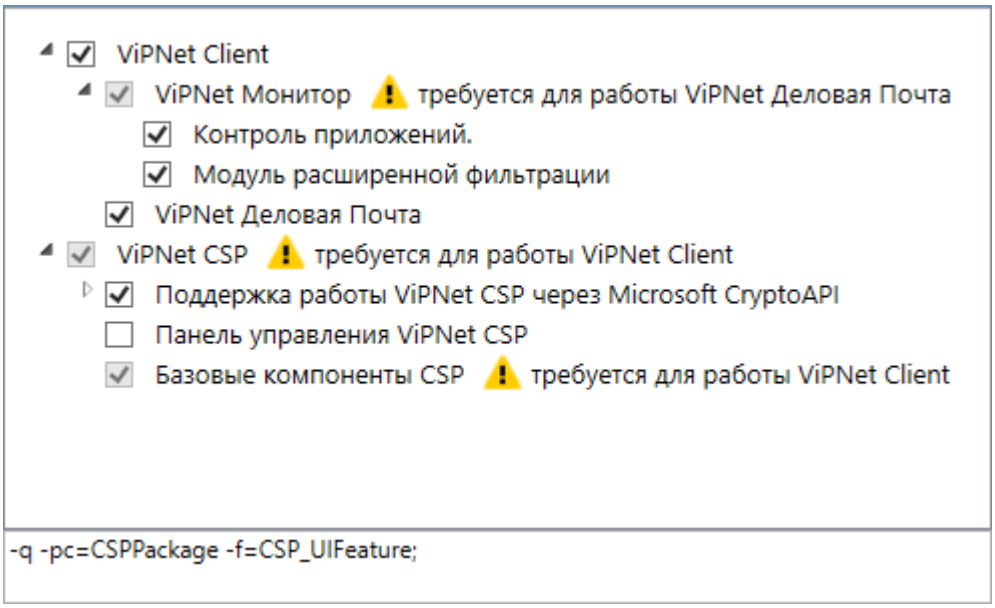


Рисунок 3. Выбор компонентов

3 Скопируйте параметры из строки внизу окна и добавьте к строке установки программы. Например: `client_lang_ver.exe -q -pc=CSPPackage -f=CSP_UIFeature;`

Установка ViPNet Client с помощью групповых политик

Примечание. Подробнее об установке программного обеспечения с помощью групповых политик см. на сайте Microsoft.

Вы можете автоматизировать установку ViPNet Client с помощью групповых политик Active Directory. В этом случае будут установлены все компоненты программы ViPNet Client. Если вы хотите изменить набор компонентов программы, выполните установку в интерактивном или в неинтерактивном режиме.

Для установки с помощью групповых политик потребуются следующие файлы из комплекта поставки ПО ViPNet:

- MSI-пакет агента для установки ПО (32- и 64-разрядная версии);
- установочный EXE-файл программы;
- файлы настроек:
  - `parameters.xml` — расположение файлов для установки и папки для регистрации событий во время установки;
  - `commands.xml` — набор команд для установки ViPNet Client;

Дополнительно потребуется скачать с сайта Microsoft:

- установщик .Net Framework 4.5;
- программу для создания MST-файлов ORCA MSI Editor.

Для установки ПО с помощью групповых политик выполните предварительные действия:

1 В произвольной сетевой папке, доступной всем компьютерам, на которые требуется установить ПО ViPNet, создайте папки `Distributives` и `logs`.

В сетевую папку поместите файлы `parameters.xml` и `commands.xml`, в папку `Distributives` — установочные файлы ViPNet Client и .Net Framework 4.5 и MSI-пакеты агента для установки. Для корректной установки ViPNet Client с помощью групповых политик ОС компьютера должна быть обновлена до последней версии.

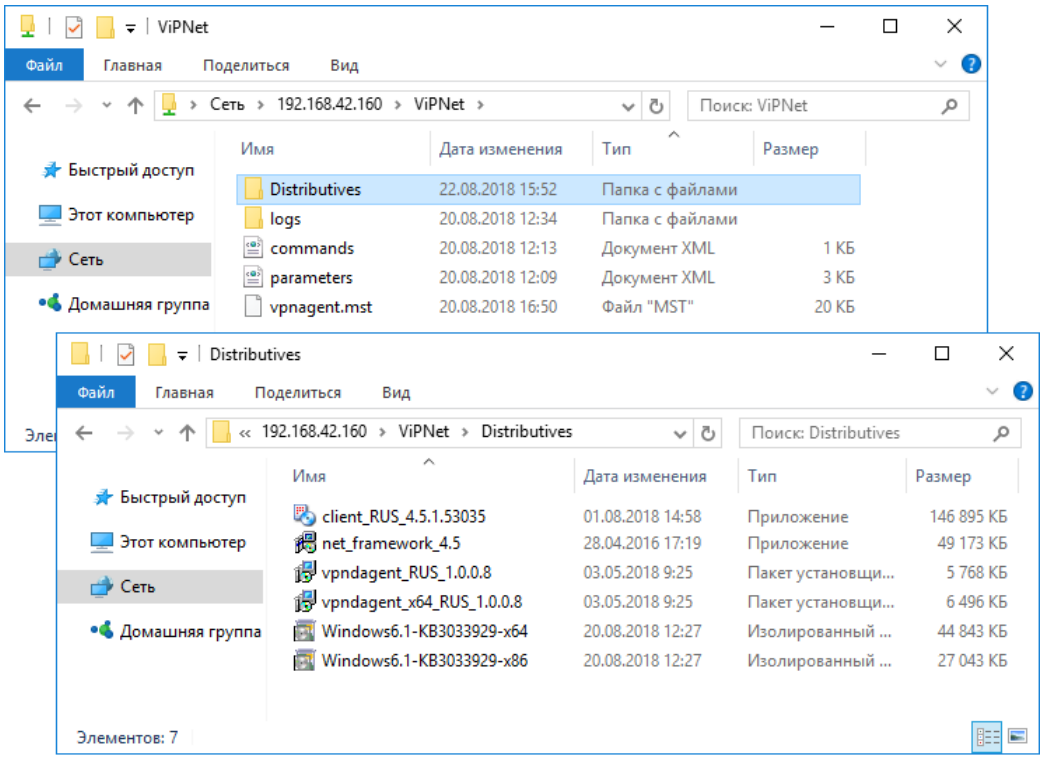


Рисунок 4. Папки с установочными пакетами

2 С помощью программы ORCA MSI Editor создайте файл трансформации MST (см. Создание файла трансформации MST) для MSI-пакета агента нужной разрядности. Поместите созданный файл MST в ту же сетевую папку.

3 Откройте для редактирования файл `parameters.xml` и замените путь `\\DC1\Shared` на путь к вашей сетевой папке.

   Убедитесь, что названия установочных файлов, указанных в `parameters.xml`, совпадают с названиями файлов в вашей папке `Distributives`.

Создайте объекты групповой политики (GPO) для установки ПО ViPNet на компьютеры вашей сети (на примере Windows Server 2016):

1 В домене Active Directory создайте одну или несколько групп, включающих компьютеры, на которые вы хотите установить ViPNet Client с помощью групповых политик. Параметры групп оставьте по умолчанию.

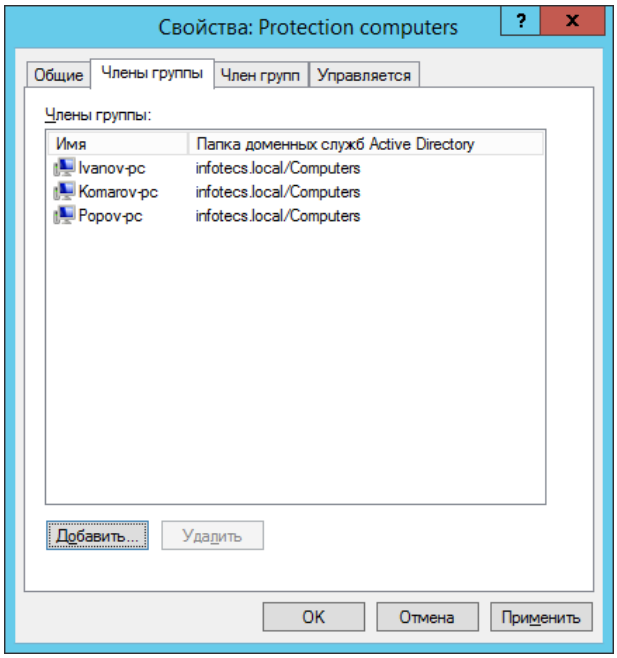


Рисунок 5. Состав группы компьютеров

2 Создайте новый объект групповой политики (GPO) и свяжите его с доменом.

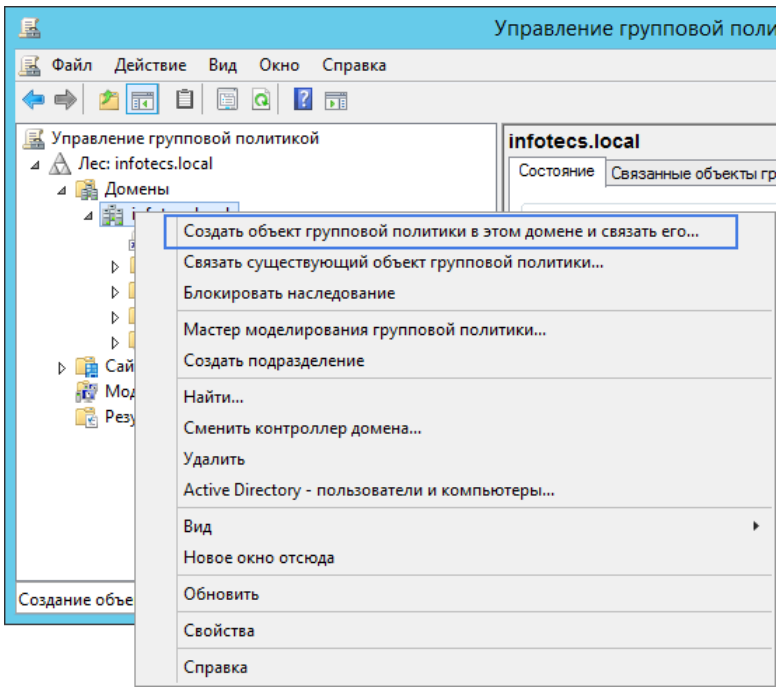


Рисунок 6. Создание нового объекта групповой политики

3 Откройте окно свойств объекта групповой политики и на вкладке **Область** в разделе **Фильтры безопасности** нажмите **Добавить**, чтобы добавить созданные ранее группы компьютеров.

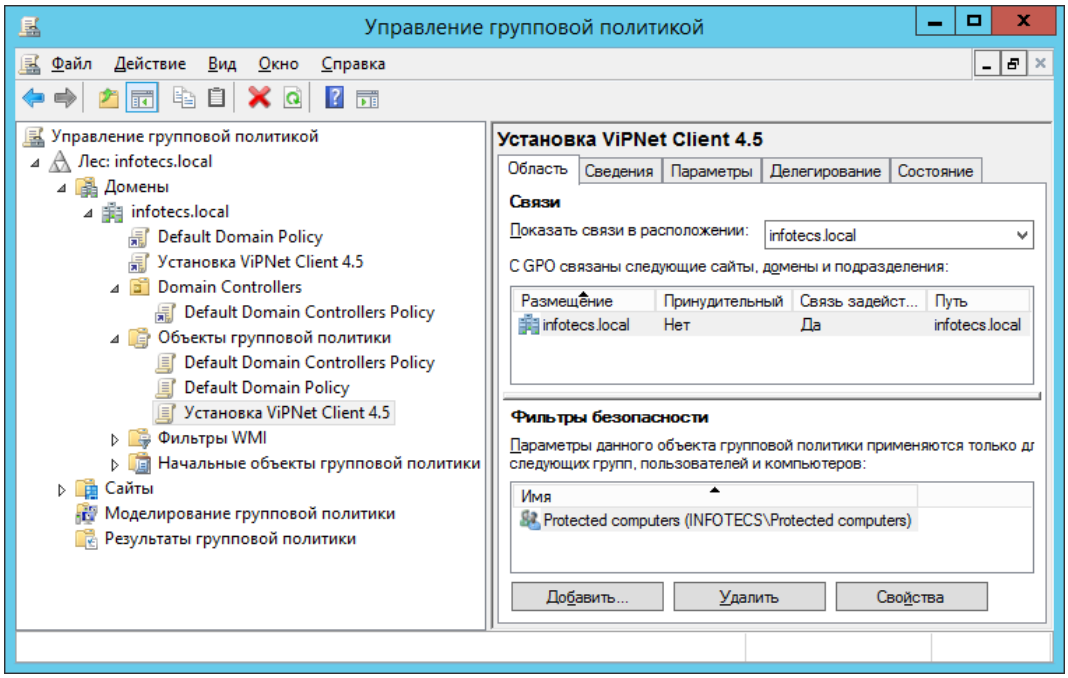


Рисунок 7. Свойства объекта групповой политики

4 Щёлкните объект групповой политики правой кнопкой мыши и выберите **Изменить**.

5 В окне редактора групповых политик выберите **Конфигурация компьютера** > **Политики** > **Конфигурация программ** > **Установка программ**.

6 Щёлкните правой мышкой раздел **Установка программ**, выберите **Создать** > **Пакет** и укажите сетевой путь к MSI-пакету агента нужной разрядности. Нажмите **Открыть**.

7 В окне **Развертывание программ** выберите метод развёртывания **Особый**.

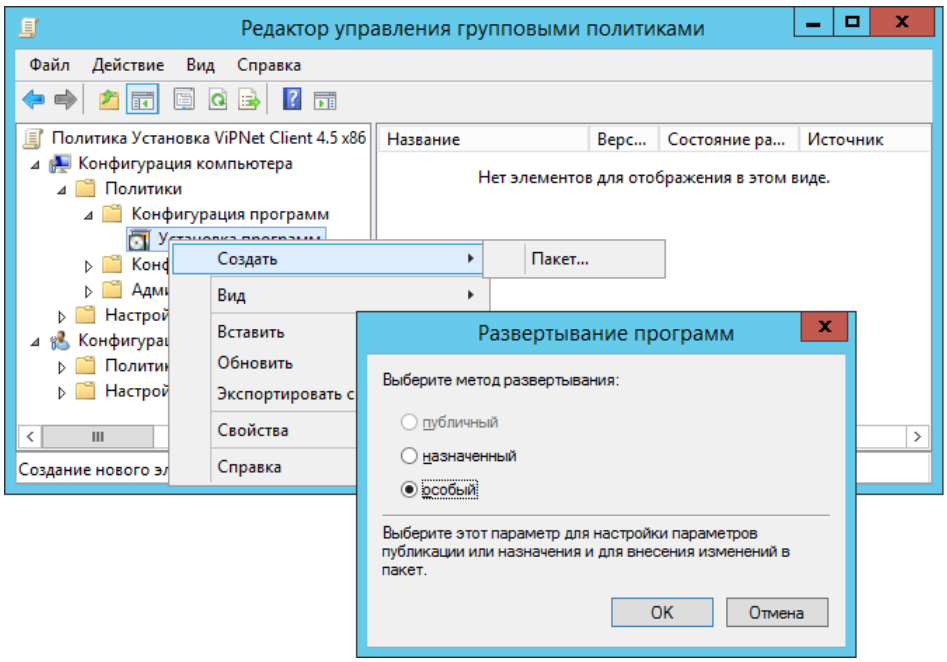


Рисунок 8. Добавление установочного пакета

8 В окне свойств установочного пакета на вкладке **Модификации** укажите сетевой путь к соответствующему файлу MST.

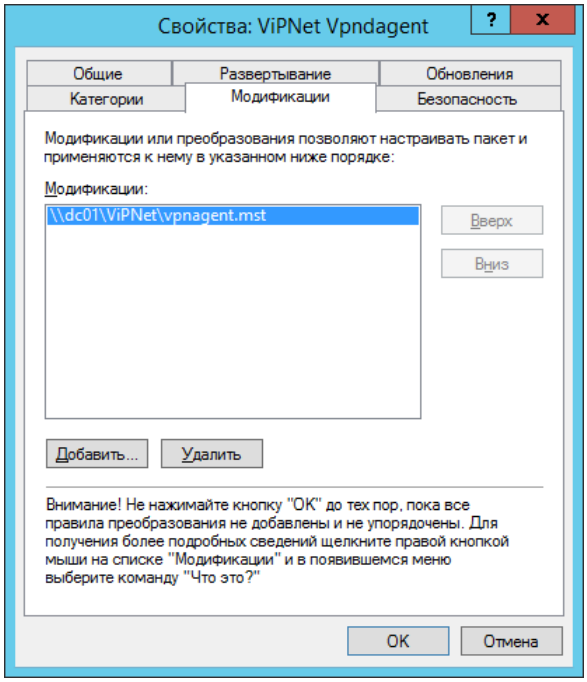


Рисунок 9. Добавление файлов настроек MST

9 На вкладке **Обновления** удалите все строки из списка **Приложения, обновляемые данным пакетом**.

10 На вкладке **Развертывание** нажмите **Дополнительно**, затем в окне дополнительных параметров:

- установите флажок **Не использовать языковые установки при развертывании**;
- снимите флажок **Сделать это 32-разрядное X86 приложение доступным для компьютеров с архитектурой Win64**.

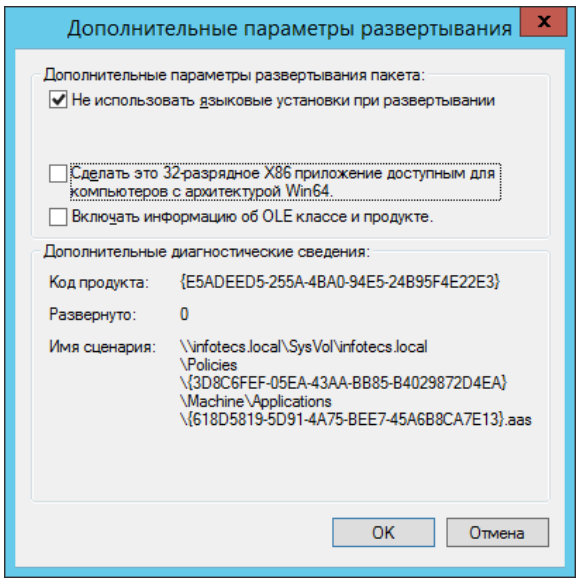


Рисунок 10. Дополнительные параметры развёртывания

11 При необходимости повторите шаги 6-10 для MSI-пакета агента другой разрядности.

12 Если вы хотите отключить журналирование процесса установки программ ViPNet Client, выполните следующие действия:

12.1 Щёлкните правой кнопкой мыши созданный объект групповой политики и выберите команду **Изменить**.

12.2 В окне редактора групповых политик на панели навигации выберите **Конфигурация компьютера** > **Политики** > **Административные шаблоны** > **Компоненты Windows** > **Установщик Windows**.

12.3 На панели просмотра дважды щёлкните параметр **Отключение ведения журнала с помощью параметров пакета** и в открывшемся окне установите переключатель в положение **Включено**.

13 После того как вы создадите объект групповой политики для автоматической установки необходимо перезагрузить компьютеры пользователей.

Примечание. Обновление групповых политик на компьютерах пользователей может происходить не сразу, если на контроллере домена задан большой интервал времени для обновления политик (по умолчанию — 90 минут). Чтобы инициировать немедленное обновление групповых политик в командной строке ОС Windows выполните команду `gpupdate`, а затем перезагрузите компьютеры пользователей.

Для отложенного обновления групповых политик в файле `parameters.xml` укажите дату и время для параметра `StartTime` и время отсрочки в секундах для параметра `CheckForNewCommandsMinutes`.

На компьютерах пользователей установка ViPNet Client будет выполняться в невидимом для пользователя режиме во время загрузки операционной системы. После установки программного обеспечения ViPNet Client и загрузки ОС на каждом сетевом узле появится предложение установить дистрибутив ключей ViPNet.

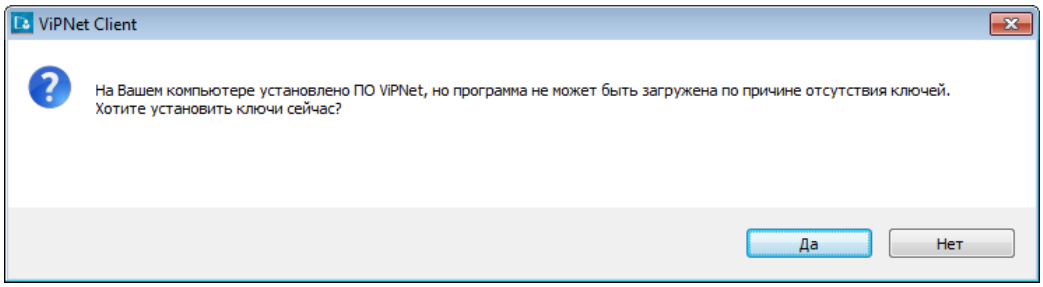


Рисунок 11. Предложение установить ключи

Для установки дистрибутива ключей ViPNet в окне с сообщением нажмите **Да**. Откроется окно программы установки ключей, следуйте инструкциям в разделе Установка справочников и ключей одного пользователя. При необходимости вы можете отказаться от установки дистрибутива ключей и выполнить её позже, для этого в окне с сообщением нажмите **Нет**.

Создание файла трансформации MST

Файл трансформации MST позволяет задать параметры для установочного пакета MSI. Для установки ПО ViPNet с помощью групповых политик агенту ViPNet требуется указать путь к файлу с параметрами установки ПО ViPNet (`parameters.xml`). Поскольку этот путь зависит от сетевых настроек в организации, то создание файла MST следует выполнять администратору организации.

1 Установите программу ORCA MSI Editor.

2 В программе ORCA в меню **File** выберите **Open** или нажмите **Ctrl+O**, затем укажите путь к файлу агента (`vpndagent_RUS_xxxx.msi`) нужной разрядности.

3 В меню **Transform** выберите **New Transform**.

4 В списке **Tables** выберите **Property**.

5 Если в таблице нет строки "PARAMETERS", нажмите **Ctrl+R**.

В окне **Add Row** для параметра **Property** введите "PARAMETERS".

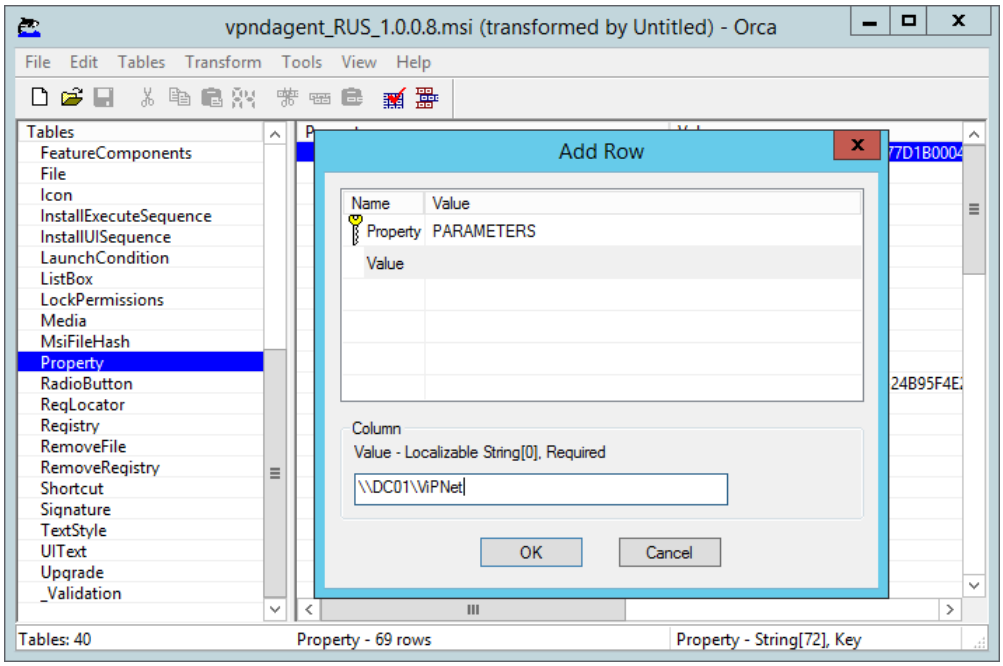


Рисунок 12. Добавление свойства Parameters для файла MST

6 Для строки "PARAMETERS" укажите **Value** — сетевой путь к папке с файлом `parameters.xml`.

7 В меню **Transform** выберите **Generate Transform** и сохраните файл трансформации в указанной выше сетевой папке под именем `vpnagent.mst`.

8 При необходимости создайте файл MST для MSI-пакета агента другой разрядности.

Удалённая установка ViPNet Client

Администратор сети ViPNet может выполнить установку или обновление программы удалённо, подключившись к компьютеру по протоколу RDP.

Внимание! На компьютере должно быть разрешено подключение к удалённому рабочему столу и настроен вход в систему без нажатия клавиш **Ctrl+Alt+Del**. Подробнее см. Настройка автоматического входа в Windows.

Для подключения на удалённом компьютере используйте учётную запись Windows, обладающую правами администратора и защищённую паролем.

Для дистанционной установки:

1. Скопируйте на удалённый компьютер программу установки ViPNet и набор ключей для сетевого узла (файл `*.dst` или `*.enc`).
2. С помощью стандартной программы Windows «Подключение к удалённому рабочему столу» установите доверенное подключение компьютеру, на который требуется установить ПО ViPNet.
3. В сеансе удалённой работы выполните установку ПО ViPNet (см. Установка ViPNet Client).
4. По завершении установки программы появится предложение установить набор ключей. Нажмите **Да**, укажите расположение файла `*.dst` (`*.enc`) и следуйте указаниям мастера установки ключей.

   После установки, если необходимо, перезагрузите удалённый компьютер. Удалённый сетевой узел ViPNet готов к работе.

Обновление ViPNet Client

Перед обновлением программы убедитесь, что:

- Компьютер соответствует системным требованиям, на нем не установлены сторонние межсетевые экраны и программы, обеспечивающие NAT.

  Иначе при установке программы с помощью мастера появится сообщение о проблемах совместимости. При других способах установки сообщение не появится, программа установлена не будет.

- В Windows 10 отключено использование Юникода (см. Отключение Юникода (UTF-8) для поддержки языка во всем мире).
- На компьютере установлен ViPNet Client версии 4.3.2 и выше. Для более ранней версии сначала установите версию 4.3 (2.37273). Затем закройте программу и установите 4.5.x.
- Лицензия на сеть ViPNet разрешает использовать новую версию. Если разрешения нет, программа не будет работать.
- Если на компьютере установлены программы ViPNet IDS HS и Wireshark, то перед обновлением выполните восстановление программы. Для этого в меню **Пуск** выберите **ViPNet** > **Настройка компонентов ViPNet Client**.
- Для версии 3.x сначала обновите ПО на компьютере с программой ViPNet Центр управления сетью. Это необходимо для того, чтобы в ЦУСе правильно отображались результаты рассылки обновлений справочников и ключей.
- Для версии 4.3 сначала обновите ПО на всех компьютерах сети ViPNet, а затем на компьютере с программой ViPNet Центр управления сетью.
- Если на компьютере установлена программа SafeDisk-V, выполните рекомендации раздела Обновление при использовании программы SafeDisk-V.
- Если на компьютере установлена программа ViPNet Administrator версии 4.6.6 и ниже, обратитесь в службу поддержки ИнфоТеКС за новой версией ViPNet Administrator или используйте ViPNet Client 4.5.1 и ниже.
- Если вы используете внешнее устройство JaCarta и ПО «Единый Клиент» 2.11, то перед обновлением ViPNet Client установите «Единый Клиент» 2.12.

Примечание. Если у вас JaCarta PKI и выполняются все условия:

- «Единый Клиент» 2.11 или 2.12;
- ViPNet Client 4.5.1 или ниже;
- способ аутентификации — **Устройство (Персональный ключ)**,

то перед обновлением ViPNet Client:

1. Смените способ аутентификации на **Пароль** (см. Изменение способа аутентификации пользователя).
2. Установите «Единый Клиент» 2.12 или выше.
3. Обновите ViPNet Client.
4. Смените способ аутентификации на **Устройство**.

Иначе работа с ViPNet Client и вход в Windows будут невозможны. Для продолжения работы потребуется заново развернуть сетевой узел ViPNet.

Вы можете выполнить обновление несколькими способами:

- Автоматическое обновление, отправленное централизованно на сетевые узлы администратором сети ViPNet из ViPNet Центр управления сетью (см. Обновление, отправленное из ViPNet Центр управления сетью43).
- Обновление с помощью групповых политик. Обновления данного типа централизованно отправляются на сетевые узлы администратором сети ViPNet с помощью средств создания групповых политик Windows.
- Обновление вручную с помощью нового установочного файла (см. Обновление с помощью установочного файла).

Обновление, отправленное из ViPNet Центр управления сетью

Обновление ViPNet Client, отправленное из ViPNet Центр управления сетью, можно принять на сетевом узле с помощью программы ViPNet Система обновления (см. О программе ViPNet Система обновления). В зависимости от настроек, обновление принимается автоматически, либо вам необходимо принять его вручную (см. Установка обновлений вручную).

После обновления ViPNet Client перезагрузите компьютер.

Если новая версия программы не была установлена, воспользуйтесь рекомендациями из раздела Не применяется обновление ПО, отправленное из ViPNet ЦУС.

Обновление с помощью групповых политик

Администратор сети ViPNet может отправить на ваш сетевой узел обновление ViPNet Client в виде обновления групповых политик. Полученные таким образом обновления ViPNet Client устанавливаются автоматически и не требуют от вас каких-либо дополнительных действий.

Подробнее см. в разделе Установка ViPNet Client с помощью групповых политик.

Обновление с помощью установочного файла

Для обновления программы:

1. Запустите установочный файл  и дождитесь завершения проверки на совместимость вашего компьютера и программы ViPNet Client.
2. Чтобы после обновления ViPNet Client была автоматически выполнена перезагрузка компьютера, установите соответствующий флажок в окне **Обновление ViPNet Client**.

   Нажмите **Обновить**.
3. Если с некоторыми приложениями ViPNet не была завершена работа, может появиться сообщение о невозможности их обновления. Чтобы продолжить обновление, завершите работу с ними.
4. Если в процессе обновления появилось сообщение «Обнаружены проблемы совместимости», выполните предложенные рекомендации и продолжите установку программы.
5. После обновления перезагрузите компьютер, если перезагрузка не выполнилась автоматически.

Примечание. Если в вашей операционной системе включена функция быстрой загрузки Fast Startup, для завершения обновления ViPNet Client перезагрузите компьютер. Выключить и снова включить компьютер недостаточно.

Удалённое обновление ПО ViPNet Client

Если требуется обновить ПО ViPNet Client на удалённом компьютере, администратор сети ViPNet может выполнить обновление дистанционно, подключившись к удалённому компьютеру по протоколу RDP. Для дистанционной установки ViPNet Client с автоматической перезагрузкой удалённого компьютера:

1. С помощью стандартной программы Windows «Подключение к удалённому рабочему столу» установите защищённое подключение к удалённому компьютеру, на котором требуется обновить ПО ViPNet Client.

Внимание! На удалённом компьютере должно быть разрешено подключение к удалённому рабочему столу и настроен вход в систему без нажатия клавиш **Ctrl+Alt+Del**. Подробнее см. Настройка автоматического входа в Windows.

Для подключения на удалённом компьютере следует использовать учётную запись Windows, обладающую правами администратора и защищённую паролем.

2 В сеансе удалённой работы войдите в программу ViPNet Client в режиме администратора.

3 В меню **Сервис** выберите **Настройка параметров безопасности**.

Убедитесь, что в окне **Настройка параметров безопасности** на вкладке **Администратор** установлены флажки **Разрешить сохранение пароля в реестре** и **Автоматически входить в ViPNet** (см. Дополнительные настройки параметров безопасности).

4 В меню **Файл** выберите **Сменить пользователя**.

5 В окне входа введите пароль и установите флажок **Сохранить пароль**. Нажмите **OK**.

6 В сеансе удалённой работы выполните обновление ViPNet Client (см. Обновление с помощью установочного файла).

7 В процессе обновления ПО ViPNet Client в окне **Обновление ViPNet Client** установите флажок **Автоматически перезагрузить компьютер после обновления (при необходимости)**.

Иначе для завершения обновления нужно выполнить перезагрузку непосредственно на узле, на котором выполнялось обновление.

Внимание! В процессе обновления ПО ViPNet Client на удалённом компьютере соединение по протоколу RDP будет прервано.

Добавление, удаление и восстановление компонентов

При необходимости вы можете установить или удалить компоненты ViPNet Client, а также восстановить программу при обнаружении повреждений. Для этого:

1 В меню **Пуск** выберите **ViPNet** > **Настройка компонентов ViPNet Client** или запустите установочный файл .

2 В окне **Управление составом ViPNet Client** выберите нужное действие и нажмите **Далее**.

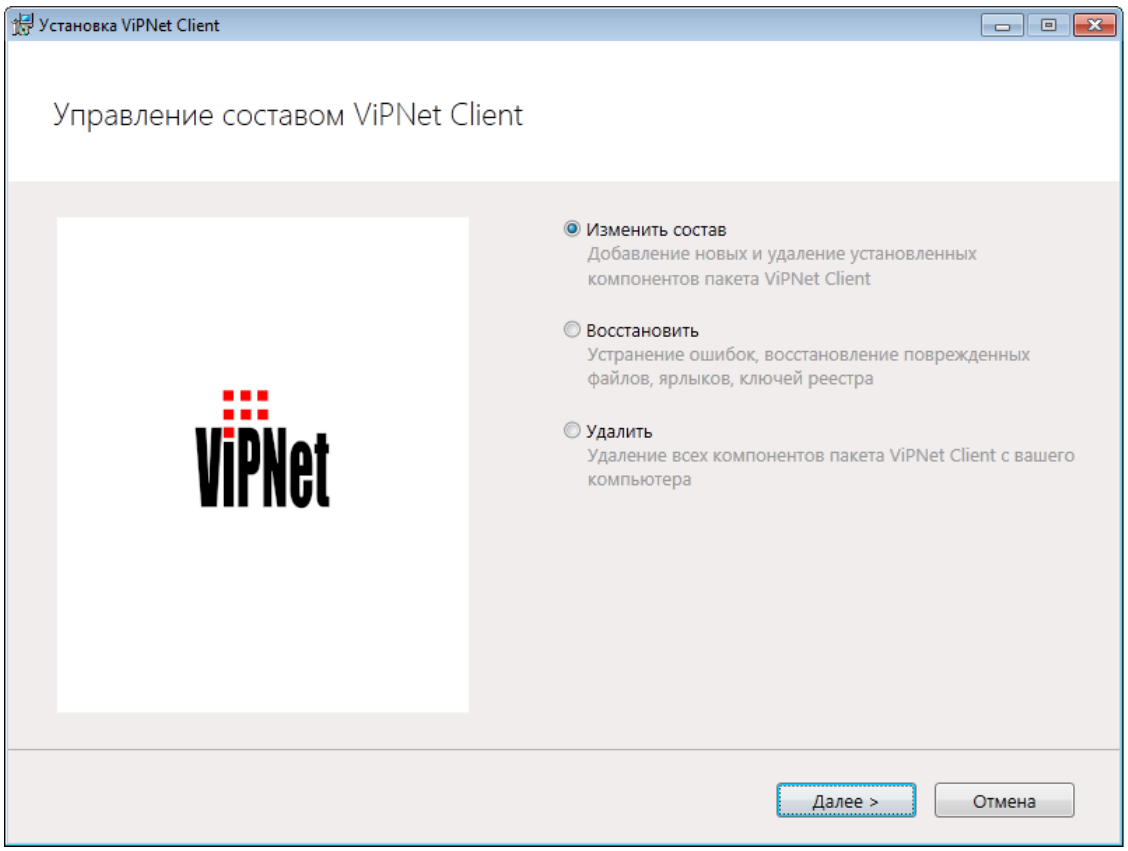


Рисунок 13. Изменение установленных компонентов

3 Если вы устанавливаете или удаляете компоненты программы, укажите нужные компоненты на странице выбора. Затем нажмите **Далее**.

Для автоматической перезагрузки после завершения изменений в ПО установите соответствующий флажок. Затем нажмите **Применить**.

4 Дождитесь завершения изменений в программе ViPNet Client.

Если вы не установили флажок автоматической перезагрузки, перезагрузите компьютер вручную, чтобы изменения вступили в силу.

Удаление ПО ViPNet Client

При удалении с компьютера программы ViPNet Client и всех её компонентов вы можете сохранить или удалить пользовательские данные, сформированные и используемые во время работы: справочники и ключи ViPNet, настройки параметров работы программы, письма программы ViPNet Деловая почта и другие.

Внимание! Начиная с версии 4.5, в программу ViPNet Client входит компонент ViPNet IDS HS. Если у вас установлена программа ViPNet IDS HS Агент, чтобы не нарушить ее работу не удаляйте ПО ViPNet Client.

1. В меню **Пуск** выберите **ViPNet > Настройка компонентов ViPNet Client**.
2. В окне **Управление составом ViPNet Client** выберите **Удалить** и нажмите **Далее**.
3. Чтобы удалить пользовательские данные, снимите флажок **Сохранить пользовательские данные**.
4. Для автоматической перезагрузки после удаления ПО установите соответствующий флажок.
5. Для продолжения нажмите **Удалить все компоненты**.

Примечание. Если при удалении ПО ViPNet Client вы также выбрали удаление пользовательских данных и при этом данные используются запущенными приложениями ViPNet, появится соответствующее предупреждение. В этом случае закройте все приложения ViPNet и нажмите **Повтор**.

6. Дождитесь удаления программного обеспечения.

   Если ранее вы выбрали автоматическую перезагрузку компьютера, то после завершения удаления ПО компьютер будет автоматически перезагружен. Иначе перезагрузите компьютер вручную, чтобы изменения вступили в силу.

Удаление в неинтерактивном режиме

Чтобы удалить программу ViPNet Client без отображения процесса на экране, в командной строке Windows выполните:

```
<путь к установочному файлу> -q -uninstall
```

При необходимости укажите дополнительные параметры:

- `-autorestart` — автоматически перезагрузить компьютер по завершении удаления;
- `-deleteuserdata="yes"` — удалить пользовательские данные.

Лицензирование программы ViPNet Client

Лицензия на вашу копию программы ViPNet Client может быть бессрочной или ограниченной по сроку действия. Информацию о сроке лицензии вы можете запросить у администратора вашей сети ViPNet. Также за 30 дней до истечения лицензии программа ViPNet Client начнёт отображать периодические оповещения.

Файл лицензии на использование вашей копии программы ViPNet Client устанавливается автоматически при установке дистрибутива ключей либо при получении обновления справочников и ключей.

Чтобы продлить срок действия лицензии, запросите обновление лицензии у администратора вашей сети. Порядок обновления лицензии может быть следующим:

- Если лицензия ещё не истекла, дождитесь поступления обновлений с новым файлом лицензии или установите дистрибутив ключей, переданный администратором.
- Если лицензия истекла, но программа сохранила ограниченную работоспособность, вы можете обновить лицензию одним из указанных выше способов.

  Программа сохраняет ограниченную работоспособность в течении 180 дней после истечения лицензии. При этом все функции программы заблокированы, но вы можете принять обновления справочников и ключей из ЦУСа. В строке заголовка ViPNet Client отображается надпись: «Защищённая сеть недоступна»/«Отправка писем недоступна».
- Если лицензия истекла и программа ViPNet Client не запускается. В этом случае вы можете обновить лицензию только с помощью установки нового дистрибутива ключей.

Внимание! Если вы обновили файл лицензии с помощью дистрибутива ключей, то после первого запуска программы ViPNet Client включите защиту трафика. Для этого в меню **Файл** выберите **Конфигурации** > **Включить защиту**.

Перенос сетевого узла на другой компьютер

Чтобы перенести узел сети ViPNet с одного компьютера на другой (например, при замене компьютера или после восстановления Windows), сохранив настройки и письма Деловой почты, потребуется вручную скопировать данные на новый компьютер. После переноса узла все данные прежнего узла надо будет удалить. В сети ViPNet не могут находиться два одинаковых узла.

Предварительные действия

- На прежнем компьютере:
  - Если версия ViPNet Client 4.3 или ниже — обновите до версии 4.5.x.

    После обновления авторизуйтесь в программе.
  - Расшифруйте все письма Деловой почты.

    См. «ViPNet Деловая почта 4. Руководство пользователя», раздел «Шифрование и расшифрование писем».
  - Убедитесь, что есть папка ключей пользователя `user_<AAAA>` (`AAAA` — идентификатор пользователя):

    `c:\Program Files (x86)\InfoTeCS\ViPNet Client\user_<AAAA>\`

    или `c:\ProgramData\InfoTeCS\ID_Узла\user_<AAAA>\`

    или в том расположении, которое вы указали при установке дистрибутива ключей.
  - Если пароль для аутентификации сохранён в системе, и вы его не помните, измените пароль.
- На новом компьютере:
  - Убедитесь, что разрядность Windows такая же, как и на прежнем.
  - Если развернут другой узел ViPNet, удалите ViPNet Client. В окне подтверждения снимите флажок **Сохранить пользовательские данные**.
  - Установите ту же версию ViPNet Client, которая установлена на прежнем компьютере, с тем же набором компонентов.
  - Если для аутентификации в ViPNet Client используется сертификат, установите в хранилище локального компьютера корневой сертификат, сертификаты из цепочки сертификации и CRL.

Перенос сетевого узла

1 На обоих компьютерах:
   - Завершите работу ViPNet Client и ViPNet Деловая почта.

- Запустите приложение Windows — **Службы** и остановите все службы ViPNet.

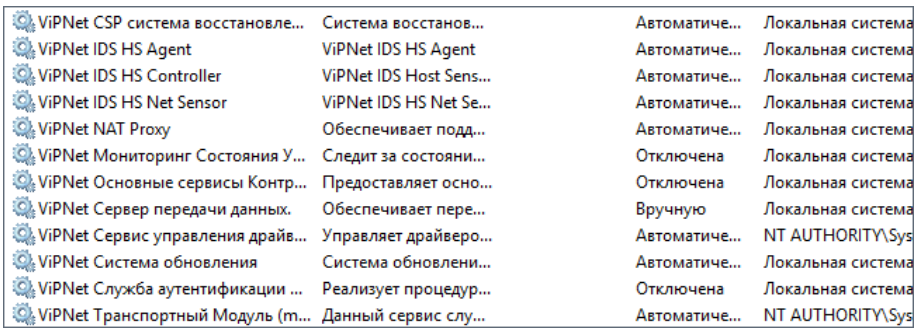


Рисунок 14. Службы ViPNet

Примечание. Некоторые службы автоматически перезапускаются после сбоя, поэтому могут помешать переносу. Для каждой из этих служб в свойствах выберите **Тип запуска** > **Отключена**:

- ViPNet NAT Proxy.
- ViPNet Мониторинг Состояния Узла.
- ViPNet Сервис управления драйвером защиты.
- ViPNet Система обновления.
- ViPNet Транспортный Модуль (mftp).

2 Перенесите указанные ниже файлы и папки с прежнего компьютера на новый. Копируйте в то же расположение с заменой всех файлов.

3 Скопируйте файлы из транспортного каталога. Для этого откройте файл `C:\ProgramData\InfoTeCS\ViPNet Client\shared.cfg` и найдите параметр `TransDir`:

- Если `TransDir=C:\ProgramData\InfoTeCS\ID_Узла`, скопируйте папку с номером узла (например, `0004011C`).
- Если `TransDir=C:\Program Files (x86)\InfoTeCS\ViPNet Client\`, скопируйте папки и файлы (у вас могут быть не все файлы):
  - `[d_station]`;
  - `[user_AAAA]`;
  - `AP*.*: APAXXXX.TXT, APCXXXX.TXT, APIXXXX.TXT, APLXXXX.TXT, APNXXXX.CRC, APNXXXX.CRG, APNXXXX.TXT, APSXXXX.TXT, APUXXXX.TXT,`

    (`XXXX` — идентификатор сетевого узла);
  - `nodeXXXX.*`;
  - `linkXXXX.txt`;
  - `afilter.hst`;
  - `[station]`;
  - `[key_disk]`;

- [databases], [config], [IPLogs];
- infotecs.re;
- iplir.cfg, iplirmain.cfg, AppWhere.cfg, postpone.cfg;
- ipliradr.do$;
- nodename.doc, extnet.doc, remote.doc, enet.doc;
- fldPPPP.txt, amatrix.dat, nmatrix.dat, sesalrt.hst, prevcrca.dat;
- данные модуля MFTP: [ARCHIVE], [CCC], [in], [out], [SMTPIN], [SMTPOUT], [TRASH], [local], [tmp], [invalid], [temp], mftp.ini, mftpconf.xml, mftpenv.db;
- из папки C:\ProgramData\InfoTeCS\ViPNet Client\ файлы и папки: [rf] (кроме файла rf.log), [$tmpdir$], [TaskDir] (если требуется сохранить файлы, принятые по файловому обмену);
- из папки C:\ProgramData\InfoTeCS\ViPNet Client\configparams\ файлы secserv.ini, rf.ini, iplir.cfg, iplirmain.cfg.

4 Из папки C:\ProgramData\InfoTeCS.Admin\ папки [ServicesPrivate] и [UpdateSystemData].

5 Если на прежнем компьютере вы настраивали ViPNet Client вручную:

- из папки C:\ProgramData\InfoTeCS\ViPNet Client\ все папки и файлы, кроме *.log.
- из папки C:\Users\<имя пользователя>\AppData\Local\InfoTeCS\ папки и файлы: [Rf], [ViPNet Client], foldertreenodes.txt, iplir.cfg.

6 Если вы используете Деловую почту:

- Из папки C:\ProgramData\InfoTeCS\ViPNet Business Mail\ скопируйте папку и файлы (у вас могут быть не все файлы):

Примечание. Если ранее у вас был установлен ViPNet Client версии 4.3 или ниже, скопируйте папку и файлы из C:\Program Files (x86)\InfoTeCS\ViPNet Client\

  - [MSArch] — папка по умолчанию для хранения архивов Деловой почты (либо другую папку, если вы изменили ее расположение);
  - wmail.crg;
  - wmail_admin.ini;
  - wmail.ini.
- Если настроены правила автопроцессинга, из папки C:\ProgramData\InfoTeCS\ID_Узла\ файл autoproc.dat (если требуется, дополнительно перенесите все папки и файлы правил автопроцессинга).

Примечание. Если ранее у вас был установлен ViPNet Client версии 4.3 или ниже, скопируйте файл из C:\Program Files (x86)\InfoTeCS\ViPNet Client\

- Из папки `C:\ProgramData\InfoTeCS\` папку с пользовательскими настройками адресной книги `[Address book]`.
- Если вы подключали дополнительные хранилища сообщений (см. «ViPNet Деловая почта 4. Руководство пользователя», раздел «Работа с архивами писем»), из каждого скопируйте папки архивов:
  - `[MS]`;
  - `[MS_дата_время]`;
  - `[дата_время]`.

7 Если вы используете сертификаты и храните контейнеры ключей на компьютере, то способ переноса зависит от того, в каком ПО вы создавали запрос и получали сертификат:

- В ПО ViPNet — перенесите контейнеры с помощью ViPNet Client (см. Перенос контейнера ключей) или ViPNet CSP («ViPNet CSP. Руководство пользователя», раздел «Перенос сертификатов и закрытых ключей между компьютерами»).
- В стороннем ПО и в стороннем УЦ — перенесите контейнеры с помощью стороннего ПО.

Запуск ViPNet Client на новом компьютере

1 Запустите все службы ViPNet, которые вы останавливали ранее.

Установите прежний тип запуска для служб, которые перезапускаются при сбое.

2 Запустите ViPNet Client, в окне аутентификации нажмите **Настройка** > **Папка ключей пользователя** и укажите путь, заданный в параметре `TransDir`.

3 Если на прежнем компьютере вы изменяли настройки запуска ViPNet Client, задайте те же настройки на новом.

4 Удалите на прежнем компьютере все данные, которые вы перенесли на новый компьютер.

5 Если вы копировали контейнеры с ключами сертификатов на новый компьютер, удалите их на прежнем.

См. «ViPNet CSP. Руководство пользователя», раздел «Удаление контейнера ключей» или документацию к стороннему ПО.

6 В целях безопасности измените пароль для аутентификации.

2

Установка и обновление справочников и ключей

Установка справочников и ключей

Установка справочников и ключей выполняется при развёртывании ПО ViPNet или при добавлении новых пользователей на сетевой узел, а также когда справочники и ключи устарели или были повреждены.

Для установки ключей выберите один из вариантов:

- Первая установка справочников и ключей одного пользователя.
- Установка справочников и ключей для нескольких пользователей.
- Чтобы задать папки, в которых будут храниться справочники и ключи, см. раздел Расширенный режим установки справочников и ключей.
- Если на узле уже установлены справочники и ключи для какой-либо программы ViPNet, см. раздел Использование справочников и ключей, установленных ранее.
- Чтобы установить справочники и ключи из командной строки Windows, см. раздел Установка справочников и ключей в неинтерактивном режиме.
- Если вы не можете войти в программу, см. раздел Повторная установка справочников и ключей после сбоя программы.

Внимание! Не устанавливайте на один компьютер ключи, предназначенные для разных сетевых узлов, это может нарушить работу программ ViPNet.

Каждому пользователю передаётся резервный набор персональных ключей (РНПК). Файл РНПК имеет вид `AAAA.pk` (где `AAAA` — идентификатор пользователя в сети ViPNet). Во время установки справочников и ключей он помещается в папку ключей пользователя.

Добавление РНПК в дистрибутив ключей зависит от версии ViPNet Administrator:

- в версии 4.6 и ниже РНПК добавляется только в первый дистрибутив.
- в версии 4.6.1 и выше РНПК добавляется в каждый дистрибутив.

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

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

Установка справочников и ключей одного пользователя

Для установки справочников и ключей:

1. Получите у администратора дистрибутив ключей (файл `*.dst` или `*.enc`).
2. Завершите работу всех компонентов программы ViPNet Client.
3. Запустите программу установки ключей сети ViPNet одним из способов:
   - Дважды щёлкните файл дистрибутива ключей (для `*.dst`).
   - Запустите ViPNet Client, в окне ввода пароля щёлкните значок  справа от кнопки **Настройка** и выберите **Установить ключи**.

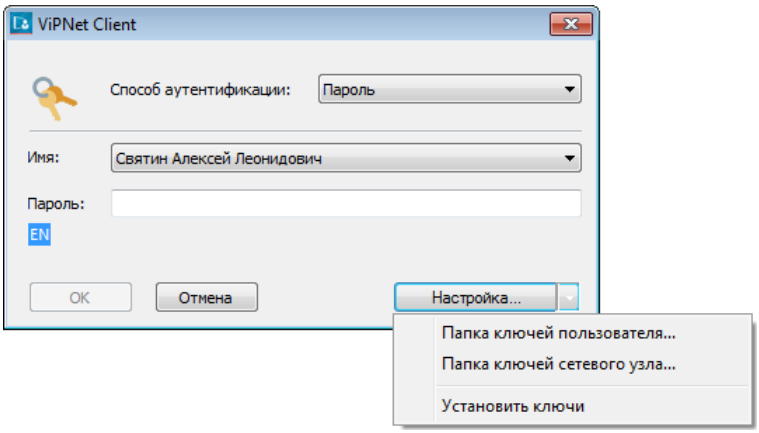


Рисунок 15. Запуск программы установки ключей

4. Если появится сообщение о завершении работы программ ViPNet, закройте указанные программы и нажмите **Повтор**.
5. На странице **Укажите файл дистрибутива ключей** задайте путь, если он не указан.
6. Убедитесь, что выбран дистрибутив ключей для вашего сетевого узла. Имя сетевого узла и имя пользователя отображаются ниже поля для указания пути к файлу дистрибутива.

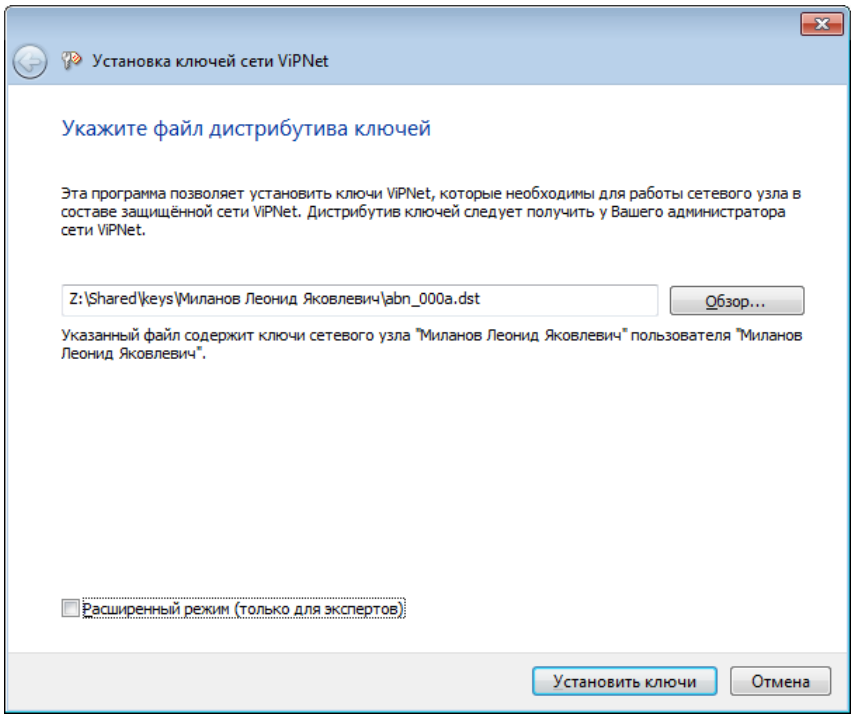


Рисунок 16. Выбор файла дистрибутива ключей

По умолчанию справочники и ключи устанавливаются в одну папку `C:\ProgramData\Infotecs\ID_Узла\`, вы можете её изменить (см. Расширенный режим установки справочников и ключей).

7 Нажмите **Установить ключи**.

8 Если установка ключей прошла успешно, появится соответствующее сообщение.

Если выполнить установку ключей не удалось, обратитесь к администратору сети ViPNet.

Примечание. Если при установке ключей будут найдены ранее установленные ключи для этого узла, новые ключи будут установлены в ту же папку поверх предыдущих.

После успешной установки ключей можно запустить ViPNet Client.

Внимание! Если в программе ViPNet уже были зарегистрированы другие пользователи, то перед первым входом в программу:

1 Войдите в программу ViPNet, используя данные для аутентификации уже зарегистрированного пользователя.

2 Дождитесь принятия обновлений на узле. Как правило, это занимает 5-30 минут.

3 Завершите работу с программой и войдите снова, используя данные для аутентификации нового пользователя.

Установка справочников и ключей для нескольких пользователей

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

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

Примечание. Справочники и ключи нескольких пользователей из разных сетей ViPNet не могут быть установлены на одном компьютере.

Для установки справочников и ключей нескольких пользователей на одном компьютере:

1. Для каждого нового пользователя получите дистрибутив ключей у администратора сети ViPNet.
2. Установите справочники и ключи для одного пользователя (см. Установка справочников и ключей одного пользователя).
3. Войдите в программу ViPNet (см. Запуск программы), используя данные для аутентификации этого пользователя.
4. Установите справочники и ключи для следующего пользователя.
   - **4.1** Войдите в программу ViPNet, используя данные для аутентификации первого пользователя. Дождитесь принятия обновлений на узле. Как правило, это занимает 5-30 минут.
   - **4.2** Завершите работу с программой и войдите снова, используя данные для аутентификации второго пользователя.
5. При необходимости повторите шаги 2-4 для установки справочников и ключей для других пользователей.

В результате в окне входа в программу (см. Запуск программы) в списке учётных записей будут отображаться пользователи, для которых вы установили справочники и ключи.

Расширенный режим установки справочников и ключей

По умолчанию справочники и ключи устанавливаются в `C:\ProgramData\InfoTeCS\ID_Узла`. Расширенный режим установки позволяет вам самостоятельно задать папки для установки справочников и ключей. Такая необходимость может возникнуть, если:

- из соображений безопасности вы хотите хранить справочники и ключи на специальном съёмном носителе;

- у вас нет прав на изменение и запись файлов в папке установки справочников и ключей. По умолчанию: `C:\ProgramData\InfoTeCS\ID_Узла`.

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

- В папках не должны находиться справочники и ключи другой программы ViPNet.
- У вас должно быть право на изменение и запись файлов в данных папках.
- Информационная защита папок должна отвечать требованиям безопасности вашей организации.
- Программа ViPNet Client должна иметь постоянный доступ к данным папкам.

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

Для установки ключей в расширенном режиме:

1. Получите новый дистрибутив ключей у администратора сети ViPNet.
2. Следуйте указаниям раздела Установка справочников и ключей одного пользователя.

   На странице указания файла дистрибутива ключей установите флажок **Расширенный режим (только для экспертов)**.
3. На следующей странице мастера укажите:
   - **Папку ключей сетевого узла**.
   - **Папку ключей пользователя**.

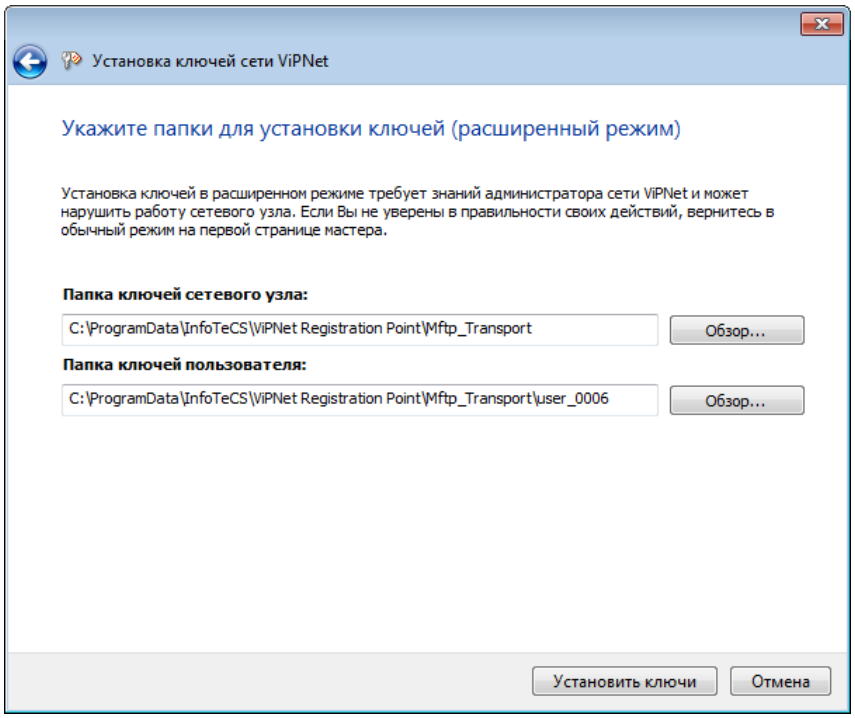


Рисунок 17. Указание папок для установки ключей узла и ключей пользователя в расширенном режиме

4 Нажмите **Установить ключи**.

Если установка ключей прошла успешно, будет выведено соответствующее сообщение. Если выполнить установку ключей не удалось, обратитесь к администратору сети ViPNet.

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

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

Установка справочников и ключей в неинтерактивном режиме

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

Использование неинтерактивного режима позволяет вам выполнять удалённую установку справочников и ключей или создавать программы, которые обращаются к командной строке

Windows и запускают автоматическую установку справочников и ключей с заданными параметрами.

Например, вы можете создать сценарий входа в систему (logon script), который запустит автоматическую установку справочников и ключей после загрузки системы. Информацию о создании сценариев входа в систему можно найти на сайте компании Microsoft. При установке справочников и ключей может потребоваться подтверждение в окне контроля учётных записей пользователей Windows.

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

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

Например:

```
"C:\Program Files (x86)\InfoTeCS\ViPNet Client\keysetup" <файл *.dst> /td "C:\ProgramData\InfoTeCS\ID_Узла" /term /check
```

Внимание! Установить таким образом можно только дистрибутивы с расширением `*.dst`. Установка зашифрованных дистрибутивов `*.enc` не поддерживается.

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

После успешного выполнения данной команды можно запустить ViPNet Client.

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

```
<путь к файлу keysetup> /?
```

Повторная установка справочников и ключей после сбоя программы

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

Внимание! Не рекомендуется проводить повторную установку справочников и ключей без особой необходимости, поскольку в этом случае не гарантируется сохранность пользовательских данных, сформированных компонентами ПО ViPNet Client (например, писем программы ViPNet Деловая почта).

Если с момента установки ключей до момента сбоя были изменены мастер-ключи в сети ViPNet или ключи были скомпрометированы, при повторной установке ключей будет потерян доступ к зашифрованным письмам программы ViPNet Деловая почта (в том числе в архивах), защищённым сообщениям и другим пользовательским данным, сформированным компонентами ViPNet Client.

Если перечисленных выше событий не происходило, то повторная установка ключей будет выполнена как обновление справочников и ключей с помощью дистрибутива ключей, и пользовательские данные сохранятся.

Для повторной установки справочников и ключей на сетевом узле:

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

Обновление справочников, ключей и политик безопасности

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

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

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

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

Приём централизованных обновлений

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

Обновления справочников, ключей и политик безопасности можно принять на сетевом узле с помощью системы обновления ViPNet. В зависимости от её настроек, обновления могут быть приняты на узле автоматически сразу после получения, либо это потребуется выполнить вручную.

Некорректные обновления не применяются. Клиент блокирует подозрительные конверты и отправляет информацию об этом на узел с ViPNet ЦУС. Вы можете посмотреть эту информацию в журнале клиента, установленного на компьютере с ViPNet ЦУС:

1. В ViPNet Client выберите **Приложения > ViPNet Транспортный модуль**.
2. На вкладке **Конверты** найдите конверты с именем `!*.ctl`.

Также информация отображается в журнале `mftpenv.log` в транспортном каталоге (по умолчанию `C:\ProgramData\InfoTeCS\ID_Узла`).

Обновление справочников и ключей с помощью дистрибутива ключей

Если по каким-либо причинам обновление справочников и ключей не может быть принято по сети (см. Обновление справочников, ключей и политик безопасности), вы можете выполнить обновление вручную с помощью дистрибутива ключей.

Примечание. Политики безопасности, включённые в дистрибутив, будут установлены, если на узле нет политик:

- установленных при первичной инициализации;
- полученных из программы ViPNet Policy Manager.

Для обновления ключей с помощью дистрибутива:

1. Получите новый дистрибутив ключей у администратора сети ViPNet.

   Следуйте указаниям раздела Установка справочников и ключей одного пользователя с использованием нового дистрибутива.

   При указании дистрибутива ключей автоматически проверяется соответствие между установленными ранее ключами и новыми ключами, которые находятся в указанном файле дистрибутива ключей (например, что ключи сформированы с помощью одного и того же мастер-ключа).

   При установке ключей в расширенном режиме (см. Расширенный режим установки справочников и ключей) дополнительно проверяется, предназначены ли данные ключи для одного и того же сетевого узла.

2. Завершите установку согласно указаниям раздела Установка справочников и ключей одного пользователя.

После успешного обновления ключей можно запустить ПО ViPNet.

Удаление справочников и ключей

Удаление справочников и ключей может потребоваться при передаче компьютера на техническое обслуживание или при переносе сетевого узла на другой компьютер.

Внимание! Если на компьютере работает несколько пользователей ViPNet, то будут удалены ключи и справочники всех пользователей. Удалить ключи только одного пользователя невозможно.

1. Завершите работу с программой.
2. В командной строке Windows перейдите в папку программы ViPNet и выполните:

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

   По умолчанию ключи и справочники находятся в папке `C:\ProgramData\Infotecs\ID_Узла\`.

Например:

```
"C:\Program Files (x86)\InfoTeCS\ViPNet Client\keysetup" /clean /td
"C:\ProgramData\InfoTeCS\2A15000D0"
```

В результате из папки `\2A15000D0` будут удалены ключи и справочники всех пользователей.

Действия при компрометации ключей

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

Различают явную и неявную компрометацию ключей:

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

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

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

К событиям, требующим проведения расследования и принятия решения о факте компрометации, также относится возникновение подозрений в утечке информации или её 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, управляемой с помощью ПО ViPNet Administrator, на случай компрометации ключей пользователя предусмотрена возможность дистанционного обновления ключей с помощью резервного набора персональных ключей (РНПК). Файл резервного набора (`AAAA.pk`, где AAAA — идентификатор пользователя в сети ViPNet) входит в состав первоначального дистрибутива ключей и при установке справочников и ключей помещается в папку ключей пользователя (см. Установка справочников и ключей).

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

3

Начало работы с ПО ViPNet Client

Запуск программы

ViPNet-драйвер активирует фильтрацию трафика во время загрузки Windows ещё до аутентификации в программе ViPNet Client. При этом работа ViPNet-драйвера определяется предустановленными фильтрами защищённой сети и фильтрами открытой сети, которые использовались в предыдущем сеансе работы. Полную защиту трафика, включающую его шифрование, ViPNet-драйвер обеспечивает после аутентификации в программе ViPNet Client.

До входа в Windows появится окно входа в программу ViPNet Client. Для запуска программы введите пароль или подключите внешнее устройство аутентификации (см. Способы аутентификации пользователя).

Примечание. Для аутентификации в ViPNet Client во время загрузки Windows, вы можете использовать экранную клавиатуру. Для этого нажмите **Win+U** > **Экранная клавиатура**.

Чтобы отказаться от запуска программы ViPNet Client, нажмите **Отмена**, в этом случае защита трафика будет отключена.

Внимание! В зависимости от уровня полномочий пользователя, который определяется в ViPNet Центр управления сетью (см. Работа в условиях ограниченных полномочий), возможность отказа от запуска ViPNet Client и отключения шифрования трафика может быть недоступна. Загрузка Windows не будет завершена, пока вы не выполните вход в программу ViPNet.

Если вы забыли пароль входа в программу или внешнее устройство аутентификации повреждено, обратитесь к администратору сети ViPNet за дистрибутивом ключей, загрузите операционную систему Windows в безопасном режиме и повторно установите ключи пользователя (см. Установка справочников и ключей).

Если вы вышли из программы или отказались от аутентификации при загрузке Windows, то для запуска ViPNet Client:

1 В меню **Пуск** начните вводить «ViPNet Client» и запустите программу. Откроется окно входа в программу.

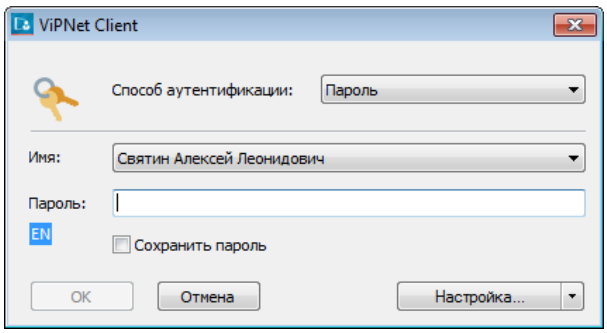


Рисунок 18. Окно входа в программу

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

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

3 Нажмите **OK**. Откроется окно программы ViPNet Client (см. Интерфейс программы ViPNet Client).

Способы аутентификации пользователя

В программе ViPNet Client предусмотрено три способа аутентификации:

- Пароль. Для входа в программу вам следует ввести свой пароль. Каждый раз после ввода пароля вычисляется парольный ключ, который используется для доступа к вашему персональному ключу.
- Устройство. Для входа в программу вам следует подключить устройство и ввести ПИН-код (и в некоторых случаях пароль).
- Пароль на устройстве. Для входа в программу вам следует подключить устройство и ввести ПИН-код. Способ не доступен в УКЦ версии 4.6.1 и выше.

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

Внимание! Способ аутентификации **Пароль на устройстве** не отвечает требованиям безопасности и используется для совместимости с программным обеспечением ViPNet ранних версий. Если вы используете данный способ аутентификации, измените его на **Пароль** или **Устройство**.

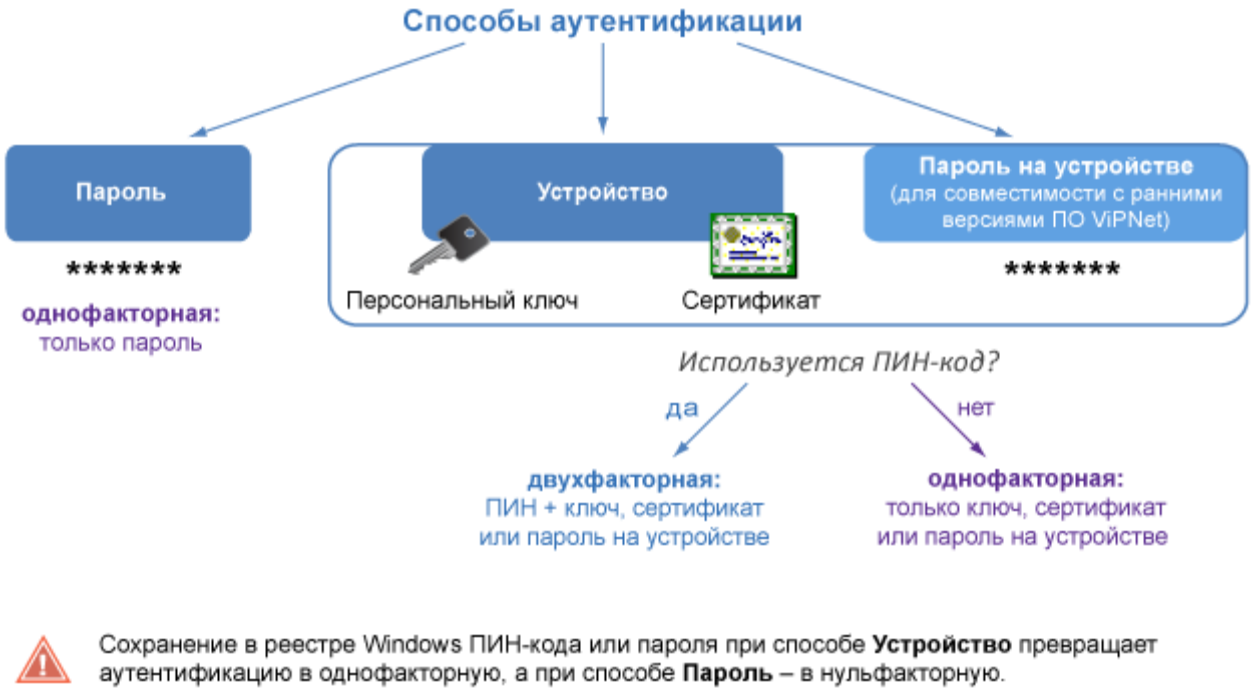
По умолчанию установлен способ аутентификации **Пароль**. Изменить способ аутентификации можно при входе в программу. Кроме того, способ аутентификации удалённо может изменить администратор сети ViPNet, отправив на ваш узел политику безопасности из программы ViPNet Policy Manager.

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

Внимание! Если при использовании способов аутентификации **Пароль на устройстве** или **Устройство** внешнее устройство будет отключено, может произойти автоматическая блокировка компьютера — в соответствии с настройками, заданными в режиме администратора (см. Параметры защиты трафика).

Уровень безопасности при входе в программу определяется количеством факторов аутентификации. Чем оно больше, тем выше уровень безопасности. Нульфакторная аутентификация не обеспечивает безопасный вход в программу и не рекомендуется к использованию.

На схеме ниже представлены возможные способы аутентификации и их факторность.



Сохранение в реестре Windows ПИН-кода или пароля при способе **Устройство** превращает аутентификацию в однофакторную, а при способе **Пароль** – в нульфакторную.

Рисунок 19. Схема соответствия между факторами и способами аутентификации

Пароль

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

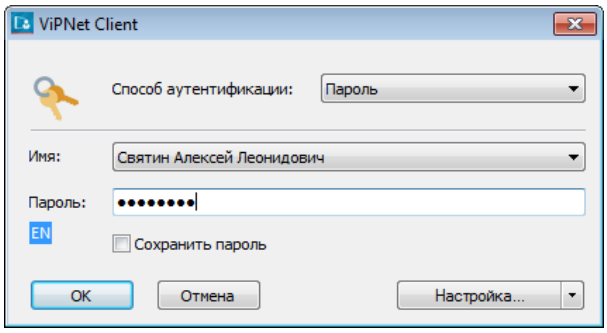


Рисунок 20. Способ аутентификации «Пароль»

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

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

---

3 В поле **Пароль** введите пароль.

Если сохранение пароля в реестре разрешено настройками программы, для сохранения пароля можно установить соответствующий флажок.

4 Нажмите **OK**.

Устройство

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

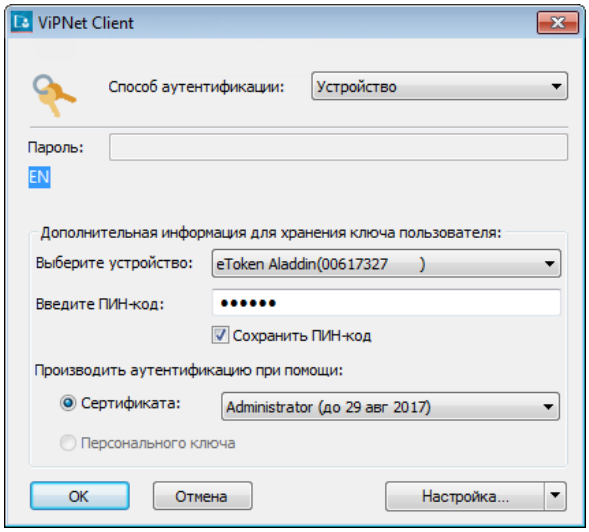


Рисунок 21. Способ аутентификации «Устройство»

2 Подключите внешнее устройство.

3 Если требуется, в списке ниже выберите ваше имя пользователя и в поле **Пароль** введите свой пароль. Необходимость ввода пароля зависит от типа используемого внешнего устройства.

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

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

Внимание! При использовании устройства JaCarta PKI/ГОСТ во избежание ошибок не следует сохранять ПИН-коды этого устройства.

Если сохранение ПИН-кода недоступно, значит эта настройка запрещена администратором вашей сети ViPNet.

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

- **Сертификата** — для аутентификации с помощью сертификата, который хранится на вашем устройстве. В списке сертификатов, обнаруженных на устройстве, выберите нужный сертификат.

  Требования, предъявляемые к сертификатам для аутентификации, представлены в разделе Особенности аутентификации с помощью сертификата. В случае возникновения затруднений см. раздел Не удаётся выполнить аутентификацию с помощью сертификата.

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

7 Нажмите **OK**.

Особенности аутентификации с помощью сертификата

Для аутентификации в программе ViPNet Client с помощью сертификата должны быть выполнены условия:

- Установлен компонент **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.

  Чтобы проверить или установить этот компонент, выберите **Пуск** > **Настройка компонентов ViPNet Client**. Затем в окне установки выберите **Изменить состав** и раскройте список компонентов ViPNet CSP.

Примечание. При создании закрытого ключа рекомендуется использовать криптопровайдер ViPNet CSP.

- Внешнее устройство поддерживает стандарт PKCS#11.
- Аутентификация с помощью сертификата ГОСТ выполняется с помощью устройства, на котором реализована аппаратная поддержка алгоритмов ГОСТ (см. Алгоритмы и функции, поддерживаемые внешними устройствами).

Примечание. Устройства JaCarta-2 поддерживают аутентификацию с помощью сертификата, если на них установлен апплет ГОСТ версии 2.55 и выше, а на компьютере используется ПО «Единый Клиент JaCarta» версии 2.12 и выше.

Узнать версию апплета вы можете в ПО «Единый Клиент JaCarta». Для этого перейдите в режим администратора и в разделе **Информация о токене** щёлкните ссылку **Подробная информация**.

- Если вы используете криптопровайдер по умолчанию, то выберите **Пуск** > **ViPNet CSP** и в разделе **Дополнительно** установите флажок **Поддержка работы ViPNet CSP через Microsoft CryptoAPI**.
- Если вы используете сторонний криптопровайдер, см. «ViPNet CSP 4.4. Руководство пользователя», раздел «Совместимость с ПО других производителей».
- Сертификат имеет назначение «Шифрование ключей» в поле **Использование ключа**.

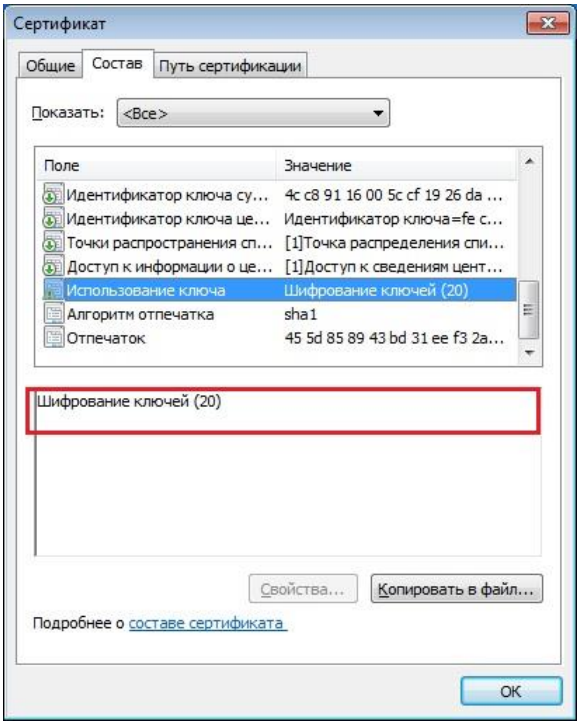


Рисунок 22. Проверка наличия назначения «Шифрование ключей» в сертификате для аутентификации

- В контейнере на устройстве находится закрытый ключ, которому соответствует используемый сертификат.

- Сертификат действителен: срок его действия не истёк, он не находится в списке аннулированных сертификатов, соответствующая ему цепочка сертификации полна, и все входящие в неё сертификаты также действительны.
- В хранилище локального компьютера и в хранилище пользователя установлены корневой сертификат и все сертификаты из цепочки сертификации, включая соответствующий список аннулированных сертификатов.

Чтобы получить сертификат ГОСТ, подходящий для аутентификации в ПО ViPNet Client:

1 Создайте запрос на сертификат. При этом убедитесь, что в поле **Использование ключа** установлено назначение «Шифрование ключей».

Примечание. Для создания запроса на сертификат рекомендуется использовать криптопровайдер ViPNet CSP.

---

2 Выпустите сертификат в удостоверяющем центре или обратитесь к администратору.

3 Установите изданный сертификат в контейнер ключей на устройстве.

4 Установите сертификаты и список аннулированных сертификатов в хранилище локального компьютера и в хранилище пользователя.

5 После установки сертификатов в хранилище перезапустите ViPNet Client.

Смена пользователя

Если на сетевом узле зарегистрировано несколько пользователей, сменить пользователя можно, не выходя из программы ViPNet Client:

1 Выберите **Файл** > **Сменить пользователя**. Откроется окно входа в программу.

2 Выберите способ аутентификации для входа в программу и в зависимости от выбранного способа введите пароль пользователя либо подключите внешнее устройство и введите ПИН-код.

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

Примечание. На сетевом узле должны быть предварительно установлены ключи пользователя, от имени которого выполняется вход в программу.

---

3 Нажмите **ОК**.

Завершение работы с программой

Чтобы свернуть окно программы, выполните одно из действий:

- Нажмите **Закрыть**  в правом верхнем углу окна.
- Нажмите сочетание клавиш **Alt+F4**.

Чтобы снова развернуть окно программы, щёлкните значок  в области уведомлений.

Чтобы выйти из программы, выберите меню **Файл** > **Выход** либо в области уведомлений в контекстном меню программы ViPNet Client выберите **Выход**.

Примечание. После выхода из программы ViPNet Client работа ViPNet-драйвера продолжается: он выполняет фильтрацию IP-трафика в соответствии с настройками интегрированного сетевого экрана.

Интерфейс ViPNet Client

Окно программы ViPNet Client представлено на рисунке.

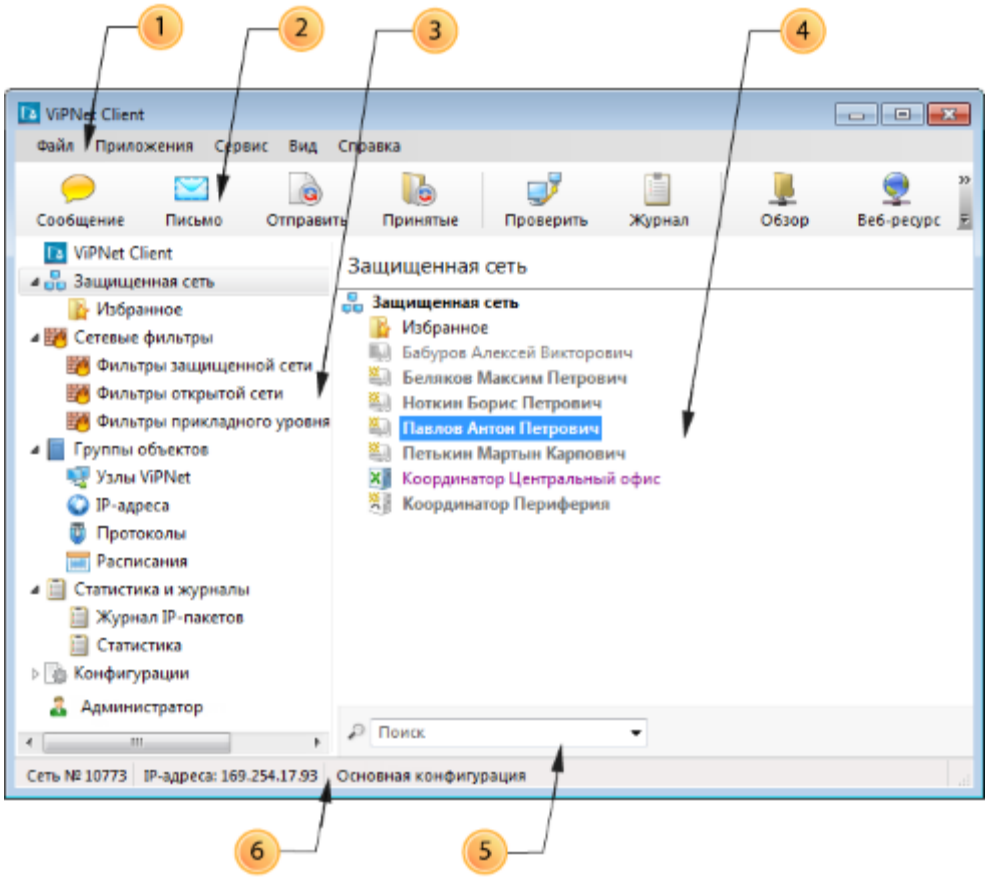


Рисунок 23. Окно программы ViPNet Client

Цифрами на рисунке обозначены:

1 Главное меню программы.

2 Панель инструментов. Чтобы отобразить или скрыть панель инструментов, в меню **Вид** выберите **Панель инструментов**. Добавить или удалить кнопки на панель инструментов вы можете с помощью кнопки  .

3 Панель навигации. Содержит перечень разделов, предназначенных для настройки различных параметров ViPNet Client:

- **Защищённая сеть** (этот раздел выбран по умолчанию) — содержит список сетевых узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью. Подробнее см. Работа со списком защищённых узлов ViPNet.

- **Сетевые фильтры**. Содержит подразделы с фильтрами IP-трафика:

- **Фильтры защищённой сети** — предназначен для настройки фильтров защищённого трафика (см. Создание фильтров для защищённой сети).
- **Фильтры открытой сети** — предназначен для настройки фильтров открытого трафика (см. Создание фильтров для открытой сети).
- **Фильтры прикладного уровня открытой сети** (доступно, если установлен модуль расширенной фильтрации) — предназначен для настройки фильтров прикладного уровня.

- **Группы объектов —** содержит списки объектов, которые могут быть использованы при создании сетевых фильтров: группы узлов ViPNet, группы IP-адресов и так далее (см. Использование групп объектов).
- **Статистика и журналы**. Содержит подразделы:
  - **Журнал IP-пакетов —** предназначен для поиска записей в журнале IP-пакетов (см. Работа с журналом IP-пакетов).
  - **Статистика —** предназначен для просмотра статистики фильтрации IP-пакетов (см. Просмотр статистики фильтрации IP-пакетов).
- **Конфигурации** — предназначен для управления конфигурациями программы ViPNet Client (см. Управление конфигурациями программы).
- **Администратор** — отображается только после входа в программу в режиме администратора и служит для настройки дополнительных параметров программы.

Примечание. Количество и порядок расположения разделов на панели навигации зависит от уровня полномочий пользователя, который определяется в ViPNet Центр управления сетью (см. Работа в условиях ограниченных полномочий).

---

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

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

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

- Имя узла (отображается в разделе **Защищённая сеть** и в окне **Свойства узла** на вкладке **Общие**).
- Имя компьютера (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**).

6 Строка состояния. Содержит следующие сведения: номер сети ViPNet, IP-адреса, назначенные узлу, и текущая конфигурация программы. При изменении сетевых фильтров или групп

объектов вместо указанных сведений в строке состояния появляется сообщение о том, что фильтры или группы объектов были изменены, но не применены.

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

Работа со списком защищённых узлов

Раздел **Защищённая сеть** (см. Интерфейс программы ViPNet Client) содержит список защищённых узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью.

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

Таблица 1. Обозначение статуса сетевых узлов

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

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

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

- Чтобы создать новую папку, в контекстном меню раздела **Защищённая сеть** выберите **Создать папку**.
- Чтобы перенести сетевые узлы в какую-либо папку, в разделе **Защищённая сеть** выберите один или несколько сетевых узлов и перетащите их в нужную папку.

- Чтобы переименовать папку, щёлкните её правой кнопкой мыши и в контекстном меню выберите **Переименовать**.
- Чтобы удалить папки:
    - Убедитесь, что папки, которые требуется удалить, не содержат сетевых узлов. В противном случае перенесите сетевые узлы в другие папки.
    - Выберите одну или несколько папок на панели навигации или в разделе **Защищённая сеть**.
    - Нажмите клавишу **Delete** либо воспользуйтесь пунктом **Удалить** в контекстном меню.

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

Для просмотра свойств сетевого узла дважды щёлкните имя узла. Откроется окно **Свойства узла**, в котором приведены общие сведения о сетевом узле и содержатся параметры доступа к узлу.

Чтобы проверить соединение с другим узлом, начать сеанс обмена защищёнными сообщениями, отправить файл или использовать другие встроенные функции программы ViPNet Client (см. Встроенные средства коммуникации), выполните одно из действий:

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

Работа в условиях ограниченных полномочий

Возможности использования программы ViPNet Client и изменения её параметров на узлах сетей ViPNet, управляемых с помощью программы ViPNet Administrator, могут быть ограничены уровнем полномочий пользователя. Кроме этого, интерфейс программы ViPNet Client может быть ограничен в режиме администратора сетевого узла (см. Работа в программе в режиме администратора).

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

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

Информация о полномочиях пользователя содержится в документе «Классификация полномочий. Приложение к документации ViPNet».

4

Система обновления ViPNet

О программе ViPNet Система обновления

ViPNet Система обновления обеспечивает получение и установку обновлений следующих типов:

- обновления ViPNet Client, полученные из программы ViPNet Administrator;
- обновления справочников и ключей, полученные из программы ViPNet Administrator;
- обновления политик безопасности (а также настройки по смене типа аутентификации и разрешении сохранения ПИН-кода), полученные из программы ViPNet Policy Manager.

Установка обновлений может осуществляться как в автоматическом режиме (см. Автоматическая установка обновлений), так и вручную (см. Установка обновлений вручную83).

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

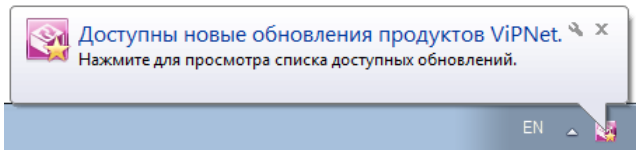


Рисунок 24. Отображение наличия обновлений в области уведомлений

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

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

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

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

Автоматическая установка обновлений

Чтобы обновления устанавливались на узле автоматически:

1. В меню **Пуск** выберите **Все программы** > **ViPNet** и запустите **ViPNet Система обновления** от имени администратора.
2. В открывшемся окне на вкладке **Параметры** установите флажок **Устанавливать обновления автоматически**.
3. Чтобы после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.
4. Нажмите **OK**.

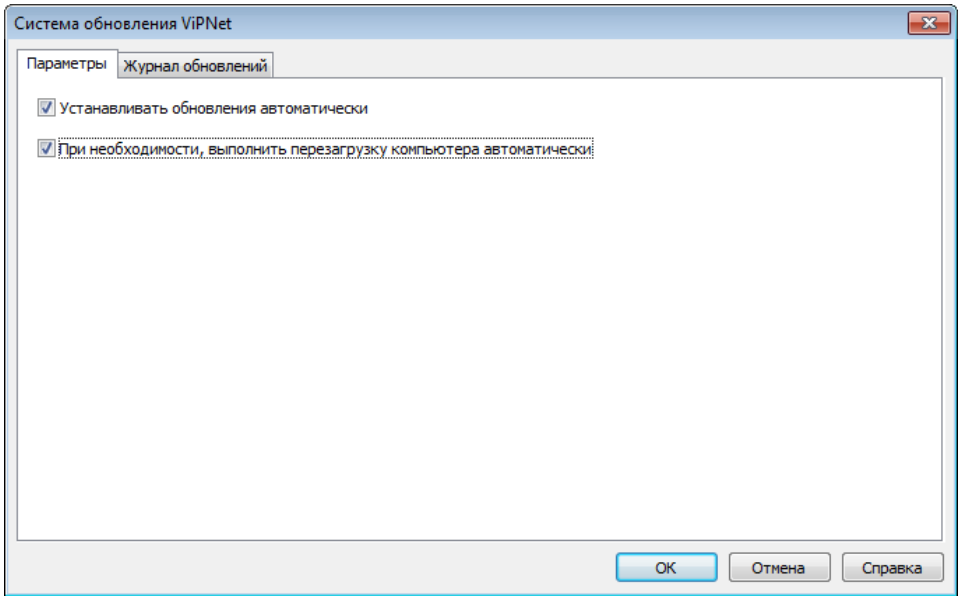


Рисунок 25. Настройка автоматической установки обновлений

Теперь, при поступлении обновлений появится сообщение об обновлении программы ViPNet. Программа автоматически закрывается, и начинается обновление.

Если после обновления требуется перезагрузка, то в зависимости от настроек, перезагрузка произойдёт автоматически или информация об этом появится в области уведомлений.

Установка обновлений вручную

Чтобы контролировать установку обновлений на сетевом узле, отключите автоматическую установку:

1 В меню **Пуск** выберите **Все программы** > **ViPNet** и запустите **ViPNet Система обновления** от имени администратора.

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

3 Чтобы после обновления перезагрузка выполнялась автоматически, установите соответствующий флажок.

4 Нажмите **ОК**.

Теперь проверять и устанавливать обновления можно вручную:

1 В области уведомлений щёлкните значок **ViPNet Система обновления** правой кнопкой мыши и в контекстном меню выберите **Доступные обновления**.

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

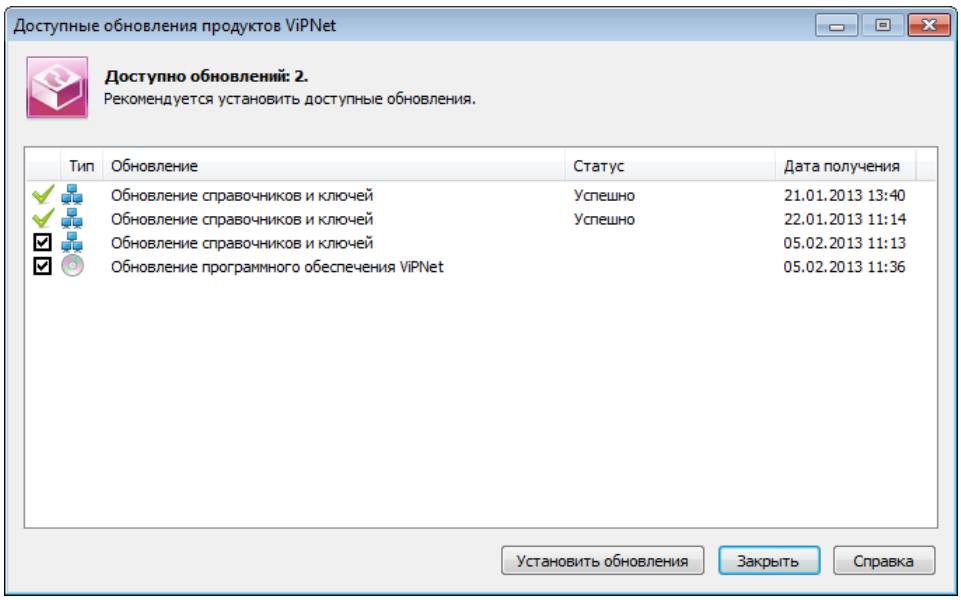


Рисунок 26. Просмотр полученных обновлений

3 Нажмите **Установить обновления**.

4 Если появилось сообщение, что есть работающие программы ViPNet, нажмите **Продолжить**. При этом программы ViPNet будут закрыты.

При обновлении в области уведомлений отображается соответствующая информация.

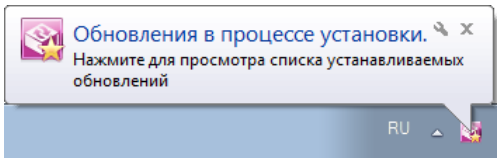


Рисунок 27. Отображение установки обновлений в области уведомлений

5 Если после обновления необходимо выполнить перезагрузку, информация об этом появится в области уведомлений.

Внимание! Обновление ПО может занять значительное время. Не прерывайте процесс обновления и не выполняйте перезагрузку компьютера до окончания процесса обновления.

Просмотр журнала установленных обновлений

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

2 В появившемся окне выберите вкладку **Журнал обновлений**.

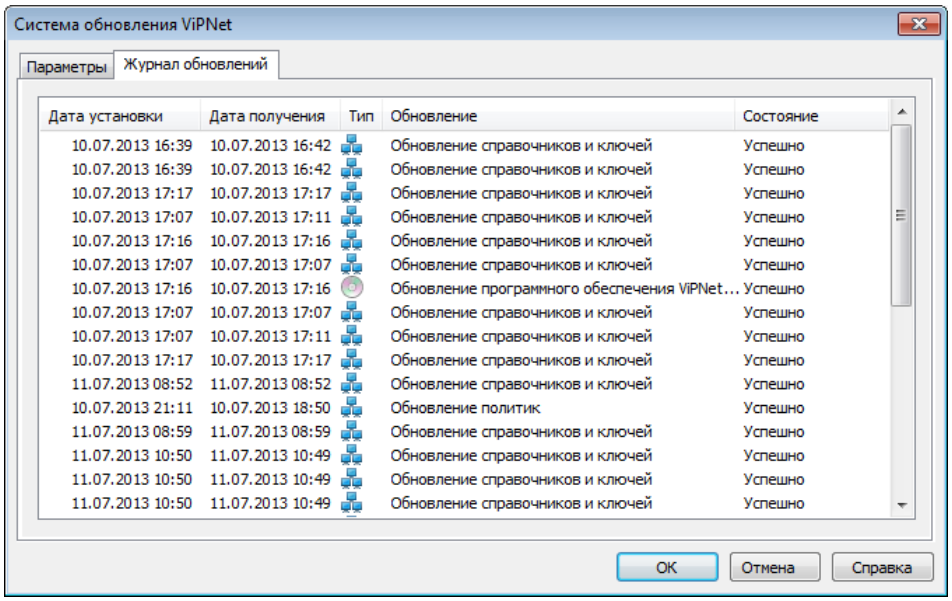


Рисунок 28. Журнал обновлений

Разные типы обновлений обозначаются следующими значками:

— обновление справочников и ключей, обновление политик безопасности.

— обновление ПО ViPNet.

5

Подключение к защищённой сети ViPNet

Протоколы соединений в защищённой сети

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

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

Рисунок 29. Сетевые узлы расположены в одном сегменте локальной сети

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

Рисунок 30. Сетевые узлы соединяются через межсетевой экран

Если на пути следования IP-пакета расположено устройство NAT, на этом устройстве должны быть настроены динамические или статические правила трансляции адресов, которые разрешают обмен UDP-трафиком с узлами сети ViPNet. При настройке статических правил должен быть указан порт инкапсуляции UDP-пакетов. По умолчанию используется порт 55777, но при необходимости он может быть изменён на любой другой. Если пакеты проходят напрямую через координатор, то номер порта узлов, расположенных за этим координатором, значения не имеет. После прохождения через координатор пакетам присваиваются IP-адреса соответствующего сетевого интерфейса координатора, то есть осуществляется трансляция адресов.

Бывают случаи, когда взаимодействие защищённых узлов по UDP-протоколу невозможно, передача UDP-пакетов провайдером услуг запрещена. Например, при удалённом подключении к

сети ViPNet из гостиниц или других общественных мест. В таком случае весь IP-трафик может передаваться через TCP-туннель, настроенный на сервере соединений узла, являющегося инициатором соединения. При настройке TCP-туннеля на сервере соединений может быть указан произвольный порт. По умолчанию используется порт 443.

Рисунок 31. Сетевые узлы соединяются через межсетевой экран

На сервере соединений полученные IP-пакеты извлекаются из TCP-туннеля и передаются дальше на узел назначения по UDP-протоколу. Прямое взаимодействие между узлами защищённой сети невозможно.

Принципы осуществления соединений в защищённой сети

Клиентские узлы в сети ViPNet автоматически выполняют соединения с другими узлами по кратчайшим доступным маршрутам. Для установки соединений они используют серверы соединений. Информацию о других узлах, параметрах доступа и их активности в данный момент клиенты получают от своего сервера IP-адресов. По умолчанию сервер IP-адресов является сервером соединений для клиента, но при необходимости сервером соединений может быть назначен другой координатор.

Параметры подключения к сети определяются клиентами автоматически также с помощью серверов соединений.

Организация соединений между клиентскими узлами осуществляется следующим образом:

- Перед установкой соединения с другим узлом клиент определяет канал доступа к своему серверу соединений. Если клиент определил, что работает через устройство NAT, то он продолжает поддерживать канал путём периодической отправки на сервер IP-пакетов. Интервал отправки IP-пакетов на сервер соединений по умолчанию равен 25 секундам. Этого, как правило, достаточно для работы через большинство устройств NAT. При необходимости интервал (тайм-аут) может быть изменён.
- После того как связь между клиентом и его сервером соединений будет установлена, клиент начинает устанавливать соединение с другим узлом. Он начинает передавать тестовые IP-пакеты удалённому узлу через свой сервер соединений. Одновременно с этим клиент передаёт тестовые IP-пакеты на сервер соединений удалённого узла и напрямую на удалённый узел.
- Если тестовые IP-пакеты дошли до удалённого узла, то удалённый узел регистрирует соединение и начинает ответный IP-трафик передавать напрямую. Клиент при получении ответного IP-трафика от удалённого узла свой последующий IP-трафик ему также начинает передавать напрямую.

Если тестовые IP-пакеты дошли только до сервера соединений удалённого узла, то сервер соединений регистрирует это соединение и отправляет напрямую клиенту ответные IP-пакеты удалённого узла.

То есть с удалённым узлом устанавливается прямое соединение или соединение через его сервер соединений. Если ответный IP-трафик так и не поступил от удалённого узла или его сервера соединений, то клиент по-прежнему осуществляет соединение с удалённым узлом через свой сервер соединений.

Рисунок 32. Взаимодействие между сетевыми узлами

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

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

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

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

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

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

- Возможность прямого соединения с удалённым узлом, стоящим за устройством с динамической трансляцией адресов, сохраняется по умолчанию в течение 75 секунд (трёх тайм-аутов или интервалов отправки IP-пакетов) с момента окончания предыдущего соединения.
- Если клиент расположен за устройством со статической трансляцией адресов, то в его настройках необходимо зафиксировать нужный порт инкапсуляции UDP-пакетов. В противном случае порт будет изменяться, а вследствие этого соединение клиента с другими узлами будет невозможно.

Использование виртуальных IP-адресов

Технология виртуальных адресов позволяет решить проблему с пересечением IP-адресов в локальных и глобальных сетях. Кроме того, виртуальные адреса можно использовать для настройки правил доступа к ресурсу. Поскольку IP-адрес используется для идентификации пользователя, то одной из сетевых угроз является подделка IP-адреса. Однако в сети ViPNet подделка адреса невозможна. В момент приёма пакета из сети ViPNet-драйвер подставляет вместо реального адреса отправителя соответствующий виртуальный адрес, затем пакет передаётся приложению. Это происходит только в случае успешной расшифровки пакета на ключах отправителя, то есть после идентификации отправителя пакета. Это обеспечивает защиту от подмены адреса отправителя и надёжное разграничение доступа к ресурсам на основе виртуальных адресов.

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

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

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

Общие принципы назначения виртуальных адресов

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

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

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

Следует учитывать, что по умолчанию для виртуальных адресов используется один из интернет-диапазонов. Поэтому при взаимодействии узла с открытыми ресурсами интернета может возникнуть конфликт, если у открытого ресурса IP-адрес совпадёт с виртуальным адресом одного из узлов сети ViPNet. Соединение с таким открытым ресурсом будет невозможно. В этом случае доступ к этому ресурсу можно настроить одним из способов:

- сменить диапазон виртуальных адресов;
- работать с ресурсом через прокси-сервер.

При этом работать с защищёнными узлами через прокси-сервер нельзя. Поэтому при использовании прокси-сервера требуется IP-адреса защищённых узлов указать в качестве исключений.

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. Виртуальные адреса для одиночных туннелируемых узлов закрепляются за каждым реальным туннелируемым IP-адресом. Виртуальные адреса закрепляются за сетевыми узлами и одиночными туннелируемыми адресами до тех пор, пока сетевые узлы или туннелируемые адреса не будут удалены.

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

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

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 подключения к защищённой сети

Для подключения клиента к защищённой сети ViPNet в общем случае не требуется никаких настроек. Дополнительные настройки при подключении могут быть нужны только в некоторых особых ситуациях. Например, вы со своим мобильным компьютером подключаетесь к локальной сети другой организации. В этой сети нет доступа к вашему серверу соединений, но в ней есть координатор, имеющий связь с вашим узлом. В этом случае в настройках подключения к сети ViPNet вам потребуется изменить сервер соединений.

Совет. Если вы часто подключаетесь к другой локальной сети, то для удобства вы можете создать конфигурацию, в которой этот вариант настройки подключения будет сохранен. Информацию по созданию конфигурации см. в разделе Управление конфигурациями программы.

Выбрать другой сервер соединений вы также можете, если ваш координатор по каким-то причинам оказался недоступным.

Чтобы назначить сервер соединений:

1. В меню **Сервис** выберите **Настройка приложения**.
2. В окне **Настройка** выберите раздел **Защищённая сеть**.
3. В списке **Сервер соединений** выберите координатор, с помощью которого клиент будет устанавливать соединения с другими узлами. Если нужного координатора нет в списке, нажмите  и выберите координатор в окне **Выбор сетевого узла**.

   Этот координатор должен быть доступен либо напрямую, либо через межсетевой экран со статической трансляцией адресов.
4. Нажмите **Применить**.

Если необходимо, нажмите **Показать дополнительные настройки** и укажите:

- **Весь трафик направлять через сервер соединений**.

  Направлять IP-трафик через сервер соединений может потребоваться в том случае, если есть необходимость в контроле всего передаваемого IP-трафика. При этом стоит учитывать, что передача IP-трафика через сервер соединений может привести к существенному снижению скорости обмена данными между узлами.
- Если требуется установить клиент за межсетевой экран со статической трансляцией адресов, установите флажок **Зафиксировать порт UDP** и в поле ниже укажите порт инкапсуляции UDP-пакетов. Для этого порта на устройстве NAT должно быть создано соответствующее статическое правило.

- Если требуется изменить интервал отправки IP-пакетов серверу соединений при работе через межсетевой экран с динамической трансляцией адресов, в поле **Тайм-аут поддержки соединений через устройства с динамическим NAT** укажите новое значение. По умолчанию отправка IP-пакетов производится каждые 25 секунд. Как правило, этого интервала достаточно, чтобы поддерживать связь с сервером соединений при работе через большинство устройств NAT.
- Выберите координатор в списке **Сервер IP-адресов**.

Внимание! Не изменяйте сервер IP-адресов без согласования с администратором сети ViPNet. Если в качестве сервера IP-адресов вы укажете координатор другой сети ViPNet, то на ваш узел поступит информация только об узлах этой сети. При этом узлы вашей сети будут недоступны.

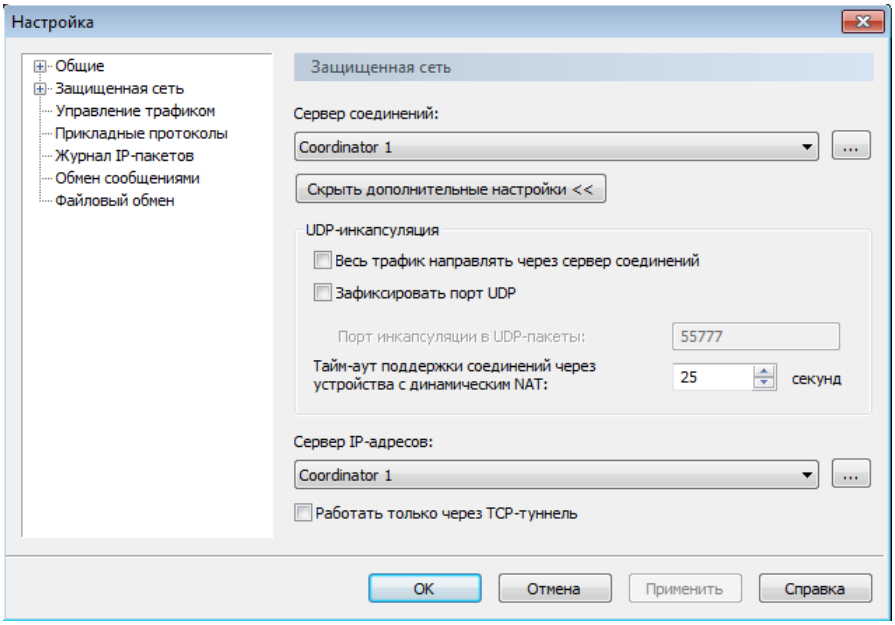


Рисунок 33. Настройка подключения клиента к защищённой сети ViPNet

- Если требуется установить принудительный режим соединения с сервером IP-адресов через TCP-туннель (см. Протоколы соединений в защищённой сети), одновременно установите следующие флажки:
  - **Работать только через TCP-туннель**.
  - **Весь трафик направлять через сервер соединений**.

  Например, это может быть полезно при подключении к интернету через канал связи, по которому TCP-пакеты передаются в более приоритетном порядке, чем UDP-пакеты.
- Если при работе с некоторыми устройствами NAT не проходит передача длинных пакетов, перейдите в подраздел **Защищённая сеть** > **Дополнительные параметры** и уменьшите значение MSS (максимальный размер сегмента).

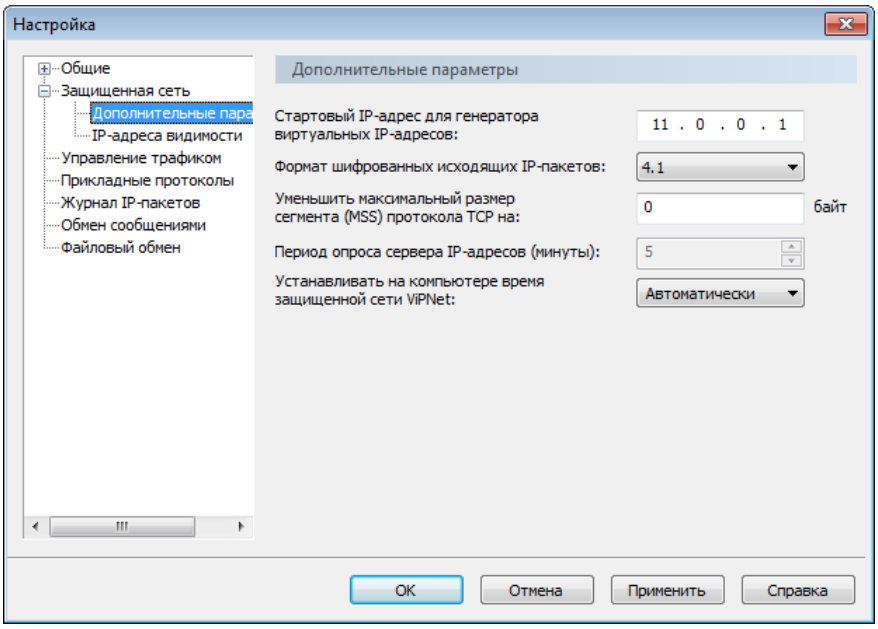


Рисунок 34. Настройка дополнительных параметров

- Если вам требуется изменить системное время на вашем компьютере, в разделе **Дополнительные параметры** в списке **Устанавливать на компьютере время защищённой сети ViPNet** выберите значение **Спрашивать** или **Не устанавливать**. Следует учитывать, что при несовпадении системного времени на вашем компьютере и на вашем сервере доступ к защищённой сети ViPNet будет невозможен.

Данная настройка доступна только для уровня полномочий пользователя «Максимальный». Подробнее см. «Классификация полномочий. Приложение к документации ViPNet».

Внимание! При работе через TCP-туннель вы не будете получать сообщения о рассинхронизации времени на вашем компьютере и в сети ViPNet.

Настройка доступа к защищённым узлам

Для соединения с другими узлами в сети ViPNet должны быть настроены параметры доступа. На клиенте достаточно настроить параметры доступа только для координатора, который является сервером IP-адресов и сервером соединений. При этом данная настройка требуется в том случае, если в программе ViPNet Administrator IP-адреса и параметры подключения координаторов не были заданы централизованно.

Необходимые параметры доступа к другим сетевым узлам будут автоматически получены у сервера IP-адресов после установления с ним связи. Вы можете их изменить, например, при возникновении конфликта IP-адресов. В других случаях изменять их не рекомендуется.

Чтобы настроить доступ к сетевому узлу:

1. Выберите раздел **Защищённая сеть** и дважды щёлкните нужный сетевой узел.
2. В окне **Свойства узла** на вкладке **IP-адреса** добавьте в список реальный IP-адрес сетевого узла. Автоматически новому адресу будет сопоставлен виртуальный IP-адрес.

   Если вам неизвестен IP-адрес узла, то вы можете определить его по имени компьютера. Для этого нажмите **Определить имя/IP-адрес**  и в появившемся окне выполните поиск IP-адреса по указанному имени.

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

   Вы также можете выполнить проверку на конфликт IP-адресов вручную. Для этого нажмите **Проверить конфликты**  .

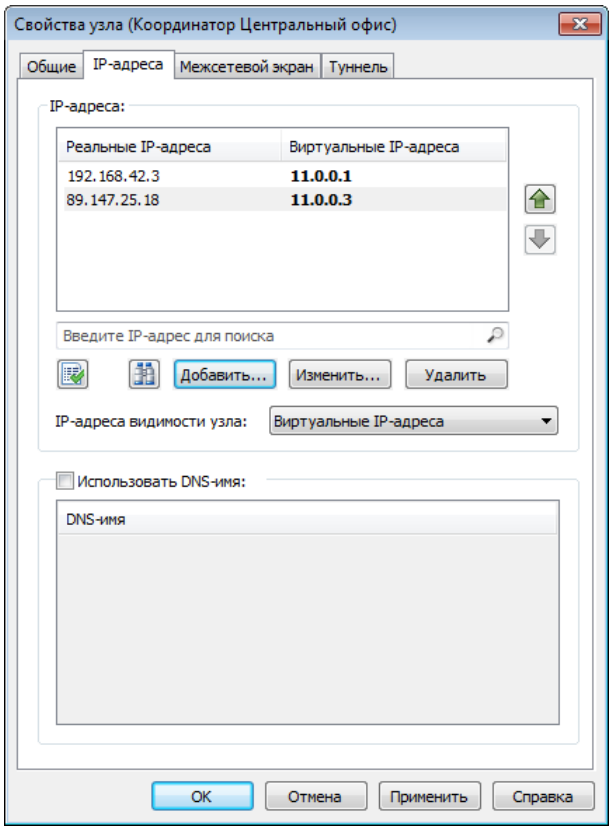


Рисунок 35. Задание IP-адреса сетевого узла

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

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

4 Если для доступа к сетевому узлу необходимо использовать DNS-имя, убедитесь, что узел доступен по этому имени в сети. Затем установите флажок **Использовать DNS-имя** и добавьте в список DNS-имя сетевого узла.

Если вам неизвестно DNS-имя узла, то вы можете определить его по IP-адресу компьютера. Для этого нажмите **Определить имя/IP-адрес** и в появившемся окне выполните поиск по IP-адресу.

При добавлении DNS-имени будет автоматически выполнена его проверка на наличие конфликта с DNS-именами, уже заданными в программе. Если в ходе проверки будет обнаружен конфликт DNS-имён, устраните его (см. Обнаружен конфликт IP-адресов или DNS-имён). Вы также можете выполнить проверку на конфликт DNS-имён с помощью кнопки **Проверить конфликты**.

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

Для клиента порядок DNS-имён в списке не имеет значения. Для координатора в первой строке списка нужно указать DNS-имя, соответствующее IP-адресу координатора. Подробная информация об использовании службы DNS в сети ViPNet см. в разделе Настройка и использование служб имён DNS и WINS в сети ViPNet.

5 При настройке параметров доступа к координатору на вкладке **Межсетевой экран** добавьте IP-адрес межсетевого экрана, если он используется. При необходимости укажите дополнительные IP-адреса. Если будет указано несколько IP-адресов доступа через межсетевой экран, то вы можете указать приоритет этих адресов с помощью метрик.

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

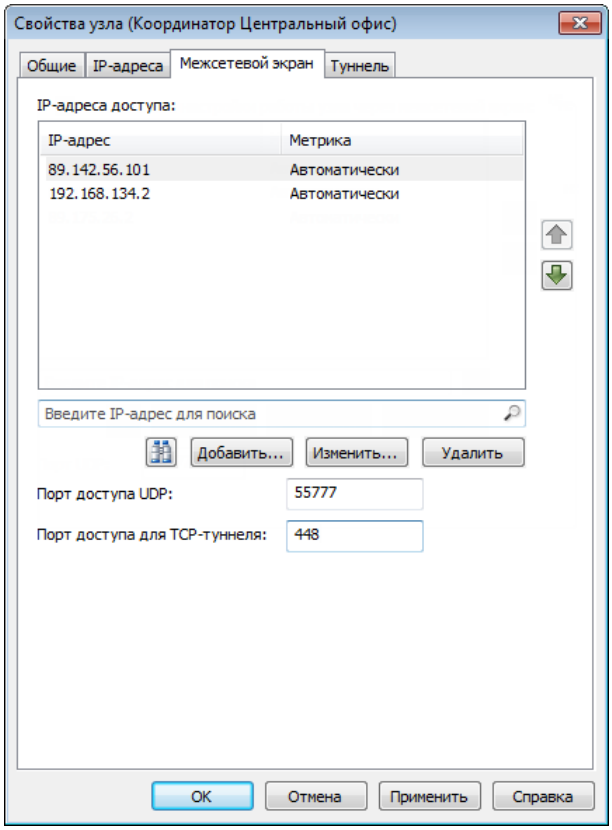


Рисунок 36. Настройка доступа к координатору через межсетевой экран

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

Как правило, информация о номере порта доступа по TCP-протоколу поступает на сетевой узел автоматически сразу после настройки на координаторе TCP-туннеля. Поэтому если в свойствах координатора порт доступа по TCP-протоколу указан, изменять его не следует.

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

Настройка приоритета IP-адресов доступа к координатору

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

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

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

- Метрика определяет задержку (в миллисекундах) отправки тестовых IP-пакетов при выполнении опроса для определения доступности адреса. Соединение устанавливается по тому адресу, доступность которого быстрее определяется в результате опроса.
- Опросы осуществляются в следующих случаях:
  - При запуске ViPNet Client.
  - При проверке соединения с узлом вручную.
  - Периодически. Период опросов задаётся на координаторе: **Сервис** > **Настройка приложения** > **Защищённая сеть** > **Дополнительные параметры**. По умолчанию период опроса координаторами других координаторов равен 15 минутам, период опроса своего координатора клиентами равен 5 минутам.
- Адрес с наименьшей метрикой считается самым приоритетным. Соединение с координатором устанавливается по адресу с наименьшей метрикой всегда, когда этот адрес доступен.
- Если для всех адресов доступа узла метрика назначена автоматически, то значение метрики равно 0. Если для части адресов метрика назначена вручную, а для остальных — автоматически, то значение автоматически назначенной метрики всегда на 100 миллисекунд больше максимального значения метрики, присвоенной вручную.
- Чем больше разница между наименьшей метрикой и остальными метриками, тем меньше вероятность того, что в случае кратковременного сбоя самого приоритетного канала будет выбран менее приоритетный канал. При использовании менее приоритетного канала сетевой узел быстрее сможет вернуться к работе через самый приоритетный канал, когда он станет доступен.

- Если все метрики равны, то для работы будет выбран тот канал, через который соединение с координатором будет установлено быстрее. После того как канал выбран, определение доступности других каналов связи выполняется только при потере соединения по текущему каналу. Этот же механизм действует в случае, если выбран канал связи с наименьшей метрикой.
- Если хотя бы для одного адреса доступа значение метрики задано вручную и выбран не самый приоритетный канал, то определение доступности других каналов связи с целью возвращения к каналу с наименьшей метрикой начнётся одновременно с периодическим опросом по выбранному каналу.
- После определения канала доступа текущий адрес доступа отобразится в окне свойств координатора в первой строке списка IP-адресов на вкладке **Межсетевой экран**.

Чтобы назначить метрики для адресов доступа к координатору:

1. Выберите раздел **Защищённая сеть** и дважды щёлкните координатор.
2. В окне **Свойства узла** откройте вкладку **Межсетевой экран**.
3. В случае необходимости настройте параметры доступа к координатору через межсетевой экран (см. Настройка доступа к защищённым узлам).
4. Чтобы назначить IP-адресу доступа метрику, выберите в списке адрес и нажмите **Изменить**.

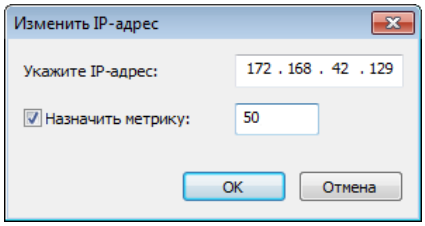


Рисунок 37. Назначение метрики

5. В появившемся окне установите флажок **Назначить метрику** и в поле рядом введите значение метрики в миллисекундах (допустимые значения от 0 до 9999), после чего нажмите **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, причём 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 ViPNet Client или при проверке соединения с координатором сетевой узел будет пытаться установить соединение с координатором по каналу A. Чем меньше период опроса, тем быстрее происходит переход на другой канал в случае сбоев и возвращение на более приоритетный канал.

Настройка доступа к туннелируемым узлам

Если настройки параметров туннелирования для всех координаторов были сделаны в программе ViPNet Administrator, то в программе ViPNet Client на сетевом узле ничего дополнительно настраивать не требуется. Сетевой узел сможет устанавливать соединения с туннелируемыми узлами.

Если предварительных настроек не было, настройте параметры соединения:

1. Выберите раздел **Защищённая сеть**.
2. Дважды щёлкните координатор, который туннелирует нужные открытые узлы.
3. В окне **Свойства узла** на вкладке **Туннель** установите флажок **Использовать IP-адреса для туннелирования** и с помощью соответствующих кнопок сформируйте список IP-адресов туннелируемых узлов. Заданным адресам автоматически будут сопоставлены виртуальные IP-адреса.

   Если вам неизвестен IP-адрес туннелируемого узла, то вы можете определить его по имени компьютера. Для этого нажмите **Определить имя/IP-адрес**  и в появившемся окне выполните поиск IP-адреса по указанному имени.

   При добавлении IP-адреса будет автоматически выполнена его проверка на пересечение с IP-адресами, уже заданными в списке, и IP-адресами других сетевых узлов (в том числе, туннелируемых). Данная проверка позволит исключить возможность задания одинаковых IP-адресов. Если в ходе проверки будет обнаружено пересечение IP-адресов, появится соответствующее сообщение. Устраните пересечение IP-адресов (см. Обнаружен конфликт IP-адресов или DNS-имён).

   Вы также можете выполнить проверку на пересечение IP-адресов вручную. Для этого нажмите **Проверить конфликты**  .

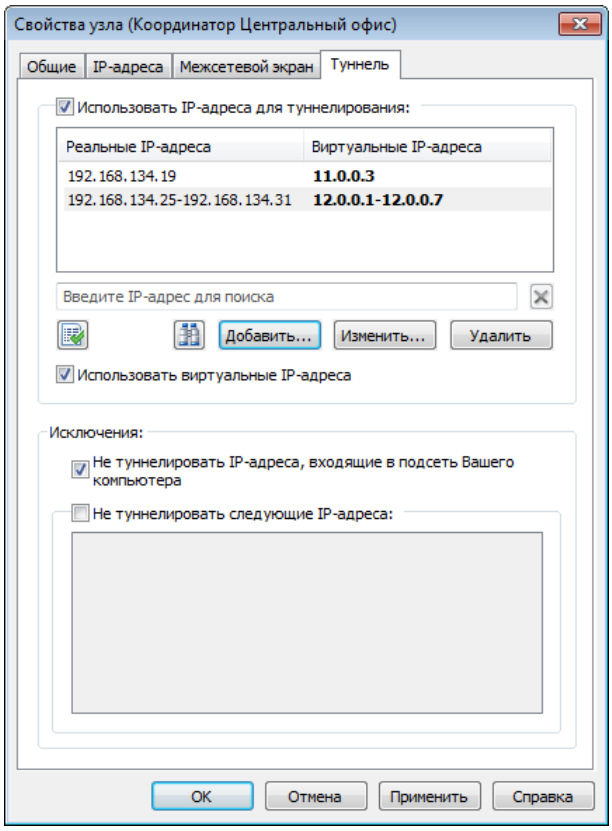


Рисунок 38. Задание адресов туннелируемых узлов

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

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

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

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

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

Установка адресов видимости туннелируемых узлов по умолчанию

При добавлении в корпоративную сеть специализированных устройств (например, IP-АТС, аппаратных IP-телефонов или серверов) используется технология туннелирования. Как правило, для доступа к этим устройствам необходимо указать реальные адреса. Это означает, что при добавлении в сеть новых координаторов, туннелирующих эти устройства, необходимо переключать видимость туннелируемых узлов на реальные адреса. Для автоматизации этого процесса вы можете установить видимость новых координаторов по умолчанию.

Чтобы установить видимость туннелируемых узлов для всех новых координаторов:

1 В меню **Сервис** выберите **Настройка приложения**.

2 В окне **Настройка** выберите раздел **Защищённая сеть** > **IP-адреса видимости**.

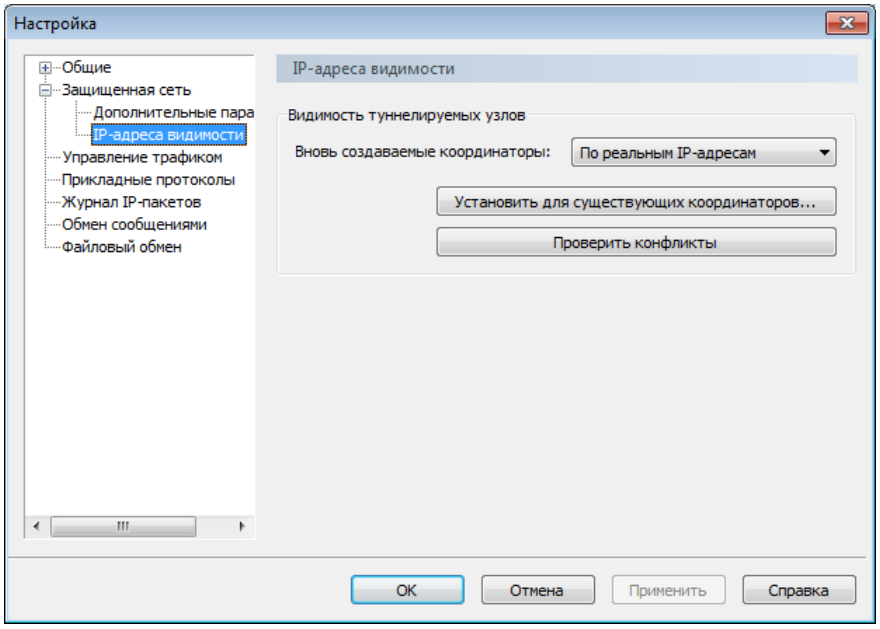


Рисунок 39. Настройка IP-адресов видимости

3 В списке **Вновь создаваемые координаторы** выберите нужный вид адресов и нажмите **OK**.

Теперь при добавлении в сеть новых координаторов адреса туннелируемых им узлов будут всегда реальными или виртуальными, в зависимости от заданного параметра.

Чтобы изменить адреса видимости уже существующих туннелируемых узлов:

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

2. На панели навигации окна **Настройка** выберите раздел **Защищённая сеть** > **IP-адреса видимости**.
3. Нажмите **Установить для существующих координаторов**.
4. В окне **Настройка видимости** выберите нужный вид адресов и нажмите **Установить**.

   Если адреса меняются на реальные, будет выполнена проверка конфликтов адресов в сети.

   Если в ходе проверки конфликтов не обнаружено, будет установлена видимость туннелируемых узлов по реальным адресам для всех существующих координаторов.

   При обнаружении конфликтов появится окно **Проверка конфликтов**. Укажите в нем одно из нужных действий:

   - **Удалить IP-адрес из параметров другого узла**;
   - **Удалить IP-адрес из списка текущего узла**;
   - **Пропустить конфликт**.
5. Для продолжения проверки на наличие конфликтов нажмите **Продолжить**. Чтобы прервать проверку и устранить конфликт другими способами, нажмите **Прервать проверку**.
6. Чтобы впоследствии вернуться к проверке конфликтов нажмите **Проверить конфликты**.

После выполнения указанных действий и устранения конфликтов, будет установлена видимость туннелируемых узлов для всех существующих координаторов по нужному виду адресов.

Просмотр информации о сетевом узле

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

Чтобы просмотреть информацию о чужом сетевом узле ViPNet:

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

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

В блоке **Текущая точка доступа** вы можете посмотреть ID, имя, адрес и порт сервера, через который устанавливается соединение с удалённым узлом. По умолчанию это сервер соединений данного узла. При установке прямого соединения с удалённым узлом значения параметров ID, имя, адрес и порт сервера изменяются и отображается надпись «Установлено прямое соединение с данным узлом».

В блоке **Возможные IP-адреса доступа** (**IP-адреса доступа через межсетевой экран** для свойств координатора) вы можете посмотреть IP-адрес узла и порт доступа к узлу через его межсетевой экран. В квадратных скобках указан тип регистрации адреса:

- -2 — адрес указан вручную.
- -1 — адрес получен из справочников.
- положительное число — адрес зарегистрирован автоматически. Это число равно номеру интерфейса, через который проводилась регистрация.

6

Настройка и использование служб имён 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 имён, обеспечивающие сопоставление имён компьютеров с их IP-адресами. В настоящее время в сетях используются две службы имён — DNS и WINS.

DNS

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

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

Рисунок 40. Общий принцип работы службы DNS

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

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

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

WINS

Аналогично DNS работает служба WINS (Windows Internet Name Service, служба имён сети интернет для Windows). Она преобразует IP-адрес в NetBIOS-имя и наоборот: например, 192.168.1.20 — в HOST-A. Служба WINS является наиболее удобным средством разрешения имён 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. Он обеспечивает доступ компьютера к собственным локальным ресурсам и к ресурсам удалённых компьютеров. Поскольку NetBIOS применяет рассылку широковещательных сообщений, он не поддерживает передачу информации через маршрутизаторы. Но усовершенствования, внесённые в NetBIOS, позволяют этой системе работать поверх протоколов маршрутизации, таких как IP и IPX.

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

Рисунок 41. Общий принцип работы службы WINS

Этот пример демонстрирует следующие события:

1. WINS-клиент HOST-A регистрирует любое из своих локальных имён NetBIOS на своём WINS-сервере WINS-A.

Если компьютер HOST-A не имеет в своём распоряжении IP-адреса WINS-сервера, он передаёт в широковещательной рассылке своё имя NetBIOS, объявляя этим о своём 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. 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.

WINS и DNS могут бесконфликтно работать в пределах одной сети, потому что их пространства имён не совпадают. DNS использует иерархическую структуру именования, а WINS — одноранговую. Служба WINS особенно актуальна для сетей, где есть компьютеры с ОС Windows Server 2003. В сетях, в которых применяются и доменные имена, и имена NetBIOS, рекомендуется использовать обе службы.

Службы DNS и WINS в сети ViPNet

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

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

Если на DNS (WINS) сервере, к которому обращаются приложения, установлено ПО ViPNet или этот сервер туннелируется координатором, поддержка DNS (NetBIOS) имён для виртуальных адресов обеспечивается без дополнительных настроек ПО ViPNet при соблюдении определённых правил (см. DNS- (WINS-) сервер на защищённом или туннелируемом узле).

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

- Обеспечивается безопасная работа приложений с удалёнными защищёнными узлами ViPNet по DNS-именам при использовании открытых (публичных) DNS-серверов (см. Незащищённый).
- Появляется возможность взаимодействия защищённого узла ViPNet со своим координатором по DNS-имени путём публикации на DNS-сервере IP-адреса, не принадлежащего координатору (например, IP-адреса доступа к координатору через NAT-устройство). При автоматической публикации адреса доступа к координатору на публичном DNS-сервере (технология динамического DNS, или DYN DNS) можно организовать безопасный доступ к координатору, адрес доступа к которому динамически изменяется.

DNS- (WINS-) сервер на защищённом или туннелируемом узле

Особенности использования

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

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

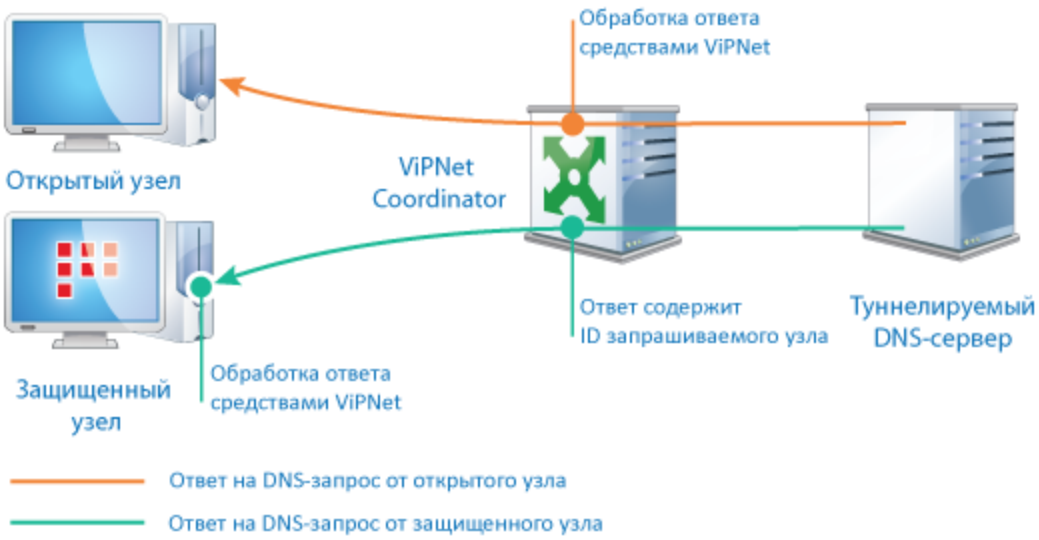


Рисунок 42. DNS-сервер на защищённом или туннелируемом узле

Рекомендации по настройке

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

- При регистрации вручную на DNS- (WINS-) сервере IP-адресов защищённых и туннелируемых узлов следует указывать их виртуальные или реальные IP-адреса, по которым эти узлы видны в программе ViPNet Client, установленной на DNS- (WINS-) сервере, или на координаторе, осуществляющем туннелирование этого сервера.
- Если DNS- (WINS-) сервер расположен на узле с ПО ViPNet, то в подсети этого сервера не следует размещать туннелируемые каким-либо координатором узлы, с которых будут поступать запросы на сервер (или адреса которых будут запрашиваться другими узлами). Если сервер расположен на координаторе, то данное требование относится к туннелируемым узлам других координаторов.
- Если DNS- (WINS-) сервер туннелируется координатором, то в подсети этого сервера не следует размещать узлы с ПО ViPNet, с которых будут поступать запросы на сервер (или адреса которых будут запрашиваться другими узлами).
- Если возникает необходимость размещения узлов в нарушение приведённых рекомендаций, то на узлах с ПО ViPNet следует снять флажок **Не туннелировать IP-адреса, входящие в подсеть Вашего компьютера** (см. Настройка доступа к туннелируемым узлам), а на туннелируемых узлах настроить частный маршрут на узлы с ПО ViPNet через координатор.

Незащищённый DNS- (WINS-) сервер

Особенности использования

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

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

Рисунок 43. Атака на публичный DNS-сервер

Чтобы предотвратить атаки подобного рода, для защищённых прикладных серверов, регистрируемых на публичном DNS-сервере и доступных с защищённого узла, в программе ViPNet Client на этом узле следует указать DNS-имена (см. Настройка доступа к защищённым узлам). Тогда при обращении к серверу по DNS-имени независимо от адреса, подставленного злоумышленником, при приёме ответа на DNS-запрос ViPNet-драйвер подставит уже известный ему IP-адрес видимости узла (реальный или виртуальный), соответствующий заданному в программе ViPNet Client DNS-имени.

Рекомендации по настройке

При использовании открытого DNS-сервера учитывайте рекомендации:

- Если внешний IP-адрес доступа к координатору может изменяться, для организации доступа к этому координатору по DNS-имени, зарегистрированному на открытом DNS-сервере, в программе ViPNet Client на защищённых узлах для данного координатора следует указать DNS-имя.
- Если на узле с ПО ViPNet другие защищённые узлы доступны по виртуальным IP-адресам, и необходимо обеспечить доступ к этим узлам по DNS-именам, зарегистрированным на открытом DNS-сервере, то эти DNS-имена следует указать в программе ViPNet Client. При этом на открытом DNS-сервере может быть зарегистрирован любой адрес (реальный или виртуальный). Технология ViPNet обеспечит защищённое соединение по виртуальному адресу видимости узла вне зависимости от типа опубликованного адреса.
- Даже если доступ к защищённым узлам обеспечивается по реальным адресам, важно указать их DNS-имена в программе ViPNet Client.

Во всех описанных случаях DNS-имена защищённых узлов могут быть заданы вручную на каждом сетевом узле (см. Настройка доступа к защищённым узлам), однако рекомендуется указывать DNS-имена централизованно в программе ViPNet Центр управления сетью.

Использование защищённого DNS- (WINS-) сервера для удалённой работы с корпоративными ресурсами

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

Автоматическая регистрация DNS- (WINS-) серверов

Для удалённого доступа к узлам корпоративной сети по DNS-именам должны быть выполнены следующие условия:

- В системном файле `hosts`, который устанавливает соответствие между IP-адресами и именами компьютеров, не должно быть записей об узлах корпоративной сети. Этот файл расположен в папке `%systemroot%\System32\drivers\etc\` (по умолчанию это `C:\Windows\System32\drivers\etc\`).
- В ЦУСе или на сетевых узлах должен быть сформирован список корпоративных DNS (WINS) серверов.

Внимание! Если защищённый узел зарегистрирован и на корпоративном DNS-сервере, и на публичном, то могут возникнуть проблемы с доступом к нему. Чтобы избежать проблем с доступом к такому сетевому узлу, укажите его DNS-имя в окне свойств узла на вкладке **IP-адреса**.

Вы можете указать адрес корпоративного DNS-сервера вручную (см. Создание списка DNS (WINS) серверов вручную). Однако рекомендуется задать адреса корпоративных DNS-серверов централизованно. Для этого администратору сети ViPNet следует указать сетевые узлы или туннелируемые узлы, на которых расположены DNS-серверы, в программе ViPNet Центр

управления сетью. В этом случае список корпоративных DNS-серверов будет передан на сетевые узлы ViPNet вместе с ключами и справочниками. На сетевых узлах программа ViPNet Client будет определять текущие IP-адреса видимости корпоративных DNS-серверов (реальные или виртуальные) и автоматически изменять адреса DNS-серверов в настройках сетевых интерфейсов компьютера.

Если сетевой узел настроен на работу с корпоративными DNS-серверами, то для него существуют следующие особенности работы с публичными и корпоративными сетевыми ресурсами:

- Корпоративные DNS-серверы настроены на преобразование как внутренних, так и внешних имён.

  В этом случае при подключении к защищённой сети будут использоваться только корпоративные DNS-серверы. Запросы на преобразование имён внешних и внутренних ресурсов (например, www.google.com и http://portal.internal) будут направляться на корпоративный DNS-сервер.

- Корпоративные DNS-серверы настроены только на преобразование внутренних имён.

  В этом случае запросы на преобразование внешних имён (например, www.google.com) будут направляться на внешний (незащищённый) DNS-сервер. Запросы на преобразование имён внутренних ресурсов (например, http://portal.internal) будут направляться на корпоративный DNS-сервер.

Обратите внимание, что если в ЦУСе заданы имена доменов, используемых внутри корпоративной сети (например, http://portal.internal), то запросы на их преобразование будут направляться только на корпоративный DNS-сервер. Запросы на преобразование имён внутренних ресурсов на внешние DNS-серверы будут блокироваться.

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

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

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

Создание списка DNS (WINS) серверов вручную

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

Для регистрации корпоративного DNS- (WINS-) сервера вручную:

1. Если вы обладаете правами администратора:
   - Перейдите в `C:\ProgramData\InfoTeCS.Admin\ServicesPrivate\IpLirControlData\databases\dnswinslist`
   - Отредактируйте файл `dns.txt`.

   Если вы не обладаете правами администратора, создайте файл `dns.txt` в транспортном каталоге (по умолчанию `C:\ProgramData\InfoTeCS\ID_Узла`).
2. Внесите в файл `dns.txt` запись о корпоративном DNS- (WINS-) сервере. О том, как указать информацию о сервере, см. в разделах ниже. Формат записей в файле `dns.txt` отличается в зависимости от того, установлен ли корпоративный DNS- (WINS-) сервер на защищённом узле или туннелируется координатором.
3. Также вы можете добавить в файл параметр, который переключает DNS-зоны (корпоративные или публичные) на вашем сетевом узле.
4. Сохраните изменения.

Примечание. Все операции по созданию и редактированию файла `dns.txt` можно производить, не закрывая программу ViPNet Client.

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

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

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

Если корпоративный DNS- (WINS-) сервер установлен на защищённом сетевом узле, то в файле `dns.txt` укажите следующую информацию:

- Для DNS-сервера:

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

- Для WINS-сервера:

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

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

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

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

В разделе ниже вы можете ознакомиться с примером составления файла `dns.txt` (см. Пример составления файла dns.txt).

Если корпоративный DNS (WINS) сервер туннелируется координатором

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

- Для DNS-сервера:

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

- Для WINS-сервера:

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

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

Примечание. Чтобы узнать идентификатор координатора, который туннелирует DNS- (WINS-) сервер, в программе ViPNet Client дважды щёлкните его в разделе **Защищённая сеть**. В окне **Свойства узла** на вкладке **Общие** в первой строке будет указан идентификатор координатора.

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

`IP-адрес` — IP-адрес DNS- или WINS-сервера.

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

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

В разделе ниже вы можете ознакомиться с примером составления файла `dns.txt` (см. Пример составления файла dns.txt).

Пример составления файла dns.txt

Ниже приведён пример того, как может быть составлен файл `dns.txt`:

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

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.

Параметр `INTERNET` необязательный и может иметь два значения:

- `ON` — использовать только корпоративные DNS-серверы;
- `OFF` — использовать любые DNS-серверы.

  В этом случае запросы на разрешение публичных имён отправляются на открытые DNS-серверы. Если их не удалось разрешить на открытых DNS-серверах, то они передаются на корпоративные DNS-серверы.

Обращение к удалённым узлам через туннелируемый DNS-сервер

Чтобы узлы внутренней сети ViPNet могли обращаться к удалённым узлам ViPNet по доменным именам через туннелируемый DNS-сервер, требуются дополнительные настройки на DNS-сервере и клиентах сети.

Внимание! Если на DNS-сервере разрешены только безопасные динамические обновления, то на координаторе, туннелирующем DNS-сервер, должна быть настроена видимость клиентов по реальным IP-адресам (см. Настройка доступа к защищённым узлам). Иначе обновления записей на DNS-сервере не будут считаться безопасными и клиенты не зарегистрируются на туннелируемом DNS-сервере.

Для примера рассмотрим схему сети, в которой корпоративный DNS-сервер туннелируется координатором, при этом:

- есть сетевые узлы без ViPNet Client, которые находятся в туннеле;
- есть сетевые узлы с ViPNet Client, которые подключаются к корпоративной сети через интернет;
- с внутренних туннелируемых узлов (1) надо обращаться к узлам с ViPNet Client в интернете (2) по доменным именам.

Рисунок 44. Схема расположения сетевых узлов и DNS-сервера

Чтобы в этой схеме доменные имена разрешались правильно:

- На DNS-сервере настройте поддержку динамического изменения DNS-записей. Как правило, по умолчанию DNS-серверы не поддерживают эту настройку.
- Для клиентов, к которым будут обращаться по DNS-имени:

    - в ViPNet ЦУС укажите корпоративный DNS-сервер;
    - на самих клиентах настройте автоматическую регистрацию на DNS-сервере.
- На всех туннелирующих координаторах, участвующих в схеме, включите обработку прикладного протокола DNS (для службы `alg`).

Использование публичного DNS-сервера

Если в вашей корпоративной сети настроены защищённые DNS-серверы (см. Использование защищённого DNS- (WINS-) сервера для удалённой работы с корпоративными ресурсами), с которыми у вас в данный момент нестабильное соединение, то вы можете включить режим «Публичный DNS». В этом режиме все запросы на преобразование имён будут направляться только на внешний DNS-сервер вашего интернет-провайдера. Имена корпоративных ресурсов при этом будут недоступны, так как их разрешение возможно только при подключении к защищённому DNS-серверу.

Чтобы включить использование публичного DNS-сервера:

1. В меню **Файл** выберите **Конфигурации** > **Публичный DNS**.
2. В окне с предупреждением нажмите **Публичный DNS**.

Чтобы вернуться к использованию защищённого DNS-сервера, в окне программы в меню **Файл** > **Конфигурации** выберите **Защищённый DNS**. Также программа ViPNet Client автоматически переключается на использование защищённого DNS-сервера после перезагрузки компьютера.

Использование DNS-серверов на контроллерах домена

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

Воспользуйтесь одним из следующих вариантов:

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

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

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

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

7

Интегрированный сетевой экран

Основные принципы фильтрации трафика

Фильтруется весь IP-трафик, который проходит через сетевой узел:

- открытый (незашифрованный) трафик;
- защищённый (зашифрованный) трафик.

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

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

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

- Все входящие и исходящие открытые и зашифрованные IP-пакеты проверяются на соответствие условиям сетевых фильтров в порядке убывания приоритета этих фильтров.
- Если IP-пакет соответствует условию одного из фильтров, то он пропускается или блокируется этим фильтром. При этом фильтры с более низким приоритетом не применяются.
- Если IP-пакет пропущен одним из фильтров, то ответные IP-пакеты (включая служебные ICMP-пакеты) в рамках текущего соединения будут пропускаться автоматически.

Если IP-пакет не обработан ни одним из фильтров, то он блокируется фильтром по умолчанию.

Это обеспечивает высокий уровень безопасности, разрешая соединения только с нужными узлами по заданным протоколам и портам.

Схематично последовательность фильтрации IP-пакетов представлена ниже.

Рисунок 45: Фильтрация IP-трафика

Общие сведения о сетевых фильтрах

Программа ViPNet Client позволяет настроить сетевые фильтры как для защищённого, так и для открытого трафика. Они выполняют следующие функции:

- Фильтры открытой сети могут разрешать либо запрещать обмен IP-трафиком с открытыми узлами.
- Фильтры прикладного уровня открытой сети позволяют блокировать IP-пакеты на уровне приложений (доступно, если установлен модуль расширенной фильтрации).

Примечание. К открытым узлам также относятся компьютеры с ПО ViPNet Registration Point.

- Фильтры защищённой сети могут разрешать или блокировать обмен IP-трафиком с защищёнными узлами ViPNet, с которыми данный узел ViPNet Client имеет связь.

Все сетевые фильтры делятся на следующие категории:

- Фильтры, определённые специальными конфигурациями.

  Данные фильтры имеют самый высокий приоритет и применяются в первую очередь. Они ограничивают трафик, который запрещён в конфигурациях «Открытый Интернет» (см. Конфигурация «Открытый интернет»), «Внутренняя сеть» или «Интернет» (см. Конфигурации «Внутренняя сеть» и «интернет»). Их нельзя редактировать и удалять.

- Фильтры, поступившие в составе политик безопасности из программы ViPNet Policy Manager.

  Данные фильтры нельзя редактировать и удалять. Их можно отключить с помощью специальной опции в режиме администратора (см. Параметры защиты трафика).

- Предустановленные фильтры (см. Предустановленные сетевые фильтры) и фильтры, заданные пользователем.

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

- Блокирующий фильтр по умолчанию. Данный фильтр блокирует весь трафик, который не соответствует условиям ни одного из предыдущих фильтров.

При запуске программы ViPNet Client, при включении защиты трафика или смене конфигурации программы сетевые фильтры загружаются в ViPNet-драйвер (см. Низкоуровневый ViPNet-драйвер сетевой защиты). При этом выполняется контроль целостности базы сетевых фильтров. Если

целостность сетевых фильтров нарушена, появится соответствующее предупреждение, и будут загружены предустановленные сетевые фильтры.

Последовательность применения сетевых фильтров согласно приоритету изображена на схеме.

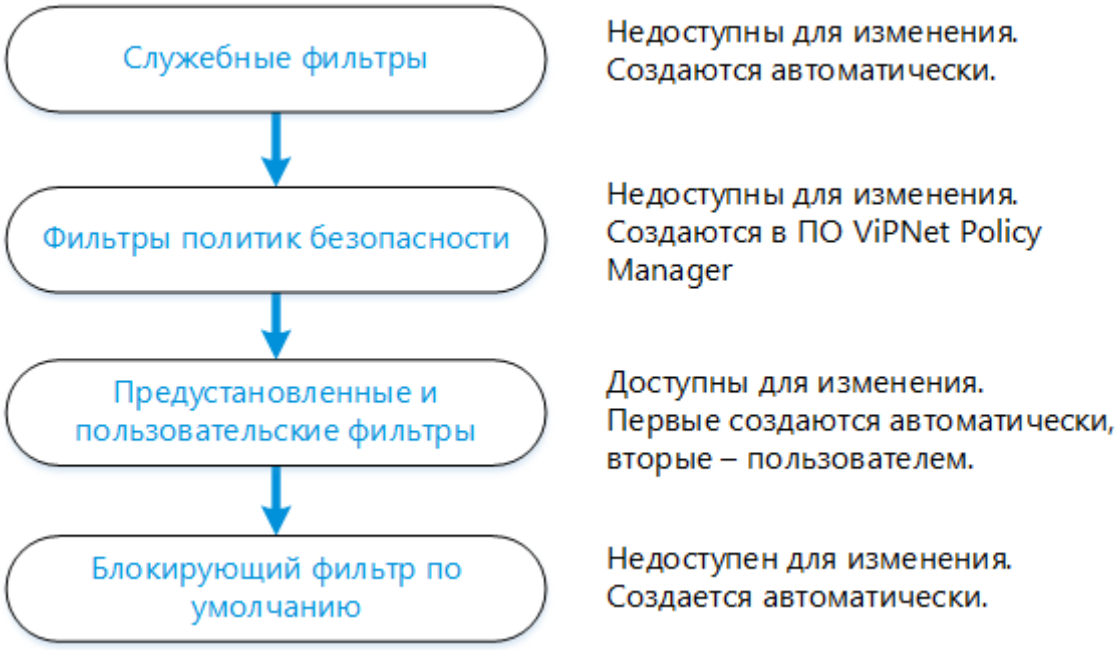


Рисунок 46. Последовательность применения сетевых фильтров

Списки сетевых фильтров представлены в разделах **Фильтры защищённой сети**, **Фильтры открытой сети** и **Фильтры прикладного уровня открытой сети**.

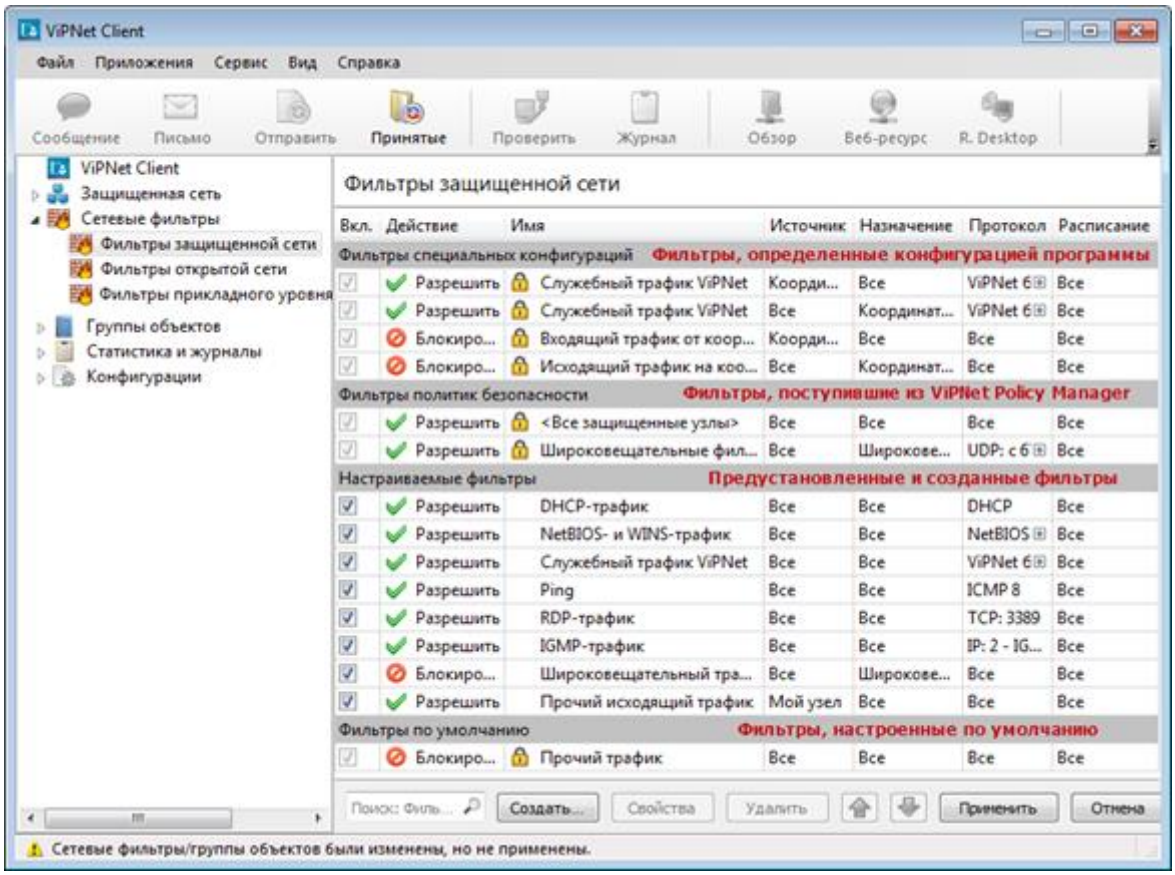


Рисунок 47. Пример отображения фильтров для защищённого трафика разных категорий

Сетевые фильтры имеют следующие особенности:

- Для каждого фильтра можно настроить:
  - Действие — пропускать (✅) или блокировать (⛔) IP-пакеты, соответствующие заданным параметрам.
  - Источник и назначение задают отправителя и получателя IP-пакетов.
  - Протоколы фильтрации IP-пакетов.
  - Расписание действия.

  Для задания параметров фильтра могут использоваться группы объектов (см. Использование групп объектов).
- Фильтры, созданные пользователем, влияют как на новые, так и на уже существующие соединения. Таким образом, если фильтр, блокирующий трафик соединения, добавлен после установления соединения, то оно будет разорвано.
- IP-пакеты проверяются в соответствии с расположением фильтров в списке, по порядку сверху вниз. Когда пакет блокируется или пропускается первым подходящим фильтром, последующие фильтры уже не оказывают никакого влияния на данный пакет.
- В программе ViPNet Client фильтры различных категорий в списках фильтров отображаются в соответствующих группах и располагаются в порядке их приоритета согласно схеме выше.

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

Фильтры, которые нельзя отредактировать и удалить, отмечены значком  .

- Чтобы изменить действие фильтра, двойным щелчком откройте свойства фильтра и в разделе **Основные параметры** выберите нужное значение. Чтобы включить или отключить фильтр, установите или снимите флажок рядом с именем фильтра.
- При изменении настроек сетевых фильтров или создании новых фильтров в строке состояния появляется сообщение о том, что фильтры были изменены, но не применены. Изменённые или новые фильтры не вступят в действие до тех пор, пока вы не нажмёте **Применить** и в течение 30 секунд не подтвердите сохранение изменений.

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

При необходимости вы можете отменить все изменения и восстановить предустановленные фильтры (см. Восстановление предустановленных фильтров и групп объектов).

Использование групп объектов

Группы объектов позволяют упростить создание сетевых фильтров. Они объединяют несколько значений одного типа и могут быть заданы при настройке параметров фильтра вместо отдельных объектов.

Группы объектов делятся на несколько видов:

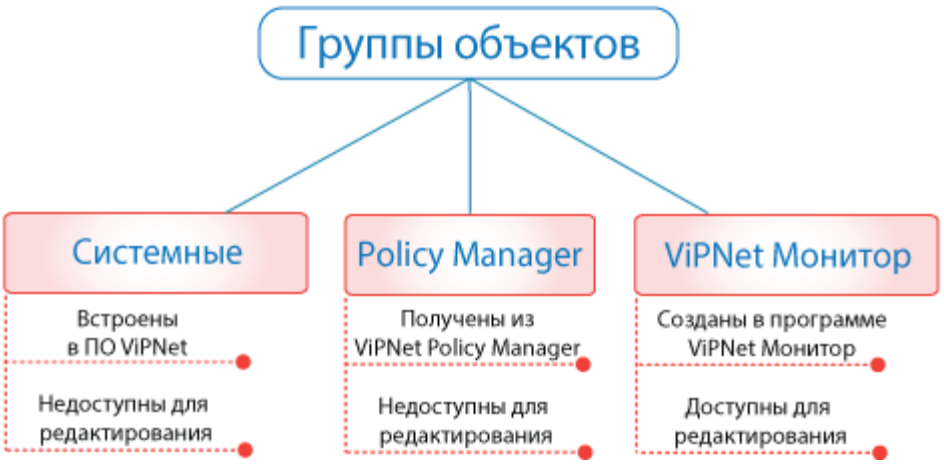


Рисунок 48. Виды групп объектов

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

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

Пользовательские группы объектов — группы объектов, создаваемые пользователем непосредственно в программе ViPNet Client, а также некоторые группы, настроенные по умолчанию. Подробнее о группах по умолчанию см. в разделе Пользовательские группы объектов, настроенные по умолчанию. У каждой группы объектов есть свой состав, при этом из состава могут быть заданы некоторые исключения. В состав и исключения группы могут быть включены другие группы объектов той же категории или некоторые системные группы объектов. Работа с такими группами объектов осуществляется в разделе **Группы объектов**.

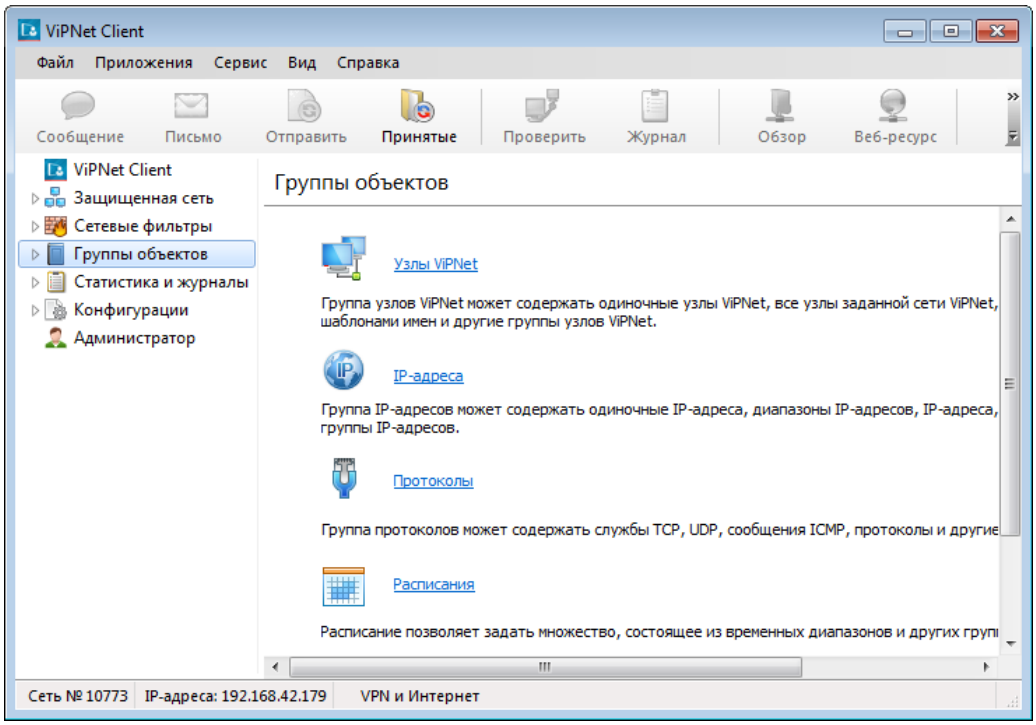


Рисунок 49. Работа с пользовательскими группами объектов

Пользовательские группы объектов делятся на следующие типы:

- **Узлы ViPNet** — группа узлов защищённой сети. Используется в фильтрах защищённой сети.
- **IP-адреса** — любая комбинация отдельных IP-адресов и диапазонов IP-адресов или DNS-имён. Используется в фильтрах открытой сети.
- **Протоколы** — любая комбинация протоколов и портов. Используется во всех фильтрах.
- **Расписания** — любая комбинация условий применения сетевых фильтров по времени и дням недели. Используется во всех фильтрах.

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

Системные группы объектов

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

Таблица 2. Системные группы объектов

Имя группы объектов	Значение
Все клиенты	Все клиенты из справочников узла
Все координаторы	Все координаторы из справочников узла
Все объекты	Совокупность всех объектов в группе конкретного типа. Задаётся только в составе группы объектов. Предназначена для создания групп, состоящих из всех объектов, кроме некоторых исключений
Широковещательные адреса	Все широковещательные адреса Используется при создании фильтров широковещательных пакетов
Мой узел	Свой узел Можно указать в качестве источника IP-пакетов для исходящих соединений узла или в качестве назначения для входящих соединений
Другие узлы	Другие сетевые узлы (любые узлы, кроме своего) Можно указать в качестве источника IP-пакетов для входящих соединений узла или в качестве назначения для исходящих соединений
Туннелируемые IP-адреса	Все IP-адреса, туннелируемые координатором
Групповые адреса	Диапазон адресов для групповой рассылки (224.0.0.0–239.255.255.255) Можно указать только в качестве назначения для локальных открытых соединений

Пользовательские группы объектов, настроенные по умолчанию

- Группы IP-адресов:
  - **Публичные IP-адреса** — группа, в составе которой указаны все IP-адреса, за исключением частных IP-адресов.
  - **Частные IP-адреса** — группа, в составе которой указаны IP-адреса локальных сетей: 10.0.0.0; 172.16.0.0; 192.168.0.0.

- **Зарезервированные IP-адреса** — адреса, зарезервированные в IPv4 под служебные цели. Группа появилась в версии 4.5, поэтому при обновлении ViPNet Client с более ранних версий группа не создаётся.

Чтобы создать группу, в разделе **Сетевые фильтры** нажмите **Восстановить фильтры по умолчанию**. Эти действия необходимо согласовать с администратором сети ViPNet, поскольку все настроенные фильтры будут удалены.

- Группы протоколов, которые чаще всего используются при создании сетевых фильтров. Например: **DHCP**, **ViPNet базовые службы**, **ViPNet удалённый просмотр журнала** и другие.
- Группы расписаний:
  - **Рабочие дни** — группа, включающая дни с понедельника по пятницу.
  - **Выходные дни** — группа, включающая субботу и воскресенье.

Создание и изменение групп объектов

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

   Откроется окно свойств группы объектов, в котором вы можете задать параметры новой группы.
4. В разделе **Основные параметры** задайте имя группы объектов. Имя группы должно быть уникальным.
5. В разделе **Состав** определите состав создаваемой группы.

   При формировании состава группы типа:

   - **Узлы ViPNet —** укажите защищённые узлы, которые необходимо включить в создаваемую группу. Подробнее см. раздел Добавление сетевых узлов.

     В состав группы узлов защищённой сети вы также можете включить системные группы объектов **Все координаторы** и **Все клиенты** (см. Системные группы объектов).

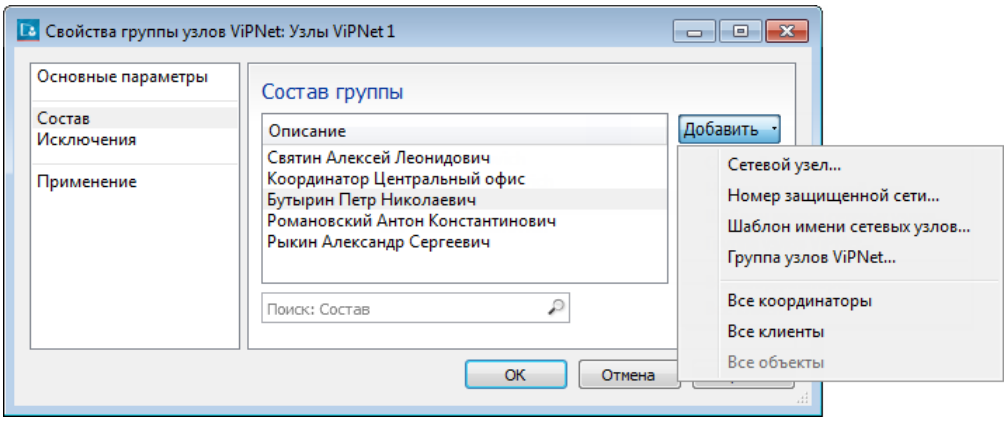


Рисунок 50. Формирование состава группы узлов

- **IP-адреса** — задайте отдельные IP-адреса, диапазон адресов или подсеть либо DNS-имена. Подробнее см. раздел Добавление IP-адресов и DNS-имён.

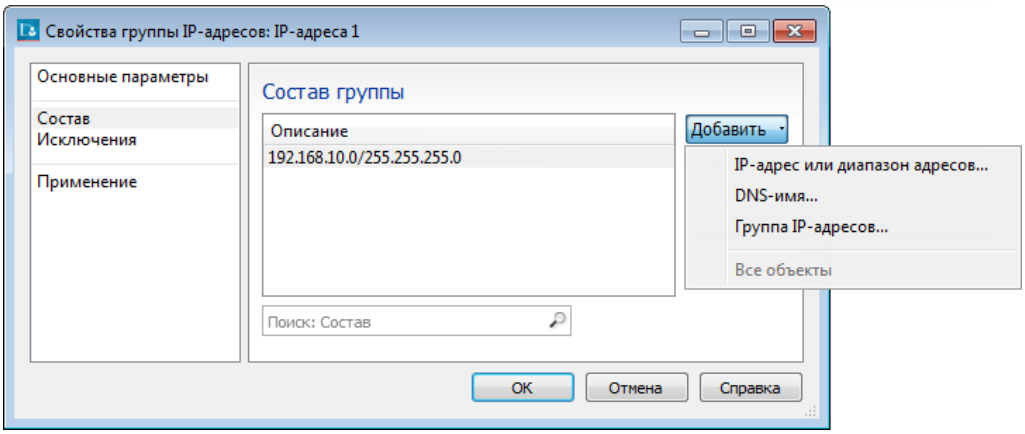


Рисунок 51. Формирование состава группы IP-адресов

- **Протоколы** — задайте протоколы и при необходимости номера портов. Подробнее см. раздел Добавление протоколов.

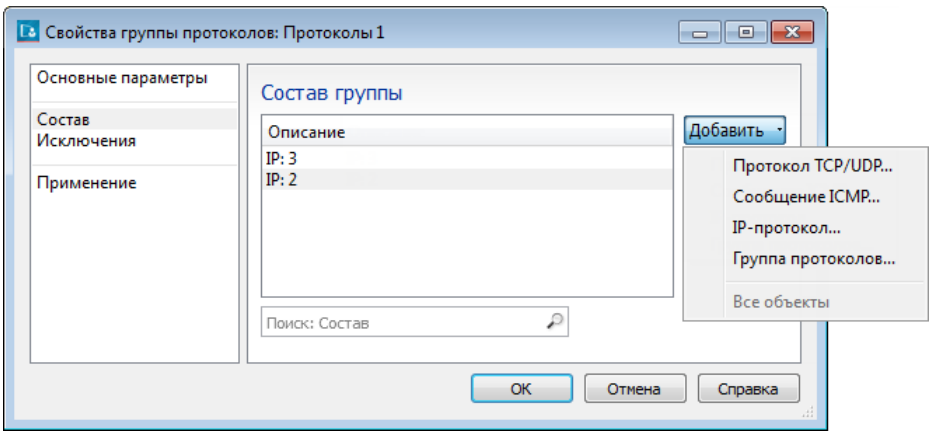


Рисунок 52. Формирование состава группы протоколов

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

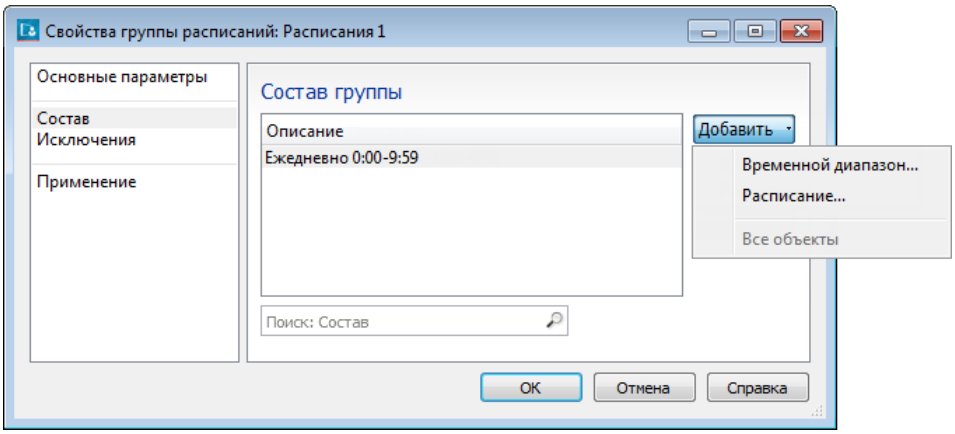


Рисунок 53. Формирование состава группы расписаний

Примечание. В каждую группу объектов могут входить группы объектов этого же типа, то есть можно организовать вложенность однотипных групп.

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

---

6 В разделе **Исключения** задайте исключения из состава группы объектов, то есть те элементы, которые в группу объектов не должны входить. Например, чтобы создать группу защищённых узлов, состоящую из всех координаторов, кроме одного, добавьте в состав системную группу **Все координаторы**, а в качестве исключения задайте конкретный сетевой узел — координатор.

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

Формирование исключений осуществляется аналогично формированию состава групп объектов.

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

---

7 По завершении нажмите **OK**.

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

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

Чтобы изменить параметры группы объектов, выберите её в соответствующем разделе групп объектов, затем дважды щёлкните или нажмите **Свойства**. После изменения основных параметров группы или её состава в окне свойств группы нажмите **OK**.

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

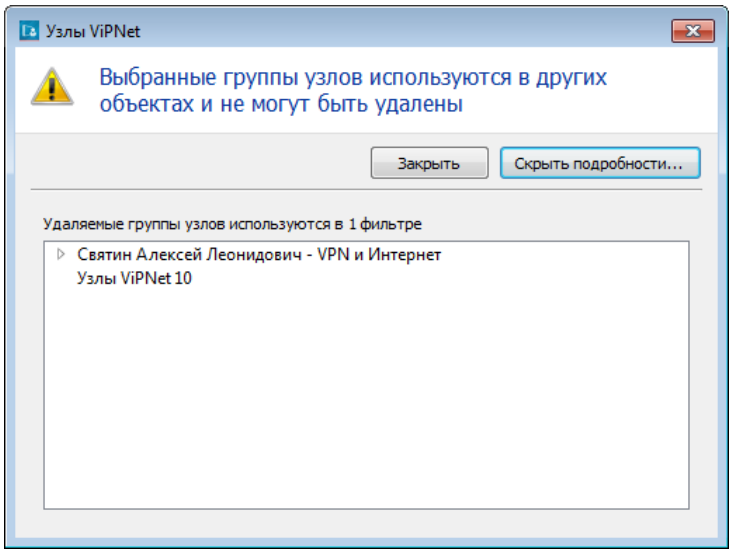


Рисунок 54. Невозможность удаления группы объектов

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

Добавление сетевых узлов

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

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

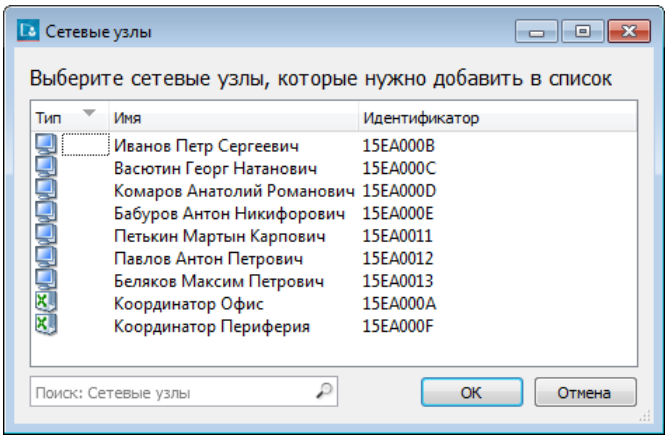


Рисунок 55. Выборочное добавление сетевых узлов

В результате будут добавлены выбранные узлы.

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

  В результате будут добавлены все узлы из заданной сети.

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

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

Добавление IP-адресов и DNS-имён

IP-адреса или DNS-имена могут быть добавлены в состав и исключения групп IP-адресов, а также заданы при определении источника и назначения в локальных фильтрах открытой сети.

Чтобы добавить IP-адреса в одном из указанных случаев:

1. В окне свойств группы IP-адресов или сетевого фильтра в соответствующем разделе нажмите **Добавить** и в меню выберите **IP-адрес или диапазон адресов**.
2. В появившемся окне выполните следующие действия:
   - Если требуется добавить один конкретный IP-адрес (в том случае, если он известен), установите переключатель в положение **IP-адрес** и в поле напротив введите данный IP-адрес.
   - Если требуется задать IP-адреса в рамках некоторой подсети, установите переключатель в положение **Подсеть**, после чего в соответствующих полях задайте адрес и маску данной подсети.

- Если требуется задать диапазон IP-адресов, установите переключатель в положение **Диапазон IP-адресов**, после чего в соответствующих полях задайте начальный и конечный адрес диапазона.

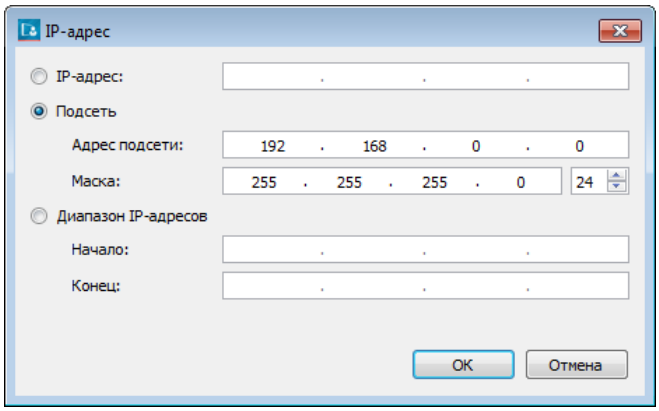


Рисунок 56. Добавление IP-адресов

После ввода необходимых данных нажмите **OK**.

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

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

В результате DNS-имя будет добавлено.

Добавление протоколов

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

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

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

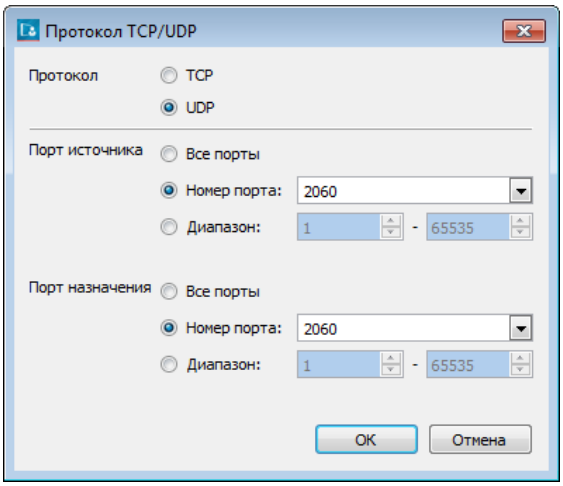


Рисунок 57. Добавление TCP- или UDP-протокола

По завершении ввода данных нажмите **OK**.

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

Добавление расписаний

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

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

1. В окне свойств группы расписаний или сетевого фильтра в соответствующем разделе нажмите **Добавить** и в меню выберите **Временной диапазон**.
2. В появившемся окне задайте параметры расписания:
   - В группе **Время выполнения фильтра** укажите временной интервал, в течение которого будет действовать сетевой фильтр.
   - Установите переключатель в положение:
     - **Ежедневно**, если сетевой фильтр должен действовать каждый день в указанное время. Если требуется, чтобы фильтр действовал в некоторый период времени (например, в течение двух недель), установите соответствующий флажок и задайте нужный период.
     - **Еженедельно**, если сетевой фильтр должен действовать в определённые дни недели. Установите флажки напротив нужных дней недели.

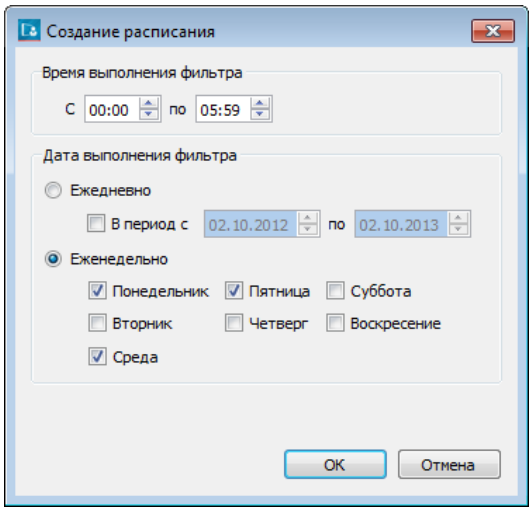


Рисунок 58. Добавление расписания

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

В результате будет добавлено расписание с заданными параметрами.

Создание сетевых фильтров

В программе ViPNet Client предусмотрена возможность создания следующих фильтров:

- фильтров для защищённой сети,
- фильтров для открытой сети,
- фильтров прикладного уровня (доступно, если установлен модуль расширенной фильтрации).

Для создания любого из перечисленных фильтров выполните следующие действия:

Примечание. Для фильтров прикладного уровня доступны не все из описанных ниже параметров.

---

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

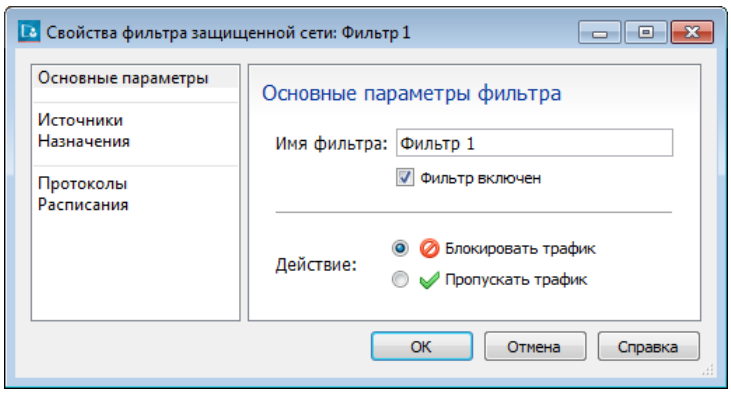


Рисунок 59. Задание основных параметров фильтра

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

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

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

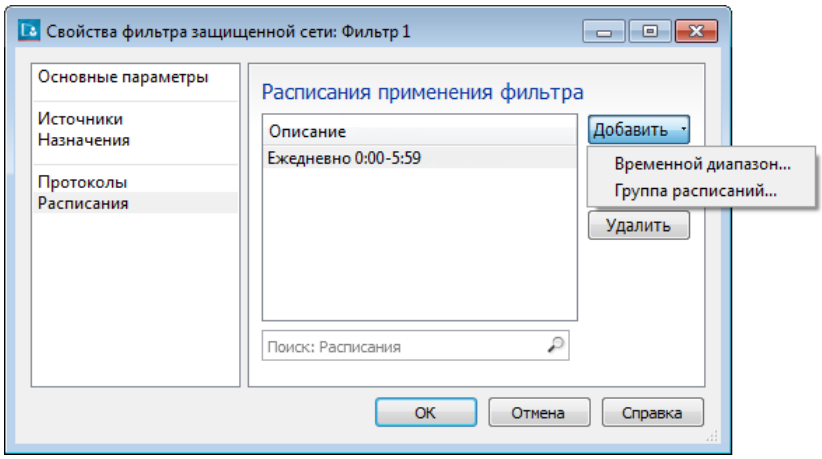


Рисунок 60. Добавление расписания при создании фильтра

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

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

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

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

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

Создание фильтров для защищённой сети

Чтобы создать фильтр для защищённого трафика (см. Общие сведения о сетевых фильтрах), выполните следующие действия:

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

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

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик.

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

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

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

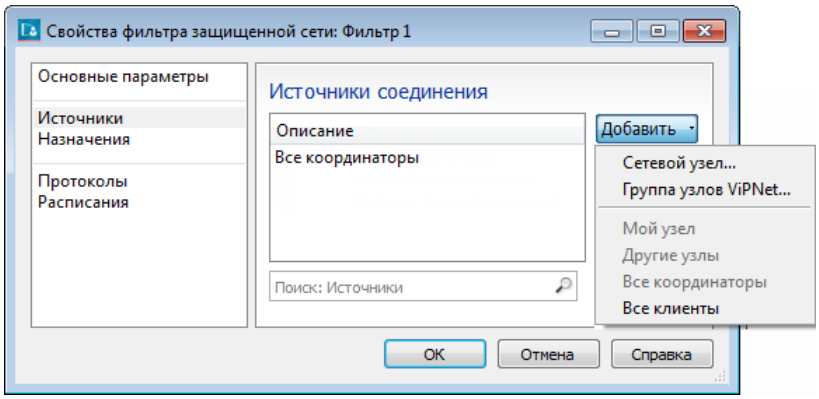


Рисунок 61. Задание отправителя защищённых IP-пакетов

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

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

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

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

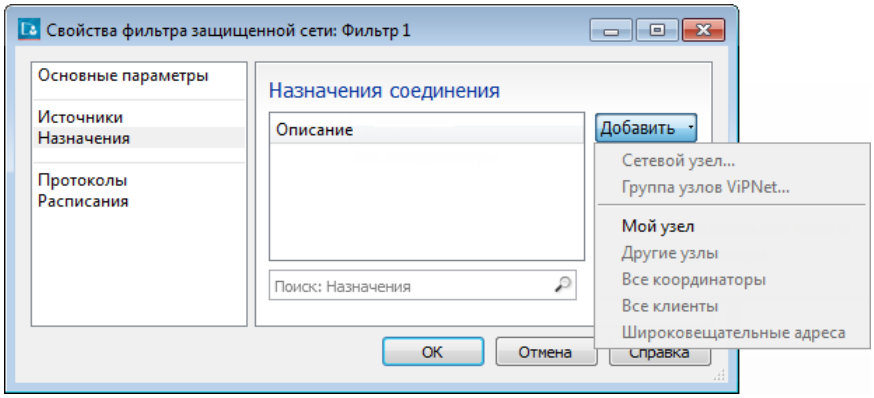


Рисунок 62. Задание получателя защищённых IP-пакетов

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

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

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

Создание фильтров для открытой сети

Чтобы создать фильтр для локального открытого трафика (см. Общие сведения о сетевых фильтрах), выполните следующие действия:

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

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

3 В разделе **Основные параметры** укажите имя фильтра и его действие: блокировать или пропускать трафик.

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

- IP-адрес или DNS-имя отправителя либо диапазон адресов, если их несколько (см. Добавление IP-адресов и DNS-имён).
- Группы IP-адресов отправителей, если такие созданы (см. Создание и изменение групп объектов).
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для исходящих открытых соединений вашего узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для входящих открытых соединений вашего узла.

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

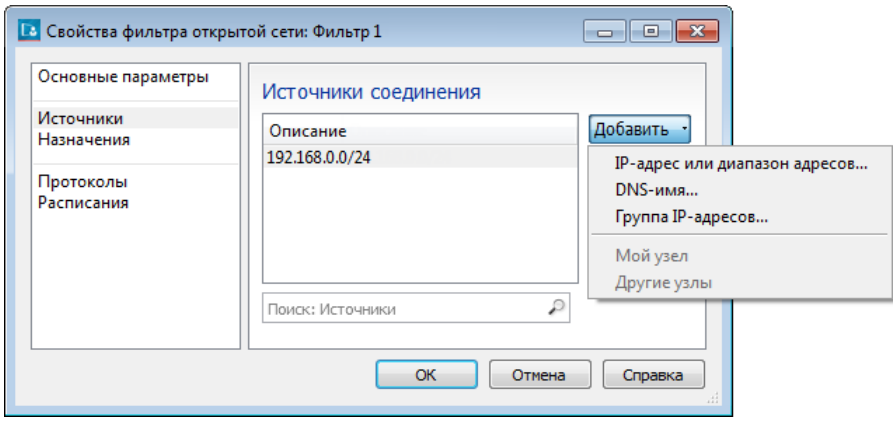


Рисунок 63. Указание источника отправки IP-пакетов в открытой сети

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

- IP-адрес или DNS-имя получателя либо диапазон адресов, если их несколько.
- Группы IP-адресов получателей, если такие созданы.
- Системную группу объектов **Мой узел**. В этом случае фильтр будет действовать для входящих открытых соединений вашего узла.
- Системную группу объектов **Другие узлы**. В этом случае фильтр будет действовать для исходящих открытых соединений вашего узла.
- Широковещательные адреса, выбрав системную группу объектов **Широковещательные адреса**. В этом случае действие фильтра будет распространяться на широковещательные пакеты.
- Системную группу объектов **Групповые адреса**. В этом случае действие фильтра будет распространяться на пакеты, отправленные по групповой рассылке.

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

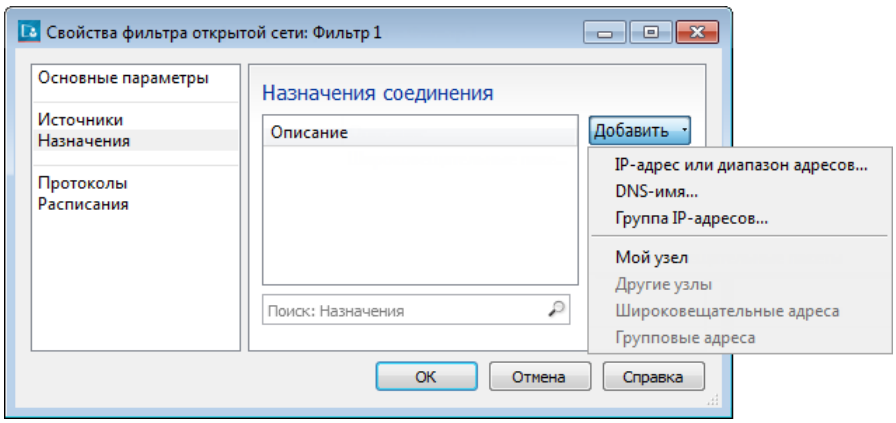


Рисунок 64. Указание получателя IP-пакетов в открытой сети

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

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

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

Создание фильтров прикладного уровня

Примечание. Фильтры прикладного уровня не предназначены для фильтрации трафика на веб-сервере.

Если настройка фильтров заблокирована, установите модуль расширенной фильтрации:

1. В меню **Пуск** выберите **ViPNet** > **Настройка компонентов ViPNet Client**.
2. Выберите **Изменить состав** и нажмите **Далее**.
3. Выберите **Модуль расширенной фильтрации.**.

Анализ трафика фильтрами открытой сети происходит на уровне заголовка IP-пакета. Это позволяет провести быстрый отсев нежелательного трафика по выбранным адресам, протоколам и портам. Фильтры прикладного уровня открытой сети анализируют тело IP-пакета. Это позволяет блокировать трафик на более высоком уровне, в зависимости от его содержания. При этом быстродействие фильтров прикладного уровня ниже, чем фильтров открытой сети. Включённые фильтры прикладного уровня могут замедлить работу в интернете.

Для эффективной обработки трафика рекомендуется создавать фильтры прикладного уровня только в том случае, когда нужно фильтровать содержимое IP-пакетов. Например, запретить запуск динамических веб-сценариев или открытие файлов определённого типа. Если требуется провести фильтрацию трафика только по прикладному протоколу, следует пользоваться фильтрами открытой сети (см. Создание фильтров для открытой сети).

Чтобы создать фильтр прикладного уровня:

1. Выберите раздел **Сетевые фильтры** > **Фильтры прикладного уровня открытой сети**.
2. На панели просмотра нажмите **Создать** и укажите параметры нового фильтра.

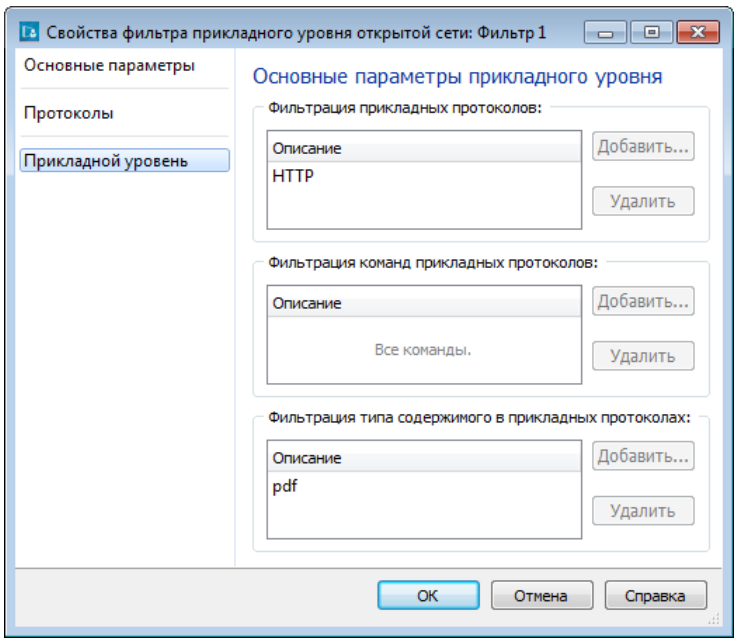


Рисунок 65. Задание параметров фильтрации прикладного уровня

3 В разделе **Основные параметры** укажите имя фильтра.

4 В разделе **Протоколы** укажите порт и протокол для фильтрации.

5 В разделе **Прикладной уровень** укажите команду или тип содержимого, который необходимо блокировать. В одном фильтре вы можете задать только один параметр для фильтрации.

6 Нажмите **OK**. В списке на панели просмотра появится новый фильтр.

Рекомендации по созданию сетевых фильтров

Чтобы обеспечить стабильную работу ПО ViPNet, необходимо контролировать число создаваемых фильтров, потому что оно зависит от количества узлов, на которые будет распространяться действие каждого из фильтров. Рекомендуется придерживаться следующих ограничений:

- Если действие каждого из создаваемых фильтров распространяется на один сетевой узел или IP-адрес, общее количество фильтров не должно превышать 3000.
- Если действие каждого из создаваемых фильтров распространяется на два или большее количество сетевых узлов или IP-адресов, общее количество сетевых узлов или IP-адресов, на которые будут распространяться действия всех созданных фильтров, не должно превышать 700. При этом действие одного фильтра не должно распространяться более чем на 500 сетевых узлов или IP-адресов.

Восстановление предустановленных фильтров и групп объектов

Если вы создали неудачный список сетевых фильтров, то вы можете восстановить предустановленные фильтры. В этом случае списки настроенных фильтров всех типов будут заменены на предустановленные. Вместе с фильтрами также будут восстановлены предустановленные группы объектов.

Для восстановления предустановленных фильтров и групп объектов выполните следующие действия:

1. В окне программы ViPNet Client на панели навигации выберите раздел **Сетевые фильтры**.
2. На панели просмотра нажмите **Восстановить фильтры по умолчанию**.
3. В появившемся окне **Сброс фильтров** нажмите **Да**.

   В результате во всех разделах сетевых фильтров в группе **Настраиваемые фильтры** будут присутствовать только предустановленные фильтры, в разделе **Группы объектов** — только предустановленные группы.

Практический пример использования групп объектов и сетевых фильтров

Рассмотрим следующий пример использования групп объектов и сетевых фильтров. Допустим, в организации развернут почтовый сервер, на котором установлена программа ViPNet Client. Этот защищённый почтовый сервер выполняет следующие функции:

- Обмен сообщениями электронной почты с внешними почтовыми серверами;
- Передача сообщений электронной почты, отправленных удалёнными сотрудниками или адресованных им.

Отправка сообщений на почтовый сервер внешними почтовыми серверами и пользователями осуществляется по протоколу SMTP. Передача сообщений электронной почты пользователям производится по протоколам POP3 и IMAP.

Чтобы организовать обмен сообщениями с внешними почтовыми серверами и пользователями и доступ пользователей к электронной почте из Интернета, на защищённом почтовом сервере необходимо создать сетевой фильтр, разрешающий приём и передачу IP-пакетов по 25-му порту протокола TCP (стандартный порт для протокола SMTP), а также по 110-му и 143-му порту (для протоколов POP3 и IMAP соответственно).

Вы можете создать группу протоколов, в которую будут входить все указанные выше протоколы. Данную группу вы сможете использовать при создании сетевого фильтра. Кроме этого, вы сможете использовать её повторно в дополнительных фильтрах для почтового сервера, если такие в дальнейшем потребуется создать.

Чтобы создать группу протоколов, выполните следующие действия:

1. В окне программы ViPNet Client на панели навигации выберите раздел **Группы объектов** > **Протоколы**.
2. На панели просмотра нажмите **Создать** и в окне свойств создаваемой группы в разделе **Состав** добавьте все нужные протоколы.
   - **2.1** Для добавления протокола SMTP в меню кнопки **Добавить** выберите **Протокол TCP/UDP**, после чего в появившемся окне укажите:
     - в качестве протокола — **TCP**;
     - в качестве порта источника — **Все порты**;
     - в качестве порта назначения — номер порта **25-smtp**.

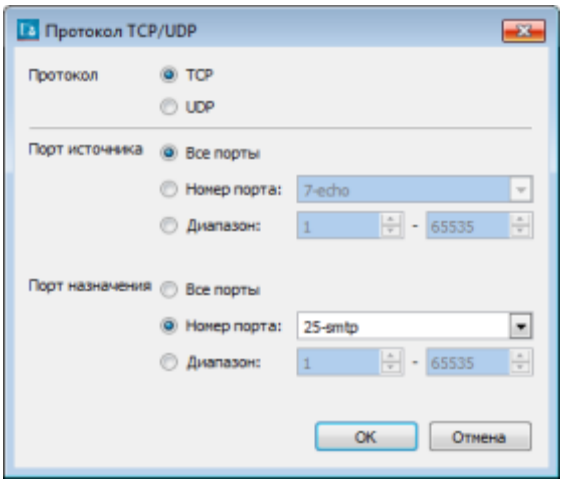


Рисунок 66. Пример добавления протокола SMTP в группу

2.2 Аналогичным образом добавьте протоколы POP3 и IMAP, указав вместо порта назначения номер порта 110 и 143 соответственно.

2.3 По завершении добавления протоколов в окне свойств группы нажмите **OK**.

В результате будет создана группа протоколов. Используйте данную группу при создании фильтра.

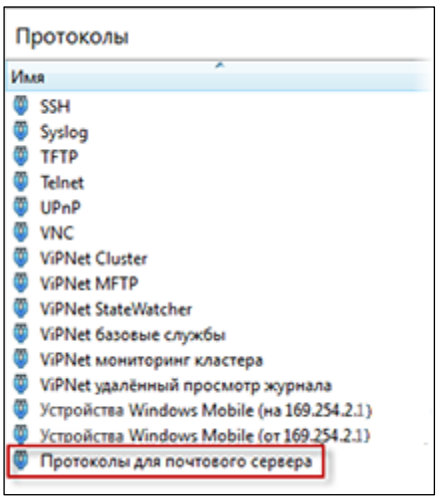


Рисунок 67. Результат создания группы протоколов для почтового сервера

Чтобы создать сетевой фильтр для обмена почтовыми сообщениями с внешними серверами и пользователями, на защищённом почтовом сервере выполните следующие действия:

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

2 В разделе **Фильтры открытой сети** создайте сетевой фильтр для всех IP-адресов, так как IP-адреса внешних почтовых серверов заранее неизвестны и создаваемый фильтр должен распространяться на IP-адреса всех пользователей. Для этого на панели просмотра нажмите **Создать** и в появившемся окне свойств создаваемого фильтра задайте его параметры.

3 В разделе **Основные параметры** установите переключатель **Действие** в положение **Пропускать трафик**.

4 Чтобы действие фильтра распространялось на все IP-адреса, в разделах **Источники** и **Назначения** не задавайте отправителей и получателей соответственно.

5 В разделе **Протоколы** в меню кнопки **Добавить** выберите **Группа протоколов**, после чего в появившемся окне выберите группу протоколов, которая была создана предварительно.

6 Расписание для данного фильтра формировать не следует.

7 Нажмите **OK**.

В результате будет создан сетевой фильтр.

Таким образом, на защищённом почтовом сервере будет разрешён обмен сообщениями с внешними серверами и сотрудниками организации и доступ сотрудников к электронной почте.

Рисунок 68. Результат создания разрешающего фильтра для протоколов SMTP, POP3, IMAP

Блокировка IP-трафика

С помощью программы ViPNet Client вы можете заблокировать весь IP-трафик компьютера. В этом случае любые соединения с защищёнными и открытыми узлами будут запрещены.

Чтобы заблокировать IP-трафик, выполните следующие действия:

1. В программе ViPNet Client включите блокировку одним из следующих способов:
   - В меню **Файл** выберите **Конфигурации** > **Блокировать IP-трафик**.
   - На панели задач щёлкните правой кнопкой мыши значок программы и в меню выберите **Блокировать IP-трафик**.
2. Если вы хотите, чтобы после блокировки трафика при определённых условиях трафик был автоматически разблокирован, в окне **Блокирование IP-трафика**:
   - Установите флажок **Разрешить IP-трафик автоматически**.
   - Из списка под флажком выберите условие для автоматической разблокировки IP-трафика: после перезагрузки компьютера или по истечении определённого промежутка времени.

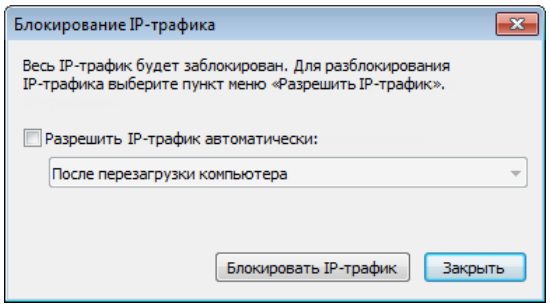


Рисунок 69. Включение блокировки IP-трафика

3. Нажмите **Блокировать IP-трафик**. Весь открытый и защищённый трафик компьютера будет заблокирован, значок программы ViPNet Client в области уведомлений примет вид .
4. Чтобы снять блокировку IP-трафика, выполните одно из следующих действий:
   - В меню **Файл** выберите **Конфигурации** > **Разрешить IP-трафик**.
   - На панели задач щёлкните правой кнопкой мыши значок программы и в меню выберите **Разрешить IP-трафик**.

Примечание. Для повышения уровня безопасности вашего компьютера настройте автоматическую блокировку трафика при обнаружении угроз.

Отключение защиты трафика

При необходимости вы можете отключить защиту трафика с помощью программного обеспечения ViPNet Client. В этом случае будет прекращена любая обработка трафика и ведение журнала регистрации IP-пакетов. Соединение с защищёнными узлами ViPNet будет невозможно.

Внимание! Не следует работать на сетевом узле с отключённой защитой трафика, так как в этом случае компьютер не защищён от попыток несанкционированного доступа из сети.

Чтобы отключить защиту трафика:

1. В меню **Файл** выберите **Конфигурации** > **Отключить защиту**.
2. Чтобы после отключения защиты трафика, она включалась автоматически, в окне **Отключение защиты**:
   - Установите флажок **Включить защиту IP-трафика автоматически**.
   - Из списка под флажком выберите условие для автоматического включения защиты трафика: после перезагрузки компьютера или по истечении определённого промежутка времени.

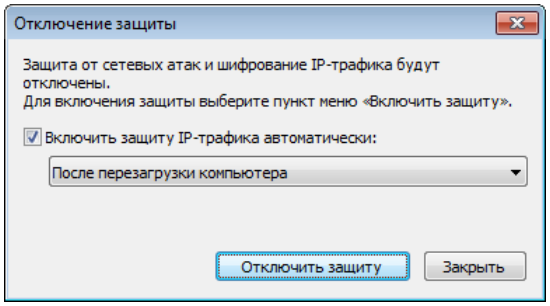


Рисунок 70. Отключение защиты трафика

3. Нажмите **Отключить защиту**. Защита трафика будет отключена, значок программы ViPNet Client в области уведомлений примет следующий вид .
4. Чтобы включить защиту трафика, в меню **Файл** выберите **Конфигурации** > **Включить защиту**.

Настройка параметров блокировки трафика

Чтобы разрешить трафик по любым протоколам (например, если требуется установить соединение по протоколу PPPoE):

1 В меню **Сервис** выберите **Настройка приложения**.

2 В разделе **Управление трафиком** снимите флажок **Блокировать все протоколы, кроме IP, ARP**.

По умолчанию флажок установлен, что обеспечивает высокую сетевую безопасность.

Внимание! Трафик IPv6 не обрабатывается сетевыми фильтрами ViPNet. Поэтому когда флажок снят, этот трафик пропускается без фильтрации. Также разрешение имён корпоративных ресурсов может выполняться по протоколу IPv6 на публичных серверах, даже если в ЦУСе отключена такая возможность. Это означает, что сетевой узел не будет надёжно защищён и может подвергнуться DNS-спуфингу.

8

Обработка прикладных протоколов

Общие сведения о прикладных протоколах

Прикладные протоколы обеспечивают работу пользовательских сетевых сервисов, например, IP-телефонии, DNS-службы, FTP-службы. При использовании данных служб IP-адреса часто передаются в теле IP-пакета. Эта особенность может повлиять на доступность сервисов в защищённой сети с виртуальной адресацией. Кроме того, некоторые прикладные протоколы, помимо управляющего соединения, открывают для передачи данных дополнительные соединения на случайно выбранный порт. Поскольку номер порта заранее неизвестен, то для IP-пакетов невозможно создать разрешающий сетевой фильтр, следовательно, соединение будет заблокировано.

ViPNet Client может выполнять роль шлюза прикладного уровня, которая позволяет решить перечисленные проблемы, обеспечивая:

- Подмену виртуального IP-адреса защищённого узла в теле IP-пакета на реальный.
- Включение разрешающего сетевого фильтра для соединения через случайный порт, который используется прикладным протоколом.

Примечание. В программе ViPNet Client обработка прикладных протоколов выполняется для открытого и защищённого трафика.

Обработка прикладных протоколов не предполагает автоматического разрешения на установление управляющего соединения с открытыми узлами. Установление управляющего соединения с открытыми узлами выполняется в соответствии с фильтрами трафика (см. Общие сведения о сетевых фильтрах).

Обработка протокола FTP

При передаче файлов между клиентом и сервером по протоколу FTP устанавливается как минимум два TCP-соединения:

- для отправки команд на сервер и получения ответов от него (управляющее TCP-соединение);
- для передачи данных (дополнительное TCP-соединение).

Установление TCP-соединений по протоколу FTP происходит в следующем порядке:

1. Клиент создаёт управляющее TCP-соединение с сервером со своего порта из диапазона 1024-65535 на 21-й порт сервера.
2. В зависимости от выбранного режима передачи данных, клиент отправляет по управляющему соединению:
   - номер порта, открытого клиентом для получения данных с сервера (активный режим);

- запрос на номер порта сервера, к которому будет подключаться клиент (пассивный режим).

3 В зависимости от используемого режима передачи данных, соединение устанавливается одним из двух способов:

- сервер создаёт дополнительное соединение для передачи данных на указанный клиентом порт (активный режим);
- сервер по управляющему соединению передаёт клиенту номер порта, к которому клиент создаёт дополнительное соединение (пассивный режим).

Таким образом, в активном режиме соединение для передачи данных создаёт сервер, а в пассивном — клиент.

Для разрешения соединений по протоколу FTP:

- Если действуют предустановленные фильтры открытой сети, которые разрешают любые исходящие соединения, то для исходящего управляющего соединения дополнительные настройки не требуются.
- В ином случае создайте фильтр открытой сети (см. Создание фильтров для открытой сети), разрешающий исходящее соединение по протоколу TCP на 21 порт FTP-сервера.
- Для разрешения дополнительного соединения в активном режиме работы включите обработку протокола FTP, которая добавляет необходимый сетевой фильтр.
- Для разрешения дополнительного соединения в пассивном режиме работы настройки не требуются.

Обработка протокола SIP

Протокол SIP предназначен для организации сеансов связи (мультимедийных конференций, телефонных соединений) и распределения мультимедийной информации.

SIP-клиент отправляет запрос (например, приглашение для начала сеанса связи, подтверждение приёма ответа на запрос, завершение сеанса связи) другому SIP-клиенту с указанием его SIP-адреса. В зависимости от способа установления соединения запрос направляется второму клиенту либо напрямую, либо с участием прокси-сервера SIP, либо с участием сервера переадресации. Вызываемый клиент передаёт вызывающему клиенту ответ на запрос (например, информацию об успешной обработке запроса, отклонении вызова, ошибке при обработке запроса).

Для организации сеанса связи протокол SIP регламентирует установление соединений TCP и UDP через порт 5060.

Чтобы установить сеанс связи между SIP-клиентами, убедитесь, что включена обработка протокола SIP, и выполните дополнительные настройки в программе ViPNet Client:

1 Чтобы SIP-клиент мог принять запрос на установление сеанса связи или принять ответ на запрос, создайте фильтр открытой сети, разрешающий входящее соединение по протоколам TCP и UDP на порт 5060.

2 Чтобы SIP-клиент мог отправить запрос на установление сеанса связи или ответ на запрос:

- Если действуют предустановленные фильтры открытой сети, которые разрешают любые исходящие соединения, настройка дополнительных фильтров не требуется.
- Если фильтры открытой сети не разрешают любые исходящие соединения, создайте фильтр открытой сети, разрешающий исходящее соединение по протоколам TCP и UDP на порт 5060.

Описание прикладных протоколов

Вы можете настроить обработку следующих прикладных протоколов:

- Протокол FTP обеспечивает передачу файлов между FTP-клиентом и FTP-сервером.
- Протокол DNS (Domain Name System) обеспечивает разрешение DNS-имён сетевых узлов в IP-адреса.
- Протокол H.323 обеспечивает работу программ для проведения мультимедийных конференций через IP-сети, в том числе Интернет.
- Протокол SCCP (Skinny Client Control Protocol) обеспечивает передачу сообщений между Skinny-клиентами (проводными и беспроводными IP-телефонами Cisco) и сервером голосовой почты Cisco Unity и Cisco CallManager.
- Протокол SIP (Session Initiation Protocol) обеспечивает установление сеансов связи при передаче голосовых звонков, видеоконференций, а также мультимедийной информации.

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

Настройка параметров обработки прикладных протоколов

Внимание! В сетях, где используется обработка прикладных протоколов средствами ViPNet, на сетевом оборудовании (маршрутизаторах, шлюзах) необходимо отключить функцию DPI (deep packet inspection — глубокий анализ пакетов). Применение DPI может привести к сбоям в работе приложений, использующих протоколы FTP, DNS, H.323, SCCP, SIP.

Чтобы настроить параметры обработки прикладных протоколов для открытого и защищённого трафика:

1 В меню **Сервис** выберите **Настройка приложения**.

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

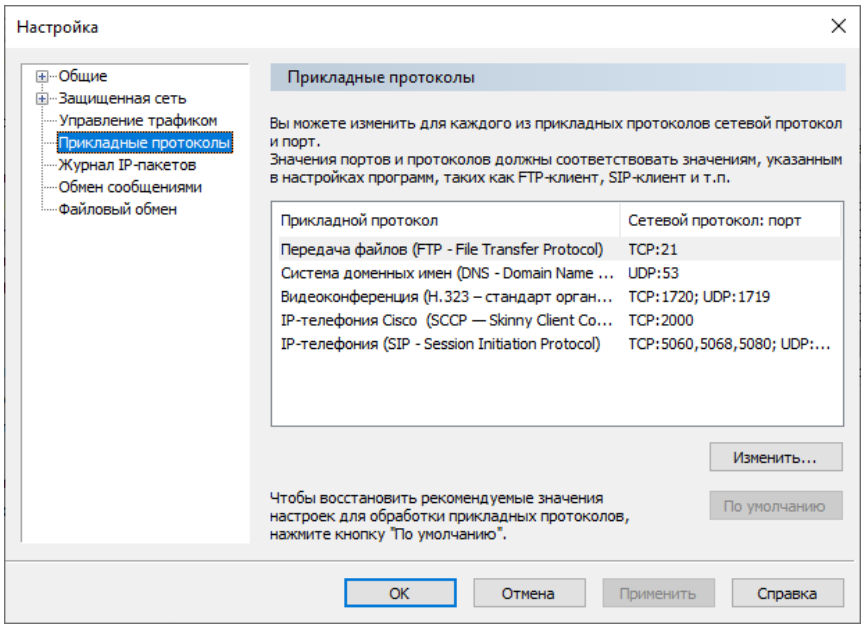


Рисунок 71. Раздел «Прикладные протоколы»

В разделе **Прикладные протоколы** приведён список поддерживаемых программой прикладных протоколов.

Примечание. По умолчанию для всех прикладных протоколов заданы наиболее часто используемые сетевые протоколы и порты.

Список поддерживаемых программой ViPNet Client 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 **Изменить**.

4 В окне **Настройка прикладного протокола** укажите сетевые протоколы и порты.

Заданные параметры должны соответствовать параметрам, указанным в настройках различных приложений, таких как FTP-клиент, DNS-клиент, SIP-клиент и других.

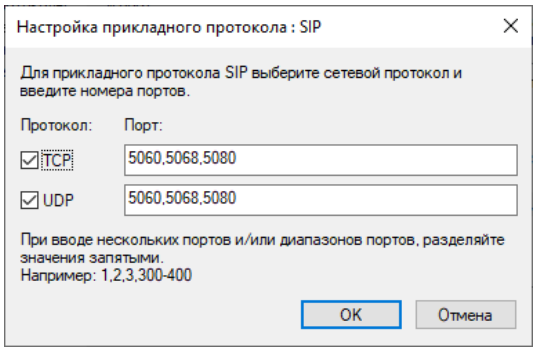


Рисунок 72. Настройка параметров обработки прикладного протокола

Внимание! Не отключайте обработку прикладных протоколов, иначе прикладные программы могут работать неправильно.

5 В окне **Настройка** нажмите **Применить**.

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

9

Встроенные средства коммуникации

Общие сведения

В состав программы ViPNet Client входит несколько дополнительных инструментов, предоставляющих возможность быстрого и защищённого обмена информацией:

- Обмен защищёнными сообщениями, защищённая конференция (см. Обмен защищёнными сообщениями).
- Быстрая отправка электронных писем (см. Отправка писем программы ViPNet Деловая почта).
- Файловый обмен.
- Вызов программы удалённого доступа (см. Удалённая работа на сетевом узле).
- Доступ к веб-ресурсу сетевого узла. (см. Просмотр веб-ресурсов сетевого узла)
- Доступ к общим ресурсам сетевого узла. (см. Обзор общих ресурсов сетевого узла)
- Проверка соединения с другим сетевым узлом ViPNet (см. Проверка соединения с сетевым узлом).

Обмен защищёнными сообщениями

Пользователи сети ViPNet могут в режиме реального времени обмениваться мгновенными сообщениями с другими пользователями ViPNet или участвовать в конференции с несколькими пользователями:

- Вы можете начать сеанс обмена сообщениями, чтобы отправлять сообщения одному или нескольким пользователям одновременно и получать от них ответы. При этом все участники сеанса будут получать ваши сообщения, но не будут получать ответные сообщения от других пользователей.

  Чтобы начать сеанс обмена сообщениями, в окне программы ViPNet Client на панели навигации выберите раздел **Защищённая сеть**, затем на панели просмотра выберите один или несколько сетевых узлов. В контекстном меню узлов выберите **Послать сообщение** или на панели инструментов нажмите **Сообщение**  .

- Вы можете начать конференцию с несколькими пользователями, чтобы все участники сеанса могли получать сообщения от других пользователей и отвечать на них. В этом заключается отличие конференции от сеанса обмена сообщениями.

  Чтобы начать конференцию, в окне программы ViPNet Client на панели навигации выберите раздел **Защищённая сеть**, затем на панели просмотра выберите несколько сетевых узлов. В контекстном меню узлов выберите **Конференция** или на панели инструментов нажмите **Конференция**  (по умолчанию эта кнопка скрыта).

Пользователь ViPNet может участвовать в нескольких сеансах обмена сообщениями одновременно. Если получено сообщение, которое не относится ни к одному из текущих сеансов, будет открыт новый сеанс обмена сообщениями.

Все сообщения, полученные и отправленные в течение сеанса, записываются в протокол сеанса. Если в рамках сеанса отправить сообщение какому-либо пользователю, его ответ придёт в том же сеансе и будет сохранен в том же протоколе. При необходимости вы можете сохранить протокол сеанса как текстовый файл.

Во время сеанса обмена сообщениями вы можете отправлять пользователям файлы и письма (см. Отправка файлов и писем из программы обмена защищёнными сообщениями).

Примечание. Если на вашем сетевом узле обмен сообщениями недоступен, обратитесь к администратору сети ViPNet с просьбой разрешить обмен сообщениями.

Интерфейс программы обмена защищёнными сообщениями

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

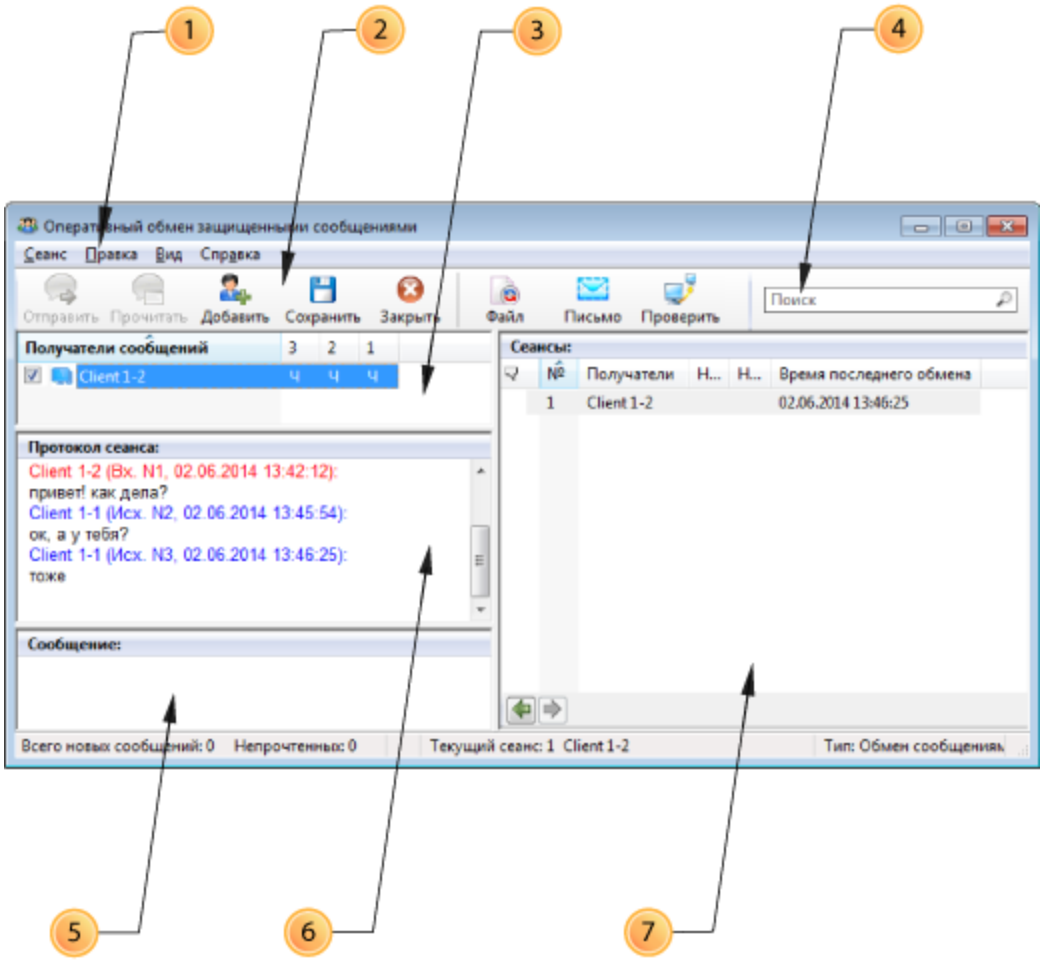


Рисунок 73. Окно обмена защищёнными сообщениями

Цифрами на рисунке обозначены:

1. Главное меню программы обмена защищёнными сообщениями.
2. Панель инструментов.
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 ещё не доставлено.
   - Д — сообщение доставлено, на экране получателя появилось уведомление о сообщении.
   - Ч — сообщение прочитано получателем.
   - П — сообщение было прочитано, получатель собирается ответить.

Сообщения пронумерованы в порядке их отправки. Колонки со статусами отправленных сообщений расположены в обратном порядке (начиная с последнего отправленного сообщения). Сообщения отправляются пользователям, рядом с именами которых установлены флажки.

4 Строка поиска, предназначенная для фильтрации списка получателей на панели **Сеансы** и для поиска слов в сообщениях на панели **Протокол сеанса**. В протоколе сеанса все вхождения заданной строки поиска отмечаются жёлтым фоном.

5 Панель **Сообщение**. Предназначена для ввода новых сообщений.

6 Панель **Протокол сеанса**. На этой панели отображается история сообщений (протокол) текущего сеанса.

7 Панель **Сеансы**. Содержит список открытых сеансов и кнопки перехода между сеансами. Описание колонок на панели **Сеансы** приведено в следующей таблице:

Колонка	Описание
	Статус сеанса: Значки отсутствуют. Сеанс открыт, все сообщения были обработаны. Сеанс открыт, получены новые сообщения. Сеанс закрыт инициатором, однако в сеансе есть непрочитанные сообщения (этот значок отображается, только если сеанс инициирован другим пользователем). Сеанс закрыт инициатором (этот значок отображается, только если сеанс инициирован другим пользователем).
№	Номер сеанса.
Получатели	Список участников сеанса.
Новых	Число новых (необработанных) сообщений. Если новых сообщений нет, это поле пусто.
Не прочитано	Число непрочитанных сообщений. Если непрочитанных сообщений нет, это поле пусто. Если в сеансе есть непрочитанные сообщения, атрибуты этого сеанса выделены полужирным шрифтом.
Время последнего обмена	Дата и время последнего сообщения сеанса.

Под списком открытых сеансов расположены кнопки  и  , с помощью которых можно перейти к предыдущему или к следующему просмотренному сеансу. В истории переходов между сеансами запоминается 10 последних сеансов, просмотр которых продолжался более 5 секунд.

Отправка сообщений

Для обмена мгновенными сообщениями выполните следующие действия:

1 Если окно **Оперативный обмен защищёнными сообщениями** закрыто, чтобы открыть его, в меню программы ViPNet Client выберите **Приложения** > **Обмен сообщениями**. В окне обмена сообщениями будут открыты все начатые ранее сеансы.

2 Чтобы начать новый сеанс обмена сообщениями или конференцию, в окне **Оперативный обмен защищёнными сообщениями** выполните следующие действия:

- В меню **Сеанс** выберите **Новый**, а затем щёлкните **Обмен сообщениями** или **Конференция**.
- В окне **Выбор сетевого узла** укажите узлы, с пользователями которых вы хотите начать обмен сообщениями или конференцию. Затем нажмите **Выбрать**.

Откроется новый сеанс обмена сообщениями. Если вы указали единственный сетевой узел, с которым сеанс обмена сообщениями уже был начат, то вместо нового сеанса откроется существующий сеанс.

Примечание. Чтобы начать новый сеанс обмена сообщениями или конференцию, вы также можете выбрать сетевые узлы в разделе **Защищённая сеть** и в контекстном меню узлов вызвать пункт **Послать сообщение**.

3 В окне **Оперативный обмен защищёнными сообщениями** выберите сеанс, в который вы хотите отправить новые сообщения.

4 На панели **Сообщение** введите текст сообщения.

5 Нажмите **Отправить** или клавишу **F5**.

Совет. В настройках программы обмена сообщениями можно выбрать, какое действие выполняется по нажатию клавиши **Enter** на панели **Сообщение**: отправка сообщения или переход на новую строку. Для этого в программе ViPNet Client в меню **Сервис** выберите **Настройка приложения**, откроется окно **Настройка**. В разделе **Обмен сообщениями** в группе **Назначить горячие клавиши** выберите **Ctrl+Enter: отправка сообщения, Enter: перевод строки** или наоборот.

Приём сообщений

По умолчанию при поступлении новых сообщений в области уведомлений появляется значок , текст сообщения отображается во всплывающем окне над областью уведомлений. Чтобы прочитать новые сообщения, выполните одно из действий:

- Щёлкните значок в области уведомлений.
- В окне **Оперативный обмен защищёнными сообщениями** на панели инструментов нажмите **Прочитать** .

Вы можете изменить способ уведомления о новом сообщении. Для этого выполните следующие действия:

1. В окне программы ViPNet Client в меню **Сервис** выберите **Настройка приложения**.
2. В окне **Настройка** в разделе **Обмен сообщениями** установите или снимите следующие флажки:
   - **Уведомлять о приходе сообщения полупрозрачным окном**.
   - **Уведомлять о приходе сообщения миганием кнопки на панели задач**.
   - **Уведомлять о приходе сообщения окном поверх всех окон**.
   - **Показывать новые сообщения в отдельном окне**.

     Если флажок **Показывать новые сообщения в отдельном окне** установлен, при получении сообщений откроется окно **Новые сообщения**.

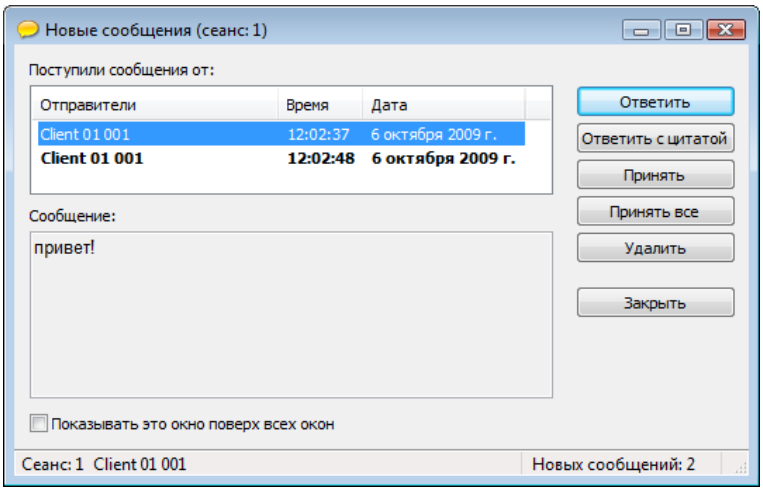


Рисунок 74. Новые сообщения в отдельном окне

В окне **Новые сообщения** отображается список новых сообщений в порядке поступления. С помощью кнопок в правой части окна вы можете принять сообщение (тогда оно будет сохранено в протоколе сеанса), ответить на сообщение или удалить его.

Отправка файлов и писем из программы обмена защищёнными сообщениями

Во время сеанса обмена сообщениями вы можете отправлять участникам сеанса файлы и письма по защищённому каналу VPN. Для этого используйте кнопки **Файл** и **Письмо**, расположенные на панели инструментов.

Отправка файлов осуществляется с помощью приложения «Файловый обмен» (см. Отправка файлов из программы обмена защищёнными сообщениями).

Отправка писем возможна, только если вашему сетевому узлу назначена роль «Деловая почта» и на нем установлена программа ViPNet Деловая почта. Чтобы отправить письмо, выполните следующие действия:

1 В окне **Оперативный обмен защищёнными сообщениями** на панели **Сеансы** выберите сеанс, участникам которого вы хотите отправить письмо.

2 На панели **Получатели сообщений** выберите участников и на панели инструментов нажмите **Письмо**  .

В результате будет запущена программа ViPNet Деловая почта и появится окно создания нового письма, в котором в качестве получателей будут указаны выбранные участники сеанса. Подробнее о том, как создать и отправить письмо, см. документ «ViPNet Деловая почта. Руководство пользователя».

Примечание. В список получателей нового письма будут включены только участники сеанса с ролью «Деловая почта», у которых установлена программа ViPNet Деловая почта. Если таких участников нет среди выбранных, то отправить письмо будет невозможно.

Прекращение обмена сообщениями

Чтобы закрыть сеанс обмена сообщениями:

1 В окне **Оперативный обмен защищёнными сообщениями** на панели **Сеансы** выберите сеанс.

2 Если вы хотите сохранить протокол сеанса в виде текстового файла, щёлкните сеанс правой кнопкой мыши и в контекстном меню выберите **Сохранить как**, затем укажите файл для сохранения протокола.

3 Выполните одно из действий:

- В меню **Сеанс** выберите **Закрыть**.
- Нажмите клавишу **F8**.
- На панели инструментов нажмите **Закрыть**  .

4 После закрытия сеанс будет удалён с панели **Сеансы**.

Чтобы закрыть программу обмена защищёнными сообщениями, выполните одно из действий:

- В меню **Сеанс** выберите **Выход**.
- Нажмите **Закрыть**  .

Примечание. При повторном открытии окна **Оперативный обмен защищёнными сообщениями** все текущие сеансы будут восстановлены.

Отправка писем программы ViPNet Деловая почта

В состав программного обеспечения ViPNet Client входит программа ViPNet Деловая почта, которая позволяет обмениваться электронными письмами в защищённой сети VPN. Если вашему сетевому узлу назначена роль «Деловая почта» и на нем установлена программа ViPNet Деловая почта, вы можете отправлять письма непосредственно из программы ViPNet Client. Для этого выполните следующие действия:

1. В окне программы ViPNet Client на панели навигации выберите раздел **Защищённая сеть**.
2. В разделе **Защищённая сеть** выберите сетевой узел, на который требуется отправить письмо. Чтобы выбрать несколько сетевых узлов, зажмите клавишу **Ctrl** и по очереди щёлкните нужные узлы. Чтобы отфильтровать список сетевых узлов, воспользуйтесь строкой поиска в нижней части раздела **Защищённая сеть**.
3. Выполните одно из действий:
   - Нажмите **Письмо**  на панели инструментов.
   - Щёлкните сетевой узел правой кнопкой мыши и в контекстном меню выберите **Отправить письмо**.

   В результате будет запущена программа ViPNet Деловая почта и появится окно создания нового письма, в котором в качестве получателей будут указаны выбранные сетевые узлы. Подробнее о том, как создать и отправить письмо, см. документ «ViPNet Деловая почта. Руководство пользователя».

Примечание. В список получателей нового письма будут включены только сетевые узлы с ролью «Деловая почта», у которых установлена программа ViPNet Деловая почта. Если таких узлов нет среди выбранных, то отправить письмо будет невозможно.

Файловый обмен

С помощью приложения «Файловый обмен» пользователи сети ViPNet могут пересылать друг другу файлы по защищённому каналу VPN. Размер файла для отправки не должен превышать 2 Гб, отправка файлов с расширениями dll и exe ограничена. Для отправки таких файлов поместите их в архив. Кроме этого обеспечивается контроль их целостности. Если целостность файла при передаче была нарушена, то данный файл автоматически удаляется.

Примечание. Для файлов, полученных от пользователей, у которых установлено ПО ViPNet версии 3.2 и ниже, проверка целостности не выполняется. В окне **Файловый обмен** для таких файлов указан статус **Целостность не подтверждена**. Решение об использовании такого файла принимается на усмотрение пользователя.

Приложение «Файловый обмен» вы можете вызвать из программы ViPNet Client, из контекстного меню Windows или из программы обмена защищёнными сообщениями.

Примечание. Если на вашем сетевом узле файловый обмен недоступен, обратитесь к администратору сети ViPNet с просьбой разрешить файловый обмен.

Интерфейс программы «Файловый обмен»

Для просмотра принятых и отправленных файлов в программе ViPNet Client выберите меню **Приложения** > **Файловый обмен**. Также окно «Файловый обмен» появляется каждый раз при отправке или приёме файлов.

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

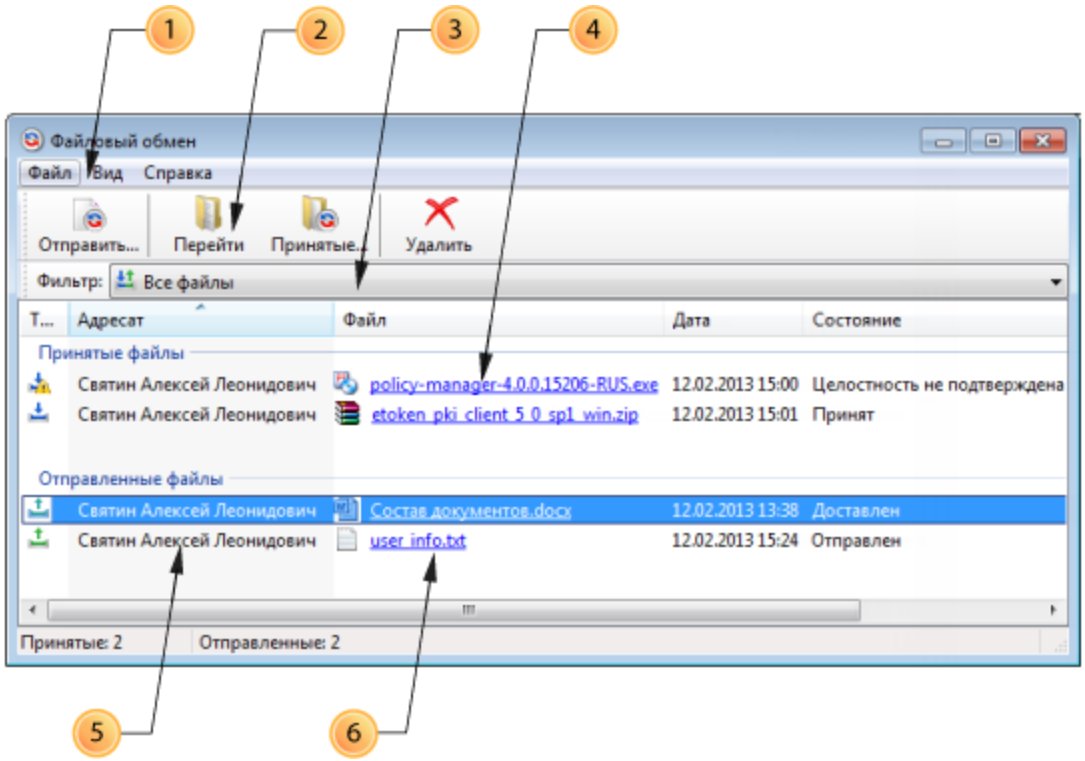


Рисунок 75. Окно файлового обмена

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.
3. Фильтр списка файлов. Предусмотрено три режима отображения списка:
   - Все файлы.
   - Принятые файлы.
   - Отправленные файлы.
4. Группа **Принятые файлы**. В этой группе отображаются файлы, полученные от пользователей других сетевых узлов ViPNet.
5. Группа **Отправленные файлы**. В этой группе отображаются файлы, переданные пользователям других сетевых узлов ViPNet.
6. Ссылка для перехода в папку, в которой находится файл.

Отправка файлов из программы ViPNet Client

Примечание. Размер файла для отправки по защищённому каналу не должен превышать 2 Гб.

1 В программе ViPNet Client на панели навигации выберите раздел **Защищённая сеть**.

2 На панели просмотра выберите один или несколько узлов, удерживая клавишу **Ctrl**. Чтобы отобразить только узлы, содержащие определённые символы, воспользуйтесь строкой поиска в нижней части раздела **Защищённая сеть**.

3 Выполните одно из действий:

- Нажмите **Отправить** на панели инструментов.
- Щёлкните сетевой узел правой кнопкой мыши и выберите **Отправить файл**.

4 Выберите файлы и нажмите **Открыть**.

Выбранные файлы будут отправлены адресату.

5 Откроется окно **Файловый обмен**, в котором отображается информация об отправленных файлах и их состоянии.

6 Когда отправленные файлы будут доставлены получателю, появится уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

Примечание. Для настройки уведомлений в окне программы ViPNet Client в меню **Сервис** выберите **Настройка приложения** > **Файловый обмен**.

Отправка файлов из программы обмена защищёнными сообщениями

1 В окне **Оперативный обмен защищёнными сообщениями** на панели **Сеансы** выберите сеанс, участникам которого вы хотите отправить файл.

2 На панели **Получатели сообщений** выберите участников и на панели инструментов нажмите **Файл**.

3 В появившемся окне укажите файлы, которые требуется отправить, и нажмите **Открыть**.

Выбранные файлы будут отправлены участникам сеанса.

4 Откроется окно **Файловый обмен**, в котором отображается информация об отправленных файлах и их состоянии.

5 Когда отправленные файлы будут доставлены получателям, программа выдаст уведомление о доставке. Чтобы отключить уведомления, в окне сообщения установите флажок **Не показывать это сообщение в дальнейшем**.

Примечание. Для настройки уведомлений в окне программы ViPNet Client в меню **Сервис** выберите **Настройка приложения** > **Файловый обмен**.

Приём файлов

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

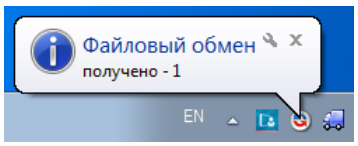


Рисунок 76. Уведомление о принятом файле

Примечание. Для настройки уведомлений в окне программы ViPNet Client в меню **Сервис** выберите **Настройка приложения** и перейдите к разделу **Файловый обмен**.

---

2 Чтобы просмотреть полученные файлы, щёлкните значок файлового обмена в области уведомлений. Откроется окно **Файловый обмен**.

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

- Щёлкните имя файла в столбце **Файл**.
- Нажмите **Принятые** на панели инструментов.

В новом окне будет открыта папка, содержащая выбранный файл.

Чтобы просмотреть файлы, полученные от определённого пользователя сети ViPNet:

1 В окне программы ViPNet Client на панели навигации выберите раздел **Защищённая сеть**.

2 В разделе **Защищённая сеть** выберите сетевой узел, от пользователя которого были приняты файлы, и нажмите **Принятые** на панели инструментов.

В новом окне будет открыта папка, содержащая файлы, поступившие с выбранного сетевого узла.

Примечание. Если в разделе **Защищённая сеть** выбрать несколько сетевых узлов и нажать **Принятые**, откроется папка, содержащая подпапки с файлами, которые были получены от разных пользователей ViPNet.

Вызов внешних приложений

Программа ViPNet Client поддерживает вызов внешних приложений для удалённого доступа к другому узлу: VNC Viewer, Remote Desktop Connection, Radmin Viewer. Подробнее о работе с этими программами см. раздел Запуск программы удалённого доступа (см. Удалённая).

Преимущество работы с внешними программами в сети ViPNet состоит в том, что весь трафик этих программ защищён криптографическими методами.

Для взаимодействия с другим пользователем ViPNet с помощью внешнего приложения:

1. В программе ViPNet Client на панели навигации выберите раздел **Защищённая сеть**.
2. На панели просмотра щёлкните сетевой узел правой кнопкой мыши, выберите **Внешние программы** и затем нужную программу.

   Внешняя программа будет автоматически запущена в защищённом 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 с ViPNet Client установлен веб-сервер или веб-приложение, то другие пользователи сети ViPNet могут соединиться с ним по защищённому каналу. При этом доступ к веб-серверу возможен только для тех пользователей сети ViPNet, которым администратор сети разрешил данное соединение.

Это позволяет реализовать защищённый интернет-портал, в который могут быть интегрированы различные приложения — CRM, CMS, базы данных и многое другое.

Чтобы установить такое соединение:

1. В окне программы ViPNet Client на панели навигации выберите раздел **Защищённая сеть**.
2. На панели просмотра выберите сетевой узел, на котором организован защищённый веб-портал, и выполните одно из действий:
   - Нажмите **Веб-ресурс**  на панели инструментов.
   - Щёлкните выбранный узел правой кнопкой мыши и в контекстном меню выберите **Web-ссылка**.

Примечание. Если вы хотите открыть веб-портал на сетевом узле, который является ПАК ViPNet Coordinator HW, ViPNet Coordinator VA или на котором установлено ПО ViPNet Coordinator for Linux, то для доступа к веб-интерфейсу координатора с ним будет установлено соединение по TCP-порту 8080 (например, 10.0.2.8:8080). Для всех остальных узлов веб-порталы будут открываться по TCP-порту 80.

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 защищённом режиме.

Чтобы открыть общий ресурс сетевого узла ViPNet:

1. В окне программы ViPNet Client на панели навигации выберите раздел **Защищённая сеть**.
2. В разделе **Защищённая сеть** выберите нужный сетевой узел и выполните одно из действий:
   - Нажмите **Обзор**  на панели инструментов.
   - Щёлкните выбранный узел правой кнопкой мыши и в контекстном меню выберите **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

В ViPNet Client можно проверить доступность и активность пользователей сетевых узлов ViPNet. Это может понадобиться, когда необходимо удостовериться, что пользователь находится на своём рабочем месте, а на рабочем месте отсутствующего пользователя нет активности. Для проверки соединения с сетевым узлом необходимо, чтобы этот узел имел версию ПО ViPNet не ниже 3.x.

1 В ViPNet Client на панели навигации выберите раздел **Защищённая сеть**.

2 На панели просмотра выберите сетевой узел, соединение с которым требуется проверить. Чтобы выбрать несколько сетевых узлов, зажмите клавишу **Ctrl** и щёлкните нужные узлы.

3 Выполните одно из действий:

- Нажмите **Проверить** на панели инструментов.
- Нажмите **F5**.
- Щёлкните один из выбранных сетевых узлов правой кнопкой мыши и выберите **Проверить соединение**.

Откроется окно **Проверка соединения**, содержащее информацию о выбранных сетевых узлах.

Внешний вид окна **Проверка соединения** представлен на следующем рисунке:

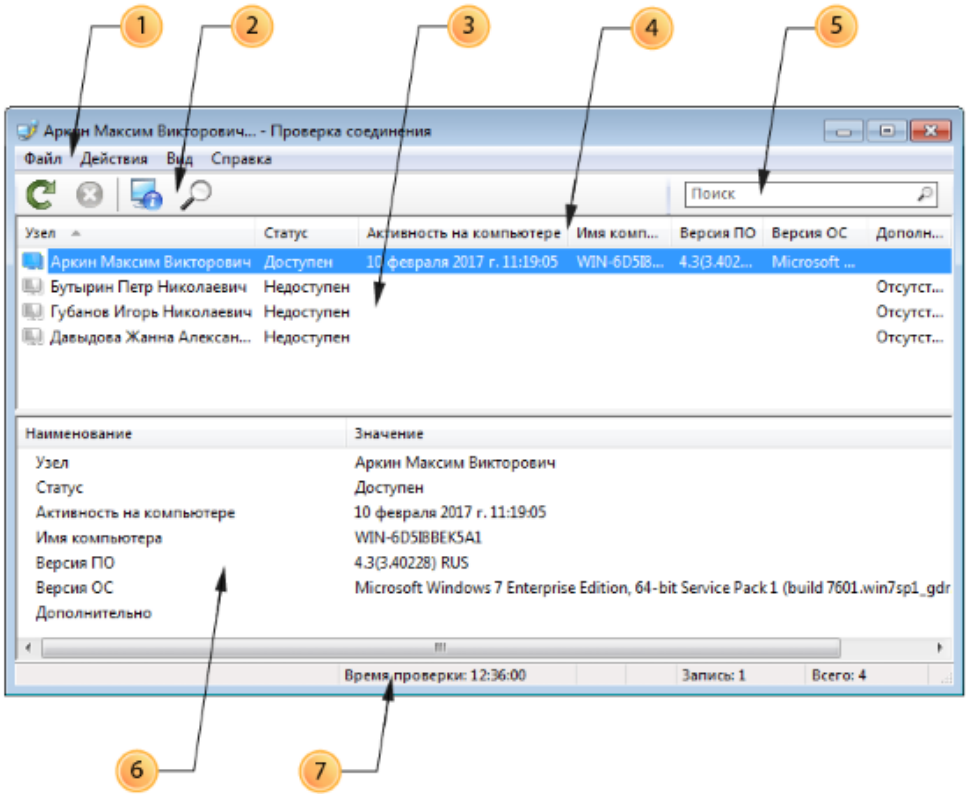


Рисунок 77. Окно проверки соединения

Цифрами на рисунке обозначены:

1 Главное меню программы проверки соединения.

2 Панель инструментов.

3 Основная панель. Содержит список сетевых узлов, с которыми выполняется проверка соединения.

Цвет и цветовое выделение (фон) имени сетевого узла обозначают его текущее состояние:

Цвет имени	Состояние сетевого узла
Фиолетовый	Сетевой узел доступен, но последние 15 минут пользователь не проявлял активности на компьютере.
Чёрный на зелёном фоне	Сетевой узел доступен, и пользователь проявлял активность за последние 15 минут
Чёрный	Сетевой узел в данный момент не подключён к сети.

- Чтобы посмотреть подробную информацию о сетевом узле в отдельном окне, выполните одно из действий:
  - Дважды щёлкните нужный сетевой узел.
  - Выберите сетевой узел из списка и нажмите **Свойства** на панели инструментов.
  - Выберите сетевой узел из списка и нажмите клавишу **F3**.

  Откроется окно **Свойства узла**.

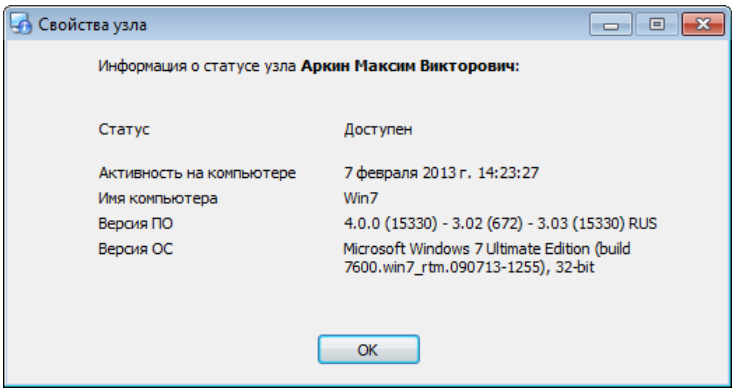


Рисунок 78. Подробная информация о статусе сетевого узла

- Чтобы отправить на один из сетевых узлов в окне **Проверка соединения** письмо программы ViPNet Деловая почта, начать сеанс обмена защищёнными сообщениями или выполнить другое действие, доступное в разделе **Защищённая сеть**, щёлкните выбранный узел правой кнопкой мыши и в контекстном меню выберите соответствующий пункт.

4 Столбцы основной панели. Статус сетевых узлов указан в столбце **Статус**. Описание возможных статусов приведено в таблице ниже.

Статус	Описание
Доступен	Есть полноценная связь с сетевым узлом.
Связь по VPN есть, но модуль управления ViPNet не доступен	На сетевом узле ПО ViPNet работает некорректно, защищённая связь с узлом будет прервана при любых обновлениях в сети.
Недоступен	Связь с сетевым узлом отсутствует.

В столбце **Активность на компьютере** указано время последней активности.

Чтобы отсортировать список по одному из столбцов, щёлкните 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.

10

Административные функции

Работа с журналом IP-пакетов

В разделе **Журнал IP-пакетов** на основе различных параметров поиска можно сформировать отчёт о зарегистрированных программой IP-пакетах. Такие отчёты позволяют контролировать все входящие и исходящие соединения компьютера.

Настройка параметров поиска IP-пакетов

Для просмотра журнала IP-пакетов:

1 Выберите раздел **Статистика и журналы** > **Журнал IP-пакетов**.

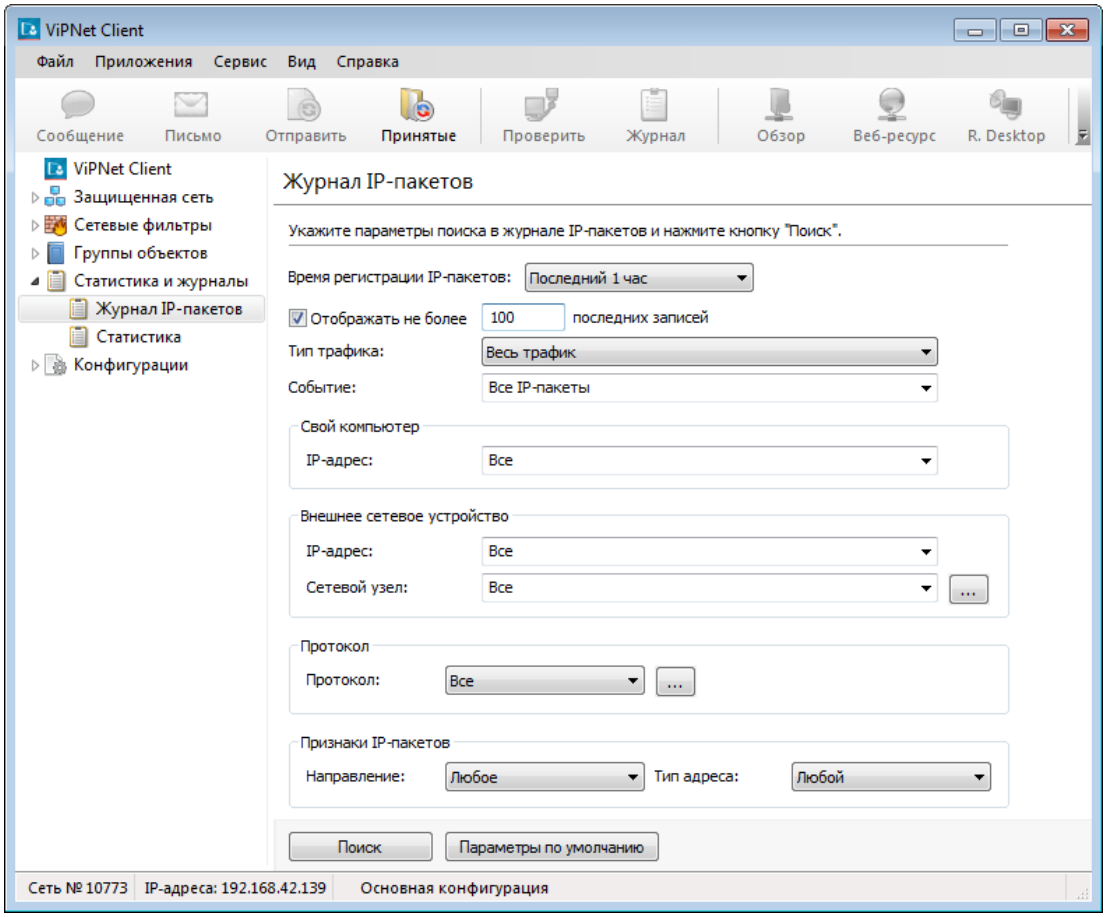


Рисунок 79. Настройка параметров поиска по журналу IP-пакетов

2 В разделе **Журнал IP-пакетов** задайте следующие параметры поиска:

- **Время регистрации IP-пакетов**, если требуется ограничить результат поиска определённым временным интервалом.
- **Число 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** укажите, какие из IP-пакетов нужно отобразить: зашифрованные, незашифрованные или все.
- В списке **Событие** укажите для поиска определённый тип или группу типов событий, которые ViPNet Client сопоставляет каждому IP-пакету (см. События, отслеживаемые ПО ViPNet).
- 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  и добавьте его в окне **Список протоколов**.
- В группе **Признаки IP-пакетов** укажите направление передачи IP-пакетов и на какой тип адреса они отправлялись.
- Чтобы восстановить начальные параметры поиска, нажмите **Параметры по умолчанию**.

3 Задайте параметры поиска и нажмите **Поиск**.

Примечание. Если выполнить поиск с параметрами по умолчанию, в отчёте будет показано не более 100 записей об IP-пакетах, зарегистрированных за последний час.

Просмотр результатов поиска

Результаты поиска пакетов с указанными параметрами будут отображены в окне **Журнал регистрации IP-пакетов**.

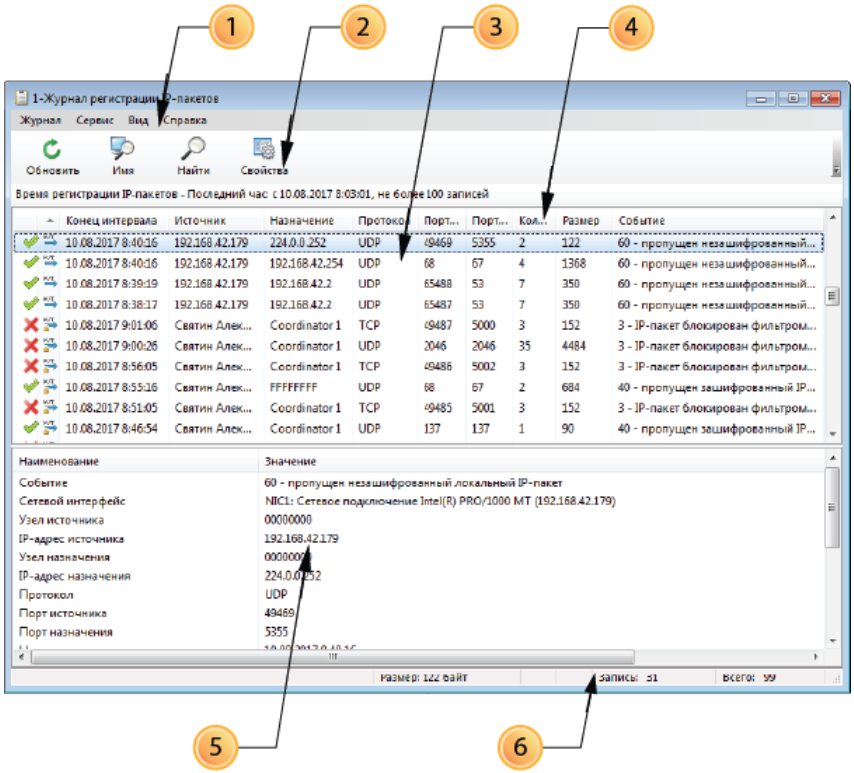


Рисунок 80. Просмотр журнала IP-пакетов

Цифрами на рисунке обозначены:

1 Главное меню.

2 Панель инструментов.

3 Основная панель. Содержит список записей журнала, соответствующих заданным параметрам поиска.

- Чтобы просмотреть подробную информацию о выбранном IP-пакете в отдельном окне, нажмите **Свойства** на панели инструментов окна **Журнал регистрации IP-пакетов**.
- Чтобы найти имя компьютера-отправителя или получателя выбранного пакета, нажмите **Определить имя компьютера** на панели инструментов или щёлкните запись о пакете правой кнопкой мыши и в контекстном меню выберите **Определить имя компьютера**.

4 Столбцы основной панели.

Чтобы отсортировать список по одному из столбцов, щёлкните заголовок столбца. По умолчанию отображаются не все столбцы. Чтобы удалить или добавить столбцы щёлкните правой кнопкой мыши по любому заголовку столбца и нажмите **Выбрать столбцы**.

Описание столбцов приведено в таблице ниже.

Таблица 3. Описание столбцов основной панели

Название столбца	Описание
Тип события	Типы событий обозначаются следующими значками: — IP-пакеты заблокированы. — IP-пакеты пропущены. — IP-пакеты относятся к служебным событиям.
Свойства пакета	Свойства IP-пакетов обозначаются следующими значками: — открытые входящие IP-пакеты. — открытые исходящие IP-пакеты. — зашифрованные входящие IP-пакеты. — зашифрованные исходящие IP-пакеты.
Начало интервала	Дата и время создания записи для группы однотипных IP-пакетов (регистрация первого пакета). Подробнее о регистрации однотипных пакетов в течение определённого интервала времени можно узнать в разделе Настройка параметров регистрации IP-пакетов в журнале.
Конец интервала	Конец интервала регистрации группы однотипных IP-пакетов. Если на данный момент интервал ещё 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 защищённых узлов ViPNet) или IP-адрес (для открытых узлов) отправителя пакета.
Узел источника	Имя сетевого узла отправителя пакета (только для защищённых узлов). Если пакет отправлен открытым узлом, этот столбец будет пустым.
IP-адрес источника	IP-адрес (если определился) отправителя пакета.
Порт источника	Номер порта отправителя пакета.
Назначение	Имя сетевого узла (для защищённых узлов ViPNet) или IP-адрес (для открытых узлов) получателя пакета.
Узел назначения	Имя сетевого узла получателя (только для защищённых узлов). Если пакет предназначен для открытого узла, этот столбец будет пустым.
IP-адрес назначения	IP-адрес (если определился) 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.

Название столбца	Описание
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**). По умолчанию панель скрыта. Чтобы показать, выберите **Вид** > **Свойства IP-пакетов**.

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** щёлкните меню **Журнал**, а затем выберите один из пунктов:

- **Просмотр в веб-браузере.** Таблица с результатами поиска будет открыта в вашем веб-браузере. В строке адреса будет указан путь к файлу отчёта.
- **Просмотр в Excel.** Таблица с результатами поиска будет открыта в приложении Microsoft Excel (для этого приложение должно быть установлено на компьютере). Чтобы сохранить эту таблицу, в Microsoft Excel воспользуйтесь командой **Сохранить как**.

Выбор IP-пакетов

Чтобы выделить IP-пакеты по одному из признаков:

1 В окне **Журнал регистрации IP-пакетов** щёлкните запись журнала правой кнопкой мыши.

2 В контекстном меню выберите:

- **Выделить по IP-адресам**, чтобы выделить все записи IP-пакетов, имеющих те же IP-адреса, что выбранный пакет, вне зависимости от направления пакета и порта соединения.
- **Выделить сессию**, чтобы выделить все записи IP-пакетов, относящихся к сессии выбранного пакета.

- **Выделить широковещательные**, чтобы выделить записи широковещательных пакетов.
- **Выделить групповые**, чтобы выделить все записи IP-пакетов, относящихся к групповой рассылке.
- **Выделить служебные**, чтобы выделить записи служебных событий.

3 Чтобы снять выделение, в контекстном меню выберите **Отменить выделение**.

Примечание. Под сессией подразумеваются все IP-пакеты, передаваемые между узлом 1 и узлом 2. Если 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.

Подсчёт объёма трафика

С помощью журнала IP-пакетов можно подсчитать общий размер IP-пакетов, удовлетворяющих критериям поиска. Для этого:

1 В окне **Журнал регистрации IP-пакетов** в основной панели выделите интересующие вас записи журнала.

Чтобы выделить все IP-пакеты, показанные в журнале, воспользуйтесь комбинацией клавиш **Ctrl+A**.

2 В строке состояния отобразится суммарный размер выделенных IP-пакетов.

Рекомендации по анализу открытых (незашифрованных) и зашифрованных соединений

Для удобства анализа открытых соединений в журнале IP-пакетов:

1 Щёлкните правой кнопкой мыши по любому из заголовков столбцов и выберите **Выбрать столбцы**.

2 Для анализа открытых (незашифрованных) соединений:

- настройте отображение столбцов: **IP-адрес источника**, **IP-адрес назначения**.
- скройте столбцы: **Источник**, **Узел источника**, **Назначение**, **Узел назначения**.

3 Для анализа закрытых (зашифрованных) соединений:

- настройте отображение столбцов: **Узел источника**, **Узел назначения**.
- скройте столбцы: **IP-адрес источника**, **IP-адрес назначения**.

Создание сетевого фильтра при просмотре журнала IP-пакетов

Если требуется пропускать IP-пакеты в рамках запрещённых соединений либо блокировать IP-пакеты в рамках разрешённых соединений, вы можете создать сетевой фильтр для таких IP-пакетов при просмотре соединений в журнале IP-пакетов. Для этого выполните следующие действия:

1. В окне **Журнал регистрации IP-пакетов** (см. Просмотр результатов поиска) выберите запись о заблокированном соединении, которое должно быть разрешено, либо разрешённое соединение, которое должно быть заблокировано.
2. Щёлкните выбранную запись правой кнопкой мыши и в контекстном меню выберите **Создать фильтр**.

   В зависимости от типа выбранного соединения появится окно создания:

   - Фильтра открытой сети — если в рамках соединения передавались незашифрованные IP-пакеты.
   - Фильтра защищённой сети — если в рамках соединения передавались зашифрованные IP-пакеты.
3. В разделах окна свойств сетевого фильтра будут автоматически заданы параметры, сформированные из записи выбранного соединения. При необходимости внесите соответствующие изменения (см. Создание сетевых фильтров).
4. В окне свойства сетевого фильтра нажмите **OK**. В результате созданный фильтр появится в списке сетевых фильтров.

Просмотр журнала IP-пакетов другого сетевого узла

При работе в режиме администратора сетевого узла можно запросить журнал IP-пакетов другого сетевого узла ViPNet, с которым у данного узла есть связь. Для этого выполните следующие действия:

1. Выполните вход в программу в режиме администратора (см. Работа в программе в режиме администратора).
2. В окне программы ViPNet Client 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  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 **Отмена**.

Примечание. Запрос журнала IP-пакетов возможен только с сетевого узла, на котором установлено ПО ViPNet версии не ниже 3.x.

Следует иметь в виду, что при просмотре журнала IP-пакетов другого сетевого узла параметры поиска соответствуют типу этого узла. То есть если в программе ViPNet Coordinator запросить журнал IP-пакетов клиента, можно указать только параметры, доступные на клиентах.

5 Задайте параметры поиска (см. Настройка параметров поиска IP-пакетов) и нажмите **Поиск**.

Примечание. Если вы просматриваете журнал координатора, то вместо групп **Свой компьютер** и **Внешнее сетевое устройство** появятся группы **Устройство** <1> и **Устройство** <2>, где вы сможете указать сетевые узлы отправителя и получателя сетевых пакетов.

Чтобы запретить администраторам доверенных сетей просматривать журналы IP-пакетов узлов вашей сети, заблокируйте на узлах вашей сети трафик из доверенных сетей на порт TCP:2047.

Настройка параметров регистрации IP-пакетов в журнале

Чтобы настроить параметры журнала IP-пакетов:

1 В меню **Сервис** выберите **Настройка приложения**.

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

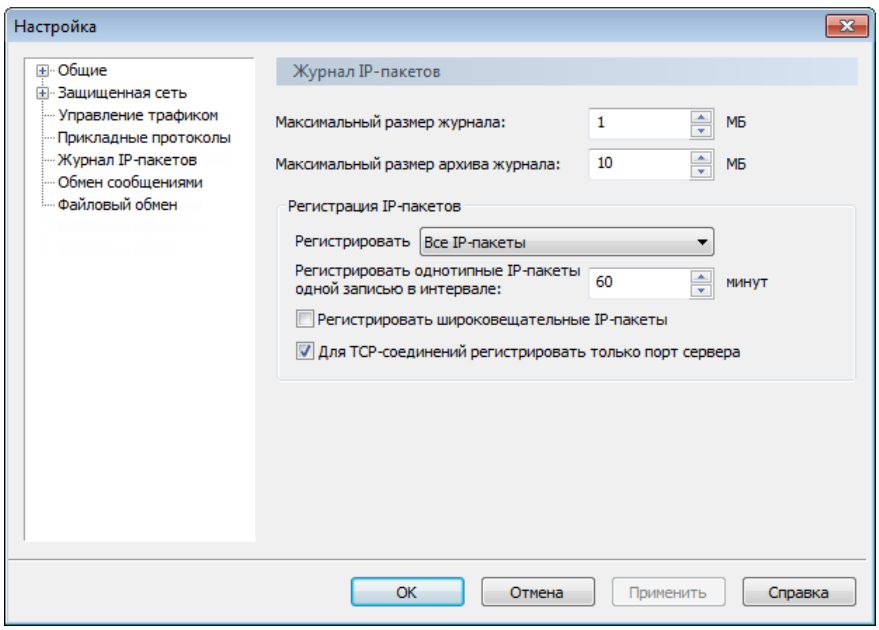


Рисунок 81. Настройка параметров журнала IP-пакетов

3 Задайте значения следующих параметров:

- В поле **Максимальный размер журнала** укажите размер журнала в мегабайтах (по умолчанию — 1 Мбайт). Если размер журнала превысит указанное значение, записи в хронологическом порядке будут переноситься в архив.

  Чтобы отключить ведение журнала, задайте значение 0. Записи о новых зарегистрированных IP-пакетах не будут добавляться в журнал. Однако записи, созданные до присвоения значения 0, будут сохранены.

- С помощью списка **Регистрировать** укажите, какие IP-пакеты следует регистрировать в журнале: **Все IP-пакеты** или **Только блокируемые IP-пакеты**.

- В поле **Регистрировать однотипные IP-пакеты одной записью в интервале** укажите интервал времени в минутах. По истечении указанного интервала для IP-пакетов определённого типа будет создаваться новая запись в журнале.

  Смысл данного параметра состоит в том, что при регистрации пакета с определёнными параметрами (IP-адрес, протокол, порт и так далее) для него создаётся запись в журнале. В течение указанного интервала времени IP-пакеты, которые имеют те же IP-адрес, протокол, порт и другие параметры, регистрируются, но записи в журнале для них не создаются. Число таких пакетов, зарегистрированных в течение интервала, указано в столбце **Количество пакетов** в окне **Журнал регистрации IP-пакетов**.

  Когда заданный интервал времени истекает, для следующего IP-пакета создаётся новая запись в журнале, даже если этот пакет имеет параметры, которые уже зафиксированы в другой записи. Если поступает пакет другого типа, для него также создаётся новая запись в журнале. После создания новой записи снова начинается отсчёт 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, объединённые одной записью, указаны в соответствующих столбцах.

  Данный механизм позволяет сократить размер журнала IP-пакетов, сохранив 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 **Применить**.

Просмотр статистики фильтрации IP-пакетов

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

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

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

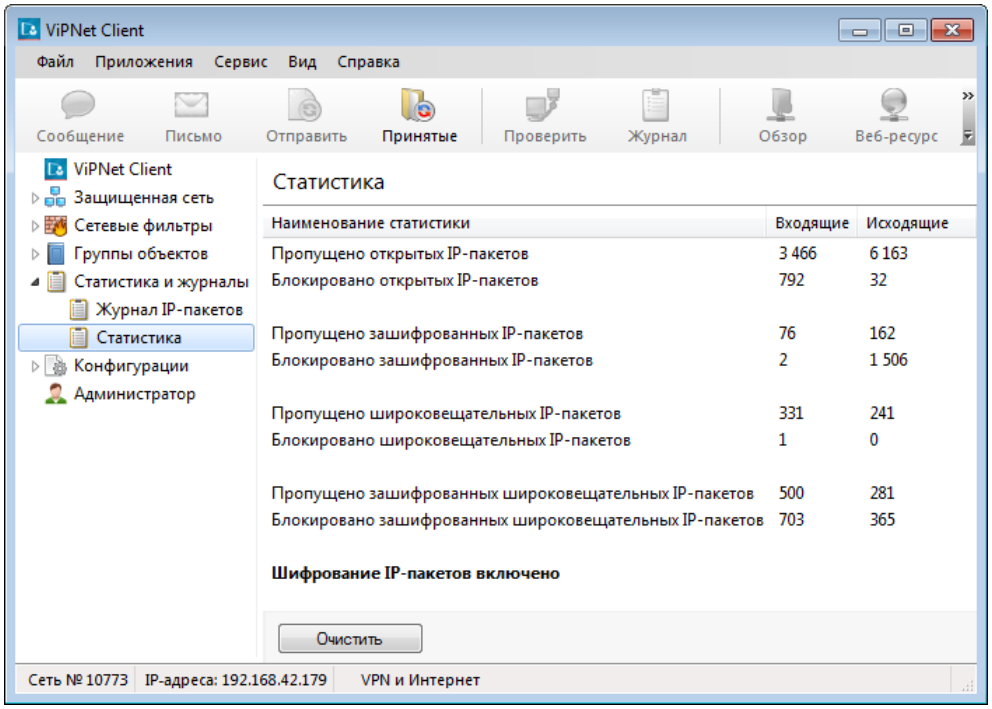


Рисунок 82. Просмотр статистики IP-пакетов

Просмотр информации о клиенте

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

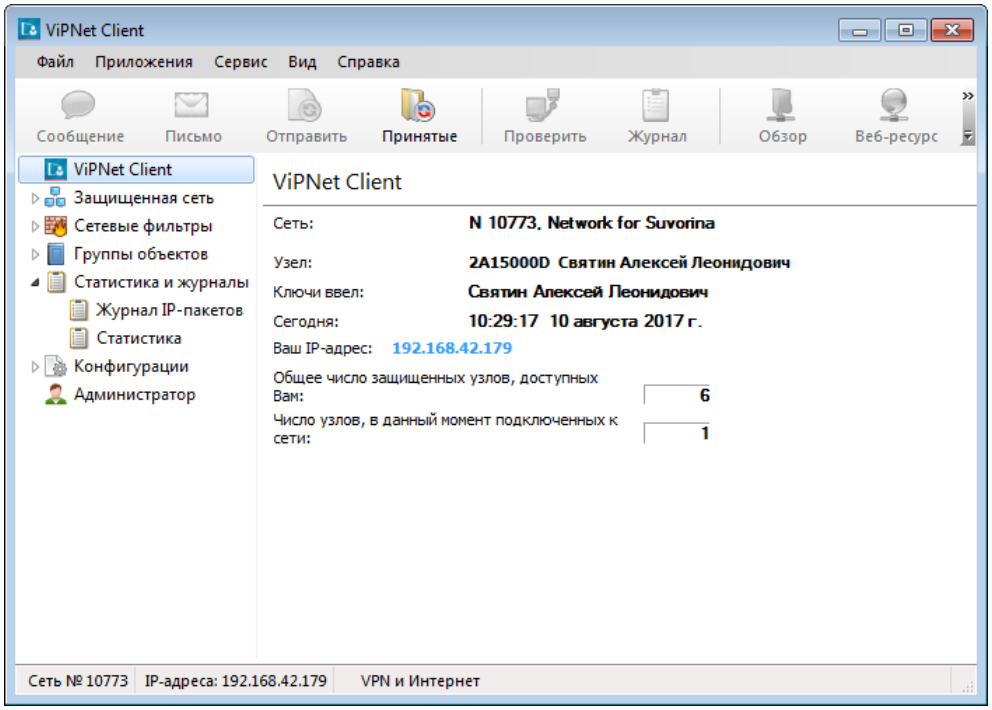


Рисунок 83. Раздел общей информации об узле ViPNet

Управление конфигурациями программы

Конфигурация — это совокупность всех настроек программы ViPNet. В разделе **Конфигурации** можно создать несколько дополнительных конфигураций и установить нужную в любой момент.

Использование нескольких конфигураций может быть полезно в следующих случаях. Предположим, что политика безопасности компании запрещает одновременно работать с локальными ресурсами и ресурсами интернета. Тогда вам следует создать две конфигурации: в одной конфигурации должна быть разрешена работа в интернете и запрещён доступ в локальную сеть, во второй конфигурации должна быть разрешена работа в локальной сети и запрещён доступ в интернет. Либо, например, вам приходится периодически изменять настройки подключения к защищённой сети. Тогда для удобства вы можете создать несколько конфигураций с разными настройками подключения к защищённой сети. В дальнейшем вам не потребуется изменять настройки каждый раз, когда возникнет необходимость. Будет достаточно просто выбрать конфигурацию с нужными настройками.

При первом запуске программы создаётся **Основная конфигурация**, которая содержит настройки по умолчанию. Эту конфигурацию нельзя переименовать, удалить или изменить её параметры. Также могут по умолчанию присутствовать специальные конфигурации, предназначенные для работы в интернете: «Открытый Интернет», «Внутренняя сеть» и «Интернет». Описание данных конфигураций приведено в разделах ниже.

Чтобы создать конфигурацию:

1 На панели навигации выберите **Конфигурации** и в контекстном меню выберите **Создать конфигурацию**.

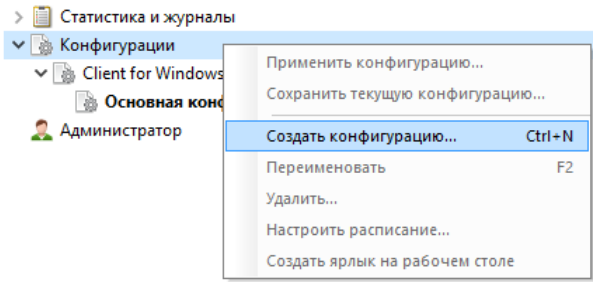


Рисунок 84. Создание новой конфигурации

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

Примечание. В режиме администратора можно создать конфигурацию программы для любого пользователя, зарегистрированного на узле. В данном режиме отображаются все конфигурации, созданные в процессе работы с программой, причём они сгруппированы по пользователям, от имени которых были созданы.

---

2 Выполните настройку программы, добавьте сетевые фильтры, которые нужно применять в данной конфигурации.

   Затем в контекстном меню выберите **Сохранить текущую конфигурацию**.

3 Чтобы переключать конфигурацию с помощью ярлыка, в контекстном меню выберите **Создать ярлык на рабочем столе**.

4 Чтобы сделать активной нужную конфигурацию, выполните одно из действий:

   - Щёлкните конфигурацию правой кнопкой мыши и в контекстном меню выберите **Применить конфигурацию**.
   - В меню **Файл** выберите **Конфигурации**.
   - Щёлкните правой кнопкой мыши по значку  в области уведомлений и выберите **Конфигурации**.
   - Дважды щёлкните по ярлыку конфигурации на рабочем столе (если ярлык был создан).

   В активной конфигурации все изменения программы ViPNet Client сохраняются автоматически.

Если в программе создано несколько конфигураций и при этом в настройках установлен флажок **Вызывать окно выбора конфигурации** (см. Настройка параметров запуска программы ViPNet Client), то при запуске ViPNet Client откроется окно выбора конфигурации.

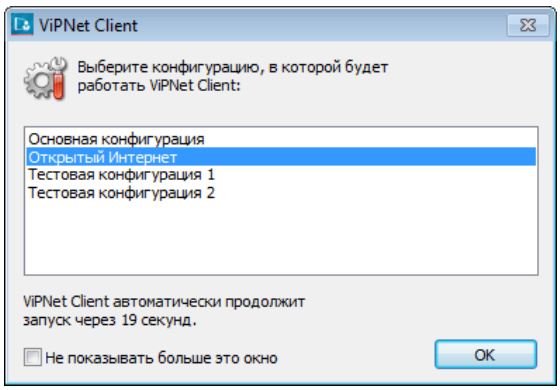


Рисунок 85. Выбор конфигурации при запуске программы

Для того чтобы загрузить одну из этих конфигураций, выберите её в списке и нажмите **OK**.

Если в течение 30 секунд с момента появления окна не будет выбрана ни одна конфигурация, программа ViPNet Client продолжит работу в основной конфигурации.

Если в программе создано несколько конфигураций, которые используются в определённые периоды времени, настройте расписание автоматической смены конфигураций (см. Настройка расписания смены конфигураций программы).

Конфигурация «Открытый интернет»

Примечание. Начиная с версии ПО ViPNet Administrator ЦУС 4.6.3, технология «Открытый Интернет» называется «Защищённый интернет-шлюз».

Если клиент связан с координатором, для которого в программе ViPNet Центр управления сетью включена функция сервера открытого Интернета, в списке конфигураций программы ViPNet Client присутствует конфигурация «Открытый Интернет».

Внимание! Не используйте перемещаемые профили пользователей Windows совместно с конфигурацией «Открытый интернет». При включении этой конфигурации ресурсы корпоративной сети недоступны, соответственно все настройки пользователя в профиле не могут быть загружены.

Если доступ клиентов в Интернет организован через сервер Открытого Интернета:

- Для работы в защищённой 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».

  При загрузке конфигурации «Открытый Интернет» в раздел **Сетевые фильтры** будут автоматически добавлены фильтры трафика, запрещающие соединение с какими-либо сетевыми узлами ViPNet, кроме сервера открытого Интернета.

Таким образом, клиент может быть подключён либо только к защищённой сети ViPNet, либо только к Интернету. Это позволяет изолировать компьютер, обменивающийся потенциально опасным трафиком в Интернете, от остальных узлов сети ViPNet.

Конфигурации «Внутренняя сеть» и «интернет»

Если администратор сети ViPNet в программе ViPNet Центр управления сетью установил для пользователей сетевого узла уровень полномочий «h», в программе ViPNet Client автоматически создаются две конфигурации: «Внутренняя сеть» и «Интернет».

Подробная информация об уровнях полномочий пользователя содержится в документе «Классификация полномочий. Приложение к документации ViPNet».

Конфигурации «Внутренняя сеть» и «Интернет» имеют следующие особенности:

- Конфигурация «Внутренняя сеть» предназначена для работы в защищённой сети ViPNet и запрещает соединения с открытыми узлами.

  При загрузке этой конфигурации в разделе **Фильтры открытой сети** автоматически добавляются фильтры, блокирующие любой открытый IP-трафик, кроме пакетов службы DHCP.

- Конфигурация «Интернет» предназначена для работы в открытой сети и запрещает соединения с защищёнными узлами ViPNet.

При загрузке этой конфигурации в разделе **Фильтры защищённой сети** автоматически добавляются фильтры, блокирующие любой защищённый IP-трафик.

Настройка расписания смены конфигураций программы

Если используется несколько конфигураций, каждая из которых должна устанавливаться в определённое время, вы можете настроить расписание автоматической смены конфигураций. Например, автоматическая смена будет удобна в том случае, если вам периодически в заданное время приходится переключаться в конфигурацию для работы в интернете. В остальных случаях, как правило, рекомендуется менять конфигурации вручную.

Настроить расписание смены конфигураций можно только в том случае, если в программе создано более двух конфигураций. Основная конфигурация и специальные конфигурации при этом не учитываются, расписание их установки настроить нельзя. Основная конфигурация автоматически устанавливается и вступает в действие в те промежутки времени, в которые не действуют по расписанию остальные конфигурации. Специальные конфигурации можно установить только вручную.

Внимание! При пересечении расписаний автоматическая смена конфигураций не гарантируется. В процессе составления расписаний рекомендуется следить за тем, чтобы расписания смены конфигураций не пересекались.

Чтобы настроить расписание смены конфигураций:

1. Щёлкните правой кнопкой мыши раздел **Конфигурации** или любую созданную конфигурацию и в контекстном меню выберите **Настроить расписание**.
2. В окне **Настройка расписания смены конфигураций** установите флажок **Устанавливать конфигурации в соответствии с расписанием**, после чего добавьте в список конфигурации, которые требуется устанавливать автоматически.
3. В окне **Параметры расписания** укажите дни и время действия.

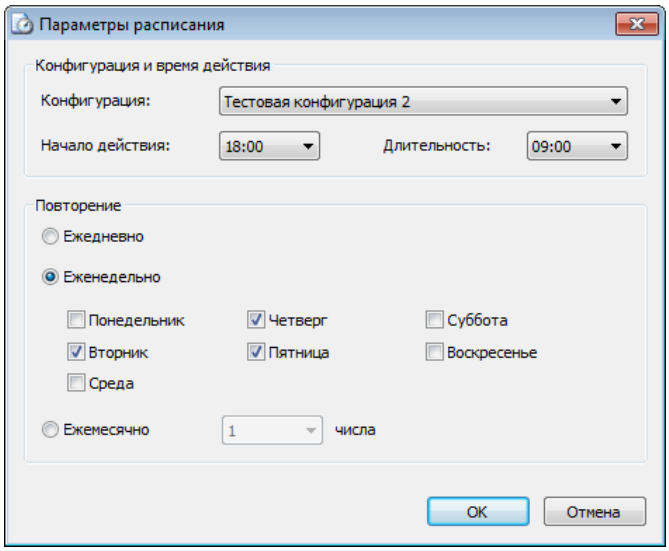


Рисунок 86. Настройка расписания смены конфигураций

4 Нажмите **OK**.

В результате расписание смены конфигураций будет настроено.

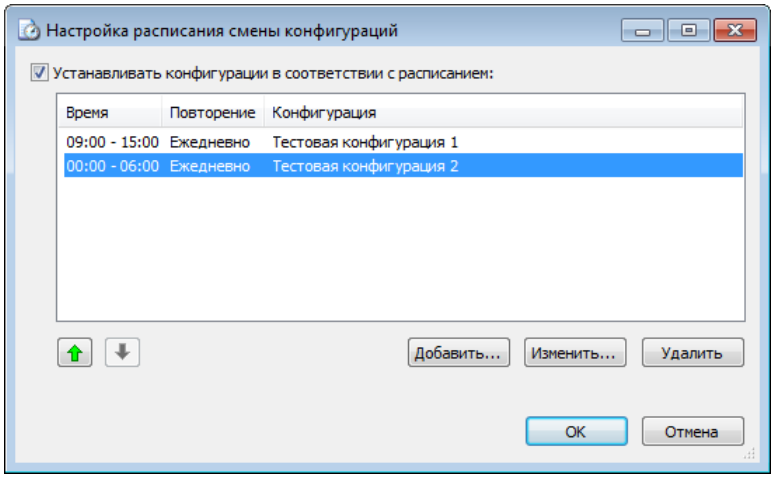


Рисунок 87. Сформированное расписание смены конфигураций

Чтобы отменить расписание, в окне **Настройка расписания смены конфигурации** снимите соответствующий флажок.

Чтобы перед каждой сменой конфигурации по расписанию производилось оповещение, в настройках программы в разделе **Предупреждения** установите флажок **Выдавать предупреждение перед сменой конфигурации по расписанию**.

Централизованная настройка ViPNet Client через ViPNet Policy Manager

Примечание. Приведённая информация предназначена для администратора сети ViPNet.

Централизованное уменьшение MSS

Иногда требуется уменьшить максимальное значение размера сегмента (MSS) протокола TCP. Например, это может потребоваться для правильной работы IP-телефонии, когда наблюдаются проблемы с разрешением DNS-имён.

Эту настройку можно выполнить непосредственно на каждом сетевом узле (см. Настройка подключения к защищённой сети). Если в вашей сети используется ViPNet Policy Manager, то вы можете отправить значение MSS централизованно. Для этого:

1. На компьютере с ViPNet Policy Manager откройте для редактирования файл `options.xml` (по умолчанию расположен в папке `c:\Program Files (x86)\InfoTeCS\ViPNet Policy Manager`).
2. Добавьте новую группу `<op:Groups type="Monitor">`:

```
<op:Groups type="Monitor">
    <op:Container label="Уменьшать максимальный размер сегмента (MSS) протокола TCP на, (байт)" checkable="false">
    <op:SpinOption defaultValue="0" minValue="0" maxValue="200" XMLName="DiminutionMSS" stepValue="1"/>
    </op:Container>
</op:Groups>
```

3. Сохраните изменения в файле и перезапустите ViPNet Policy Manager.
4. Откройте или создайте новый шаблон политики для клиентов, на которые надо отправить настройку MSS.
5. Откройте окно свойств шаблона и в разделе **Опции** нажмите **Добавить**.

   В окне **Опции безопасности** появится новый пункт **Уменьшать максимальный размер сегмента (MSS) протокола TCP на, (байт)**.

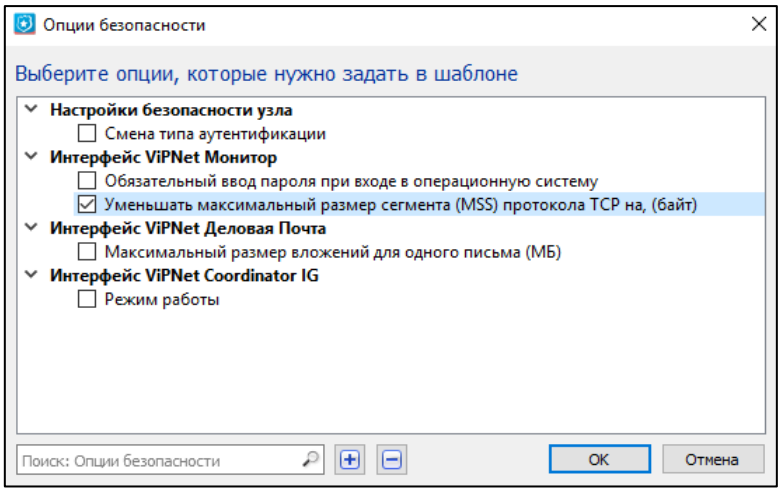


Рисунок 88. Настройка опций в ViPNet Policy Manager

Подробнее об опциях см. документ «ViPNet Policy Manager. Руководство администратора», раздел «Управление настройками программ ViPNet».

6 Назначьте шаблон политики безопасности с этой опцией нужным сетевым узлам и отправьте политику (см. главу «Рассылка политик безопасности на сетевые узлы»).

После применения политики в настройках программы ViPNet Client появится заданный параметр.

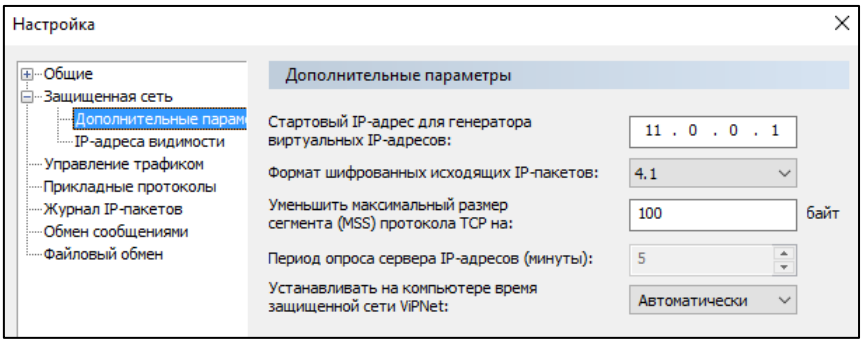


Рисунок 89. Уменьшение MSS в ViPNet Client

Централизованная настройка входа в программу

Иногда требуется разрешить пользователям ViPNet с минимальными полномочиями закрыть окно входа в программу ViPNet Client и войти в Windows. Это необходимо в экстренных ситуациях, например, чтобы разблокировать USB-устройство для аутентификации, когда несколько раз введён неправильный пароль. Не следует использовать эту возможность для повседневной работы, поскольку компьютер не будет защищён.

Эту настройку можно выполнить непосредственно на каждом сетевом узле (см. Параметры запуска программы при загрузке Windows). Если в вашей сети используется ViPNet Policy Manager, то вы можете отправить настройку централизованно. Для этого:

1 На компьютере с ViPNet Policy Manager откройте для редактирования файл `options.xml` (по умолчанию расположен в папке `c:\Program Files (x86)\InfoTeCS\ViPNet Policy Manager`).

2 Добавьте новую группу `<op:Groups type="Monitor">`:

```
<op:Groups type="Monitor">
    <op:Option label="Обязательный ввод пароля при входе в операционную систему"
    checkable="true" XMLName="ForceLogonOnStartOS" defaultValue="true"/>
</op:Groups>
```

3 Сохраните изменения в файле и перезапустите ViPNet Policy Manager.

4 Откройте или создайте новый шаблон политики для клиентов, на которые надо отправить эту настройку.

5 Откройте окно свойств шаблона и в разделе **Опции** нажмите **Добавить**.

В окне **Опции безопасности** появится новый пункт **Обязательный ввод пароля при входе в операционную систему**.

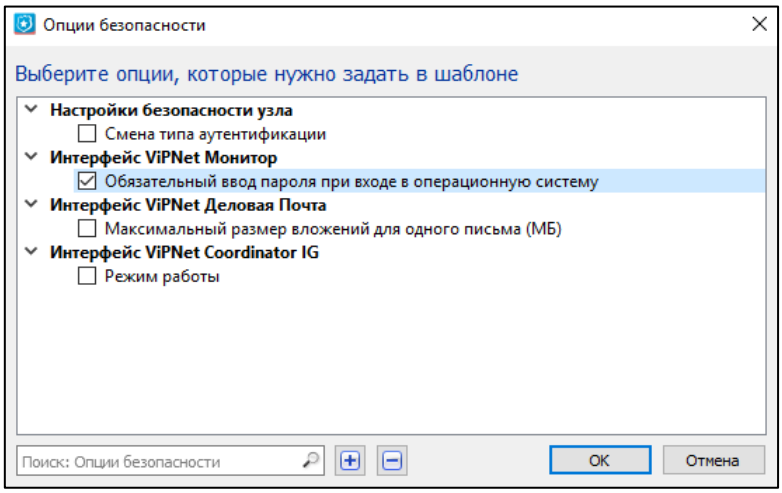


Рисунок 90. Настройка опций в ViPNet Policy Manager

Подробнее об опциях см. документ «ViPNet Policy Manager. Руководство администратора», раздел «Управление настройками программ ViPNet».

6 В окне **Свойства шаблона политики**, в разделе **Опции** снимите флажок **Обязательный ввод пароля при входе в операционную систему**.

7 Назначьте шаблон политики безопасности с этой опцией нужным сетевым узлам и отправьте политику (см. главу «Рассылка политик безопасности на сетевые узлы»).

После применения политики в программе ViPNet Client в разделе **Администратор** будет отображена эта настройка.

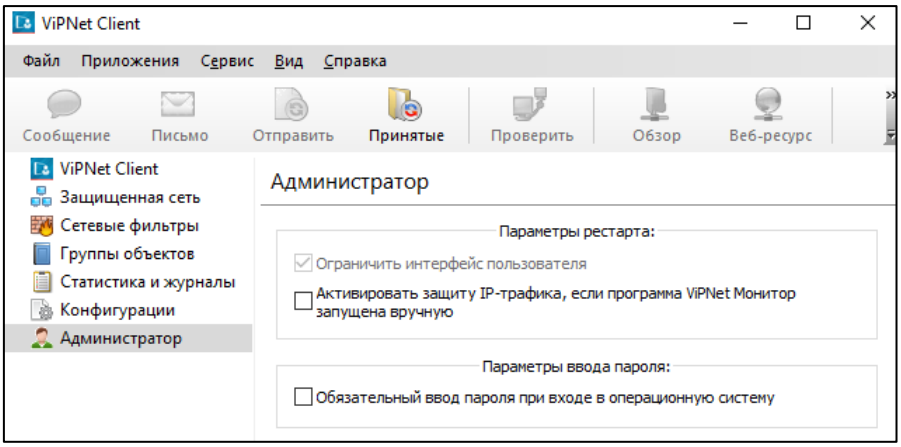


Рисунок 91. Параметры входа в программу в ViPNet Client

Разрешать открытые соединения при отсутствии связи с сервером соединений

В ViPNet Policy Manager можно централизованно установить настройку **Разрешать открытые соединения при отсутствии связи с сервером соединений** на нужных сетевых узлах. Для этого:

1. На компьютере с ViPNet Policy Manager откройте для редактирования файл `options.xml` (по умолчанию расположен в папке `c:\Program Files (x86)\InfoTeCS\ViPNet Policy Manager`).
2. Добавьте новую группу `<op:Groups type="Monitor">`:

```
<op:Groups type="Monitor">
    <op:Option label="Разрешать открытые соединения при отсутствии связи с сервером соединений" checkable="true" XMLName="AllowOpenNetworkWhenConServerUnreachable" defaultValue="false"/>
</op:Groups>
```

3. Сохраните изменения в файле и перезапустите ViPNet Policy Manager.
4. Откройте или создайте новый шаблон политики для клиентов, на которые надо отправить эту настройку.
5. Откройте окно свойств шаблона и в разделе **Опции** нажмите **Добавить**.

   В окне **Опции безопасности** появится новый пункт **Разрешать открытые соединения при отсутствии связи с сервером соединений**.

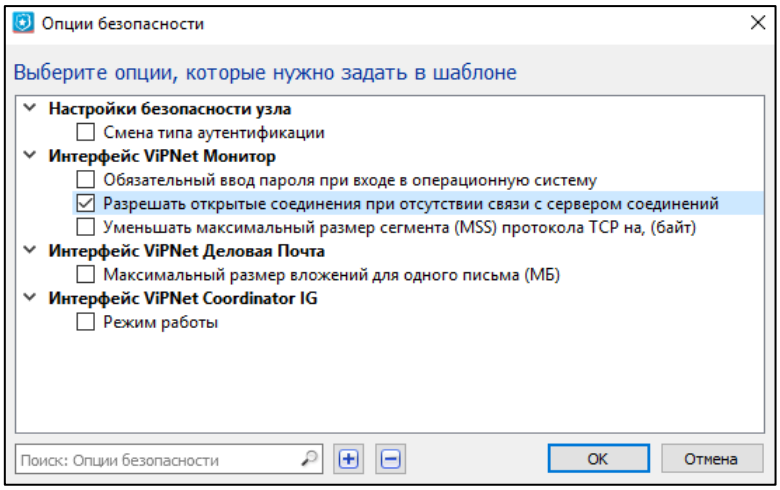


Рисунок 92. Настройка опций в ViPNet Policy Manager

Подробнее об опциях см. документ «ViPNet Policy Manager. Руководство администратора», раздел «Управление настройками программ ViPNet».

6 Назначьте шаблон политики безопасности с этой опцией нужным сетевым узлам и отправьте политику (см. главу «Рассылка политик безопасности на сетевые узлы»).

После применения политики в программе ViPNet Client в разделе **Администратор** будет отображена эта настройка.

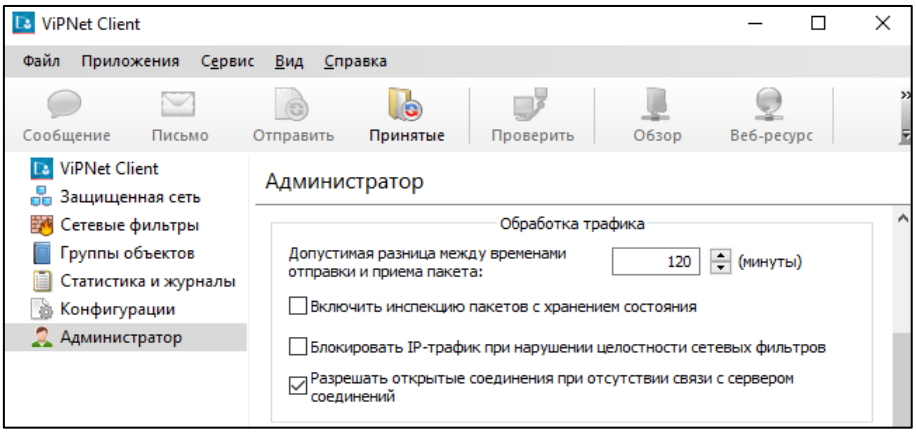


Рисунок 93. Параметры обработки трафика

Запрет сохранения ПИН-кода от внешнего устройства аутентификации

По умолчанию пользователю разрешено сохранять ПИН-код от внешнего устройства аутентификации. Для повышения безопасности вы можете централизованно запретить это, даже если пользователь включил сохранение ПИН-кода в окне входа в ViPNet Client.

Чтобы запретить сохранять пользователям ПИН-код от внешнего устройства аутентификации:

1. На компьютере с ViPNet Policy Manager откройте для редактирования файл `options.xml` (по умолчанию расположен в папке `C:\Program Files (x86)\InfoTeCS\ViPNet Policy Manager`).
2. Добавьте новую группу `<op:Groups type="NodeSecurity">`:

```
<op:Groups type="NodeSecurity">
    <op:Option label="Разрешить сохранение PIN" checkable="true"
XMLName="AllowSavingPIN" defaultValue="true"/>
  </op:Groups>
```

3. Сохраните изменения в файле и перезапустите ViPNet Policy Manager.
4. Откройте или создайте новый шаблон политики для клиентов, на которые надо отправить настройку.
5. Откройте окно свойств шаблона и в разделе **Опции** нажмите **Добавить**.

   В окне **Опции безопасности** появится новый пункт **Разрешить сохранение PIN**.

   Подробнее об опциях см. документ «ViPNet Policy Manager. Руководство администратора», раздел «Управление настройками программ ViPNet».
6. Назначьте шаблон политики безопасности с этой опцией нужным сетевым узлам и отправьте политику (см. главу «Рассылка политик безопасности на сетевые узлы»).

Удалённая работа на сетевом узле

Вы можете получить удалённый доступ к сетевому узлу ViPNet с помощью внешних программ: Remote Administrator (Radmin), VNC или Remote Desktop Connection. Эти программы должны быть установлены на вашем компьютере:

- Remote Administrator. Пакет Remote Administrator включает клиентскую и серверную части.
- RealVNC. Пакет VNC включает клиентскую и серверную части.
- Remote Desktop Connection. Программа установлена по умолчанию в Windows. Устанавливать подключения можно с компьютеров, использующих любые версии Windows. Однако подключаться можно только к компьютерам, использующим версии «Корпоративная», «Профессиональная» и «Максимальная». Подробная информация содержится на веб-сайте Microsoft.

Внимание! Не поддерживается удалённый доступ к сетевому узлу ViPNet через VMware Horizon Clients.

Чтобы запустить программу удалённого доступа:

1 Выберите раздел **Защищённая сеть**.

2 Щёлкните правой кнопкой мыши сетевой узел, к которому требуется получить удалённый доступ, выберите **Внешние программы**, затем выберите команду запуска нужной программы.

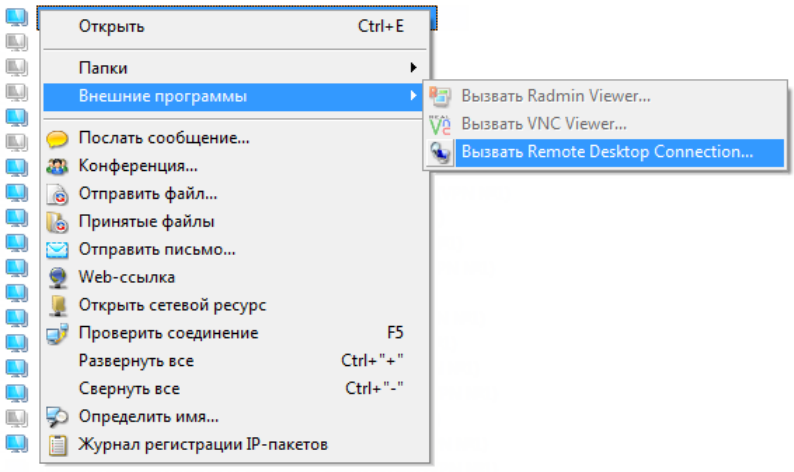


Рисунок 94. Вызов внешней программы

Команды подменю **Внешние программы** активны, только если на компьютере установлены соответствующие программы. Кроме того, выбранный сетевой узел должен иметь ненулевой IP-адрес доступа (см. Настройка доступа к защищённым узлам), 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.

При соблюдении указанных условий откроется окно соединения. Если соединение установлено, появится окно ввода пароля доступа к выбранному узлу. После ввода пароля откроется окно с отображением рабочего стола удалённого сетевого узла.

Примечание. Для успешного подключения к сетевому узлу ViPNet требуется правильно настроить программу удалённого доступа.

Например, при использовании Remote Desktop на удалённом сетевом узле должны быть выполнены настройки:

- В свойствах системы должно быть разрешено удалённое подключение к компьютеру.
- Учётная запись внешнего пользователя должна быть добавлена в список удалённых пользователей.

Настройка терминального сервера при удалённом управлении

Во время работы в терминальной сессии (например, при подключении к серверу с помощью программы Remote Desktop Connection) может возникнуть ситуация, когда после выхода из терминальной сессии программа ViPNet Client автоматически выгружается из памяти удалённого сервера и защита IP-трафика отключается. Если это произойдёт на координаторе, у всех сетевых узлов ViPNet, использующих этот координатор в качестве межсетевого экрана или сервера IP-адресов, возникнут сбои подключения.

Это происходит, когда терминальный сервер завершает все приложения пользователя после его выхода из терминальной сессии. На рисунке ниже показаны такие настройки в оснастке **Настройка служб терминалов**.

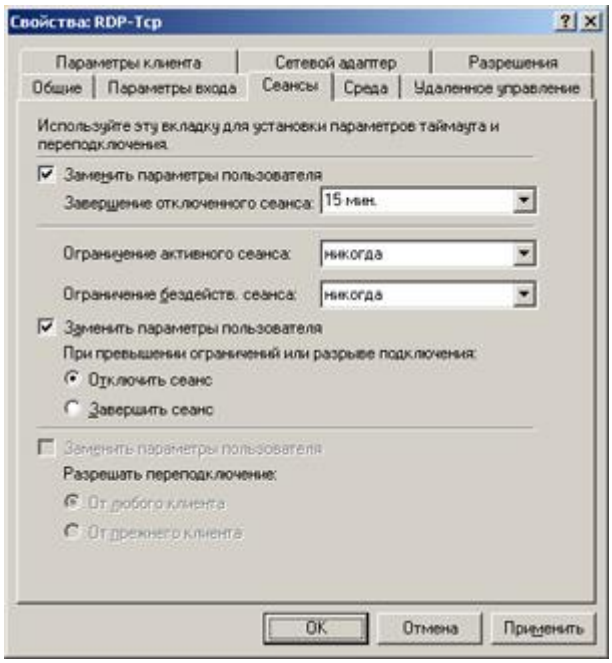


Рисунок 95. Неверные настройки терминального сервера

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

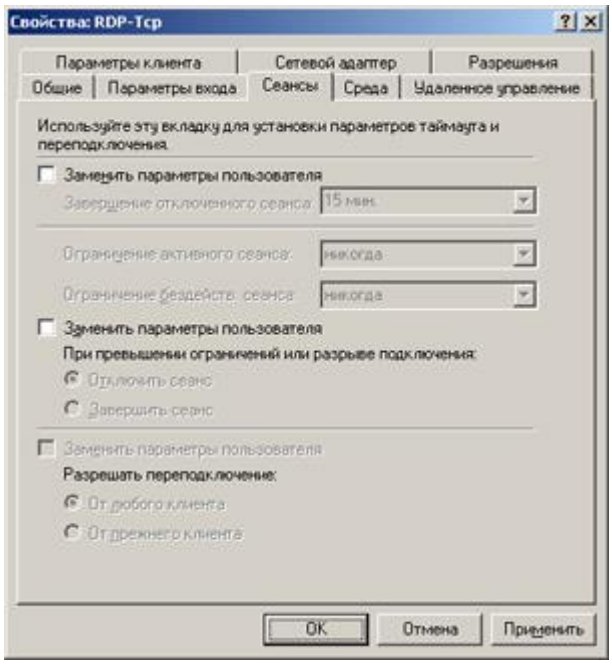


Рисунок 96. Верные настройки терминального сервера

Настройка автоматического входа в Windows и в ViPNet Client

При администрировании удалённых компьютеров необходимо после перезагрузки автоматически входить в Windows и в ViPNet Client. Это возможно, если на удалённом узле используется аутентификация пользователя по паролю (см. Способы аутентификации пользователя).

Для настройки автоматического входа:

1. Подключитесь к компьютеру непосредственно или в удалённой сессии.
2. Войдите в Windows с правами администратора.
3. Настройте параметры автоматического входа в Windows (см. Настройка автоматического входа в Windows).
4. В программе ViPNet Client:
   - **4.1** Настройте сохранение пароля при входе в программу. Для этого в меню **Файл** выберите **Сменить пользователя** и установите флажок **Сохранить пароль**.
   - **4.2** Включите автоматическую блокировку компьютера при запуске программы (см. Настройка параметров запуска программы ViPNet Client). Это поможет предотвратить несанкционированный доступ к компьютеру.

Настройка автоматического входа в Windows

Для настройки автоматического входа в Windows:

1. Нажмите клавиши **Win**+**R** или в меню **Пуск** (**Start**) выберите **Выполнить** (**Run**).
2. В поле **Открыть** (**Open**) введите команду `netplwiz`.
3. В окне **Учетные записи пользователей** (**User Accounts**):
   - **3.1** На вкладке **Пользователи** (**Users**) в списке выберите пользователя, под учётной записью которого будет выполняться вход в ОС, и снимите флажок **Требовать ввод имени пользователя и пароля** (**Users must enter a username and password to use this computer**).

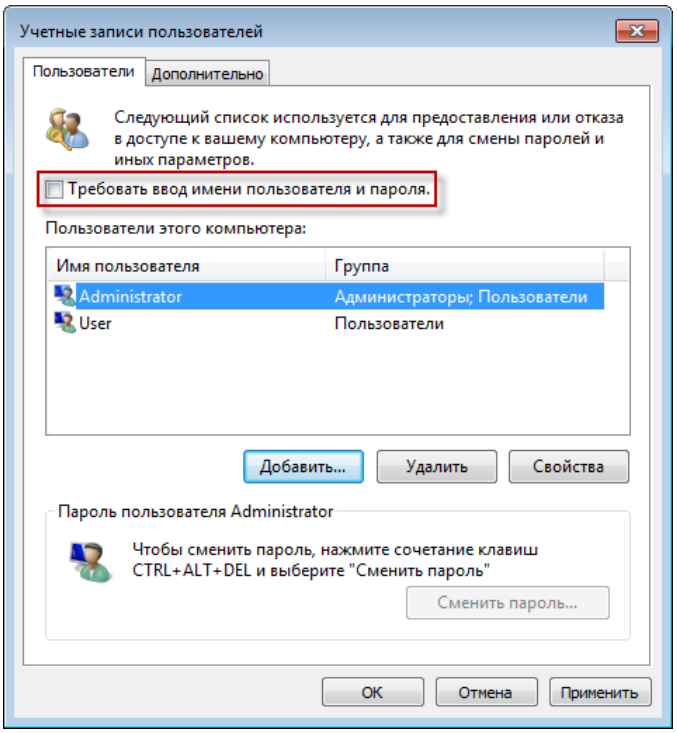


Рисунок 97. Настройка автоматического входа в ОС на вкладке Пользователи

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

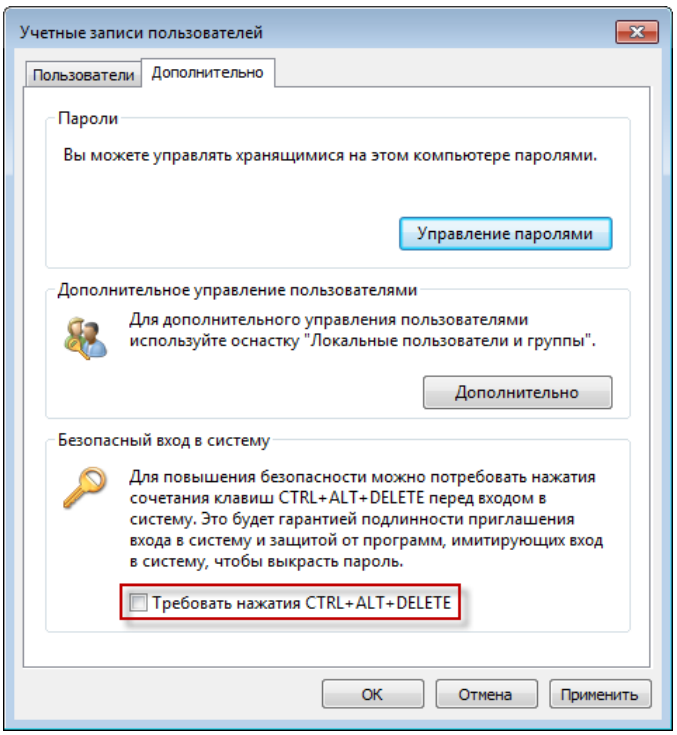


Рисунок 98. Настройка автоматического входа в ОС на вкладке Дополнительно

Примечание. Если компьютер находится в домене, то указанные флажки могут отсутствовать или быть недоступными в соответствии с групповой политикой безопасности. В этом случае автоматический вход в ОС можно настроить через реестр.

Неправильное редактирование реестра может привести к неполадкам в работе операционной системы, поэтому создайте резервную копию реестра.

Если недоступен флажок **Требовать ввод имени пользователя и пароля**, в разделе реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\PasswordLess\Device параметру DevicePasswordLessBuildVersion присвойте значение 0.

Если недоступен флажок **Требовать нажатия CTRL+ALT+DELETE**, то в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` параметру `Disablecad` присвойте значение 0.

При отсутствии указанных параметров создайте их вручную, используя тип **DWORD**.

3.3 Нажмите **Применить** (**Apply**).

4 В окне **Автоматический вход в систему** (**Automatically Log On**) введите пароль и нажмите **OK**.

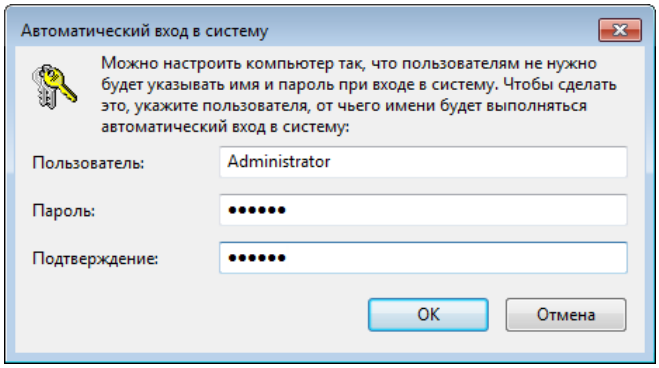


Рисунок 99. Окно ввода пароля для автоматического входа в систему

Работа в программе в режиме администратора

Общие сведения

В режиме администратора доступны дополнительные функции и настройки:

- Раздел **Администратор**, в котором можно выполнить дополнительную настройку сетевого узла ViPNet (см. Параметры защиты трафика).
- Журнал событий, содержащий записи о различных действиях, совершенных пользователем или администратором (см. Просмотр журнала событий).
- Возможность просмотреть журнал IP-пакетов определённого сетевого узла ViPNet (см. Просмотр журнала IP-пакетов другого сетевого узла).
- Возможность просмотра и изменения конфигураций программы ViPNet Client (см. Управление конфигурациями программы), созданных всеми пользователями сетевого узла.
- Снимаются все ограничения, накладываемые уровнем полномочий пользователя.

Чтобы войти в программу в режиме администратора:

1 Выполните одно из действий:

- Выберите **Файл** > **Войти в режим администратора**.
- Выберите **Сервис** > **Настройка параметров безопасности** > **Администратор** > **Вход в режим администратора**.

2 В окне **Вход в режим администратора** введите пароль администратора сетевого узла ViPNet.

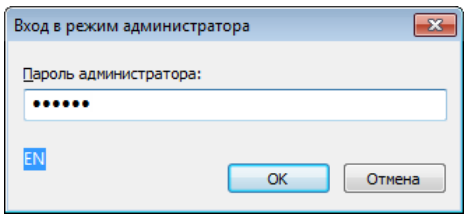


Рисунок 100. Ввод пароля администратора сетевого узла

Программа будет перезапущена и появятся дополнительные настройки.

Внимание! В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, пароли администратора для каждого сетевого узла создаются в программе ViPNet Удостоверяющий и ключевой центр.

Настройки в разделе Администратор

После входа в программу в режиме администратора, появится новый раздел **Администратор**, в котором вы можете настроить:

- Ограничение интерфейса пользователя.
- Параметры запуска программы при загрузке Windows.
- Параметры блокировки компьютера.
- Параметры защиты трафика.
- Параметры записи событий в журнал Windows (см. Настройка параметров записи событий в журнал Windows).

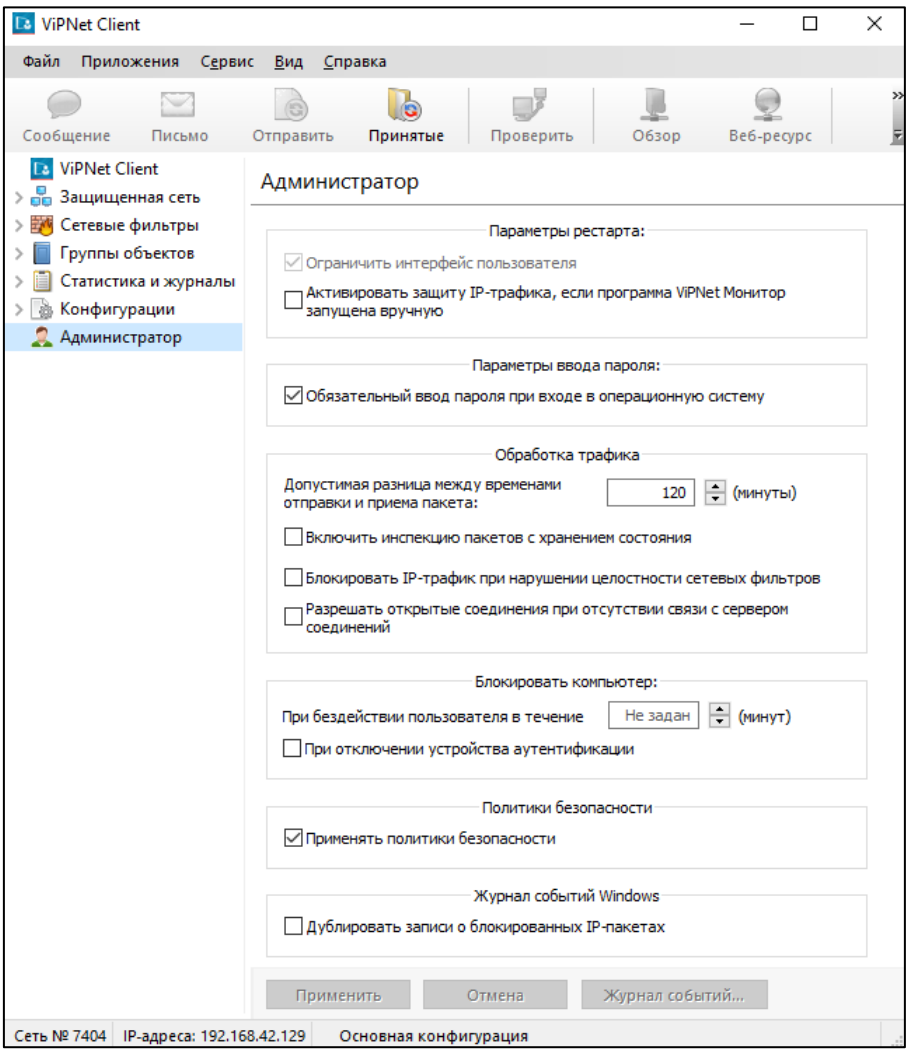


Рисунок 101. Настройка дополнительных параметров в режиме администратора

Ограничение интерфейса пользователя

Чтобы запретить пользователю настройку ViPNet Client и скрыть панели навигации, в разделе **Администратор** (см. Параметры защиты трафика) выберите **Ограничить интерфейс пользователя**.

Примечание. Если для сетевого узла задан специальный уровень полномочий 3, данный флажок установлен по умолчанию и его невозможно снять.

Если этот флажок установлен, в программе действуют ограничения:

- В окне программы отображается только панель просмотра со списком сетевых узлов ViPNet.
- В меню **Файл** отсутствует пункт **Сменить пользователя**, но при этом доступны пункты **Сменить пароль пользователя** и **Сменить способ аутентификации пользователя**.

  Пункт **Конфигурации** в меню **Файл** присутствует, если в программе создано несколько конфигураций. С его помощью можно только переключать конфигурации. Пункты **Отключить защиту**, **Блокировать IP-трафик** и **Публичный DNS** в нем отсутствуют.
- Пользователь не может создавать новые конфигурации. Если в режиме администратора сетевого узла будут созданы новые конфигурации, то они будут доступны пользователю. Если сетевой узел имеет связь с сервером открытого Интернета, на этом узле будет доступна конфигурация «Открытый Интернет».
- Недоступен пункт меню **Сервис**, в связи с этим невозможно изменение, сохранение и восстановление настроек программы ViPNet Client, а также изменение настроек параметров безопасности.

Параметры запуска программы при загрузке Windows

В разделе **Администратор** (см. Параметры защиты трафика) вы можете изменить параметры запуска программы ViPNet:

- **Активировать защиту IP-трафика, если программа ViPNet Client была запущена вручную**.

  При этом ViPNet Client не будет запускаться при загрузке Windows, защита трафика (см. Отключение защиты трафика) будет включаться только после запуска программы ViPNet и отключаться после выхода из программы.
- Чтобы при загрузке Windows пользователь не мог отказаться от запуска программы, установите флажок **Обязательный ввод пароля при входе в операционную систему**. В этом случае в окне входа в программу кнопка **Отмена** будет недоступна.

Примечание. Если установлен флажок **Активировать защиту IP-трафика, если программа ViPNet Client была запущена вручную**, параметр **Обязательный ввод пароля при входе в операционную систему** не учитывается.

Параметры блокировки компьютера

В разделе **Администратор** вы можете изменить параметры блокировки компьютера:

- При отсутствии активности пользователя в течение определённого времени. Для этого укажите продолжительность интервала блокировки в минутах в поле **При бездействии пользователя в течение.**

  Чтобы снова отключить автоматическую блокировку компьютера, укажите значение интервала блокировки, равное 0. По умолчанию значение не задано, блокировка отключена.

- По умолчанию в программе ViPNet Client включена автоматическая блокировка компьютера при отключении внешнего устройства, которое было использовано для аутентификации пользователя. Если вы хотите отключить блокировку компьютера при отключении внешнего устройства, снимите флажок **При отключении устройства аутентификации**.

Блокировка компьютера при отключении устройства аутентификации действуют только в случае использования способов аутентификации «Пароль на устройстве» и «Устройство» (см. Способы аутентификации пользователя).

Чтобы продолжить работу после автоматической блокировки, войдите в Windows.

Параметры защиты трафика

В разделе **Администратор** (см. Параметры защиты трафика) вы можете изменить дополнительные параметры защиты IP-трафика:

- Программное обеспечение ViPNet автоматически блокирует входящие IP-пакеты, если разница между временем их отправки и временем приёма больше заданного значения. Действие данной функции распространяется на сетевые узлы ViPNet, с которыми у данного узла есть связь (эти узлы отображаются в разделе **Защищённая сеть**).

  Если требуется, в поле **Допустимая разница между временами отправки и приёма пакета** измените интервал времени между отправкой и приёмом пакета в минутах (по умолчанию 120 минут).

Внимание! В результате действия данной функции могут быть заблокированы входящие IP-пакеты от сетевых узлов, на которых неправильно установлено системное время.

- Чтобы включить дополнительный анализ трафика по технологии Stateful Packet Inspection с контролем порядка установления соединения, установите флажок **Включить инспекцию пакетов с отслеживанием состояния**.
- Программа ViPNet периодически проверяет базу сетевых фильтров. В случае её повреждения появляется сообщение об этом и фильтры заменяются на предустановленные. Чтобы при этом автоматически запретить все сетевые соединения,

установите флажок **Блокировать IP-трафик при нарушении целостности сетевых фильтров**.

- Чтобы дать временный доступ к открытой сети в конфигурации с запретом открытых соединений, установите флажок **Разрешать открытые соединения при отсутствии связи с сервером соединений**.

  Это полезно, например, когда пользователи подключаются к защищённой сети через внешнего провайдера с авторизацией на Captive portal. В этом случае не потребуется переключаться между разными конфигурациями (с запретом и доступом к открытой сети). Пока нет связи с защищённой сетью, пользователь может соединиться с Captive portal, а после подключения к защищённой сети, соединение с открытой автоматически прекращается.

- При необходимости вы можете отменить действие сетевых фильтров, отправленных в составе политик безопасности из программы ViPNet Policy Manager. Например, временно отключить ошибочно отправленные на узел сетевые фильтры. Для этого снимите флажок **Применять политики безопасности**.

При этом сетевые фильтры, которые были получены в составе политик, будут скрыты и перестанут использоваться. Настройки Деловой почты и ViPNet Client, указанные в политике, останутся неизменными. Администратору ViPNet Policy Manager будет отправлена информация об отключении политик безопасности на вашем узле.

Если флажок **Применять политики безопасности** впоследствии будет повторно установлен, то действие уже принятых политик и получение новых политик из программы ViPNet Policy Manager будет возобновлено.

Настройка блокировки трафика при обнаружении вируса

Примечание. На компьютере должна быть установлена и запущена программа Kaspersky Endpoint Security 10.

Если настройка недоступна, установите модуль расширенной фильтрации:

1. В меню **Пуск** выберите **ViPNet** > **Настройка компонентов ViPNet Client**.
2. Выберите **Изменить состав** и нажмите **Далее**.
3. Установите флажок компонента **ViPNet IDS HS Agent**.

Для повышения уровня безопасности на вашем компьютере настройте совместную работу программы ViPNet Client с антивирусом. Для этого:

1. Выполните вход в программу в режиме администратора.
2. На панели навигации выберите раздел **Администратор**.
3. В группе **Взаимодействие со средством антивирусной защиты** установите флажок **Блокировать IP-трафик, если на компьютере обнаружен вирус**.

   Нажмите **Применить**.

Примечание. Если флажок **Блокировать IP-трафик, если на компьютере обнаружен вирус** принимает затенённый вид , значит в данный момент отсутствует связь с модулем расширенной фильтрации. Попробуйте выполнить настройки позднее.

Теперь, при обнаружении вируса, программа ViPNet Client автоматически заблокирует весь трафик. Для продолжения работы:

1. Выполните рекомендации, предлагаемые программой-антивирусом по устранению угрозы.
2. Отключите блокировку трафика. Для этого в окне программы ViPNet Client в меню **Файл** выберите **Конфигурации** > **Разрешить IP-трафик**.

Дополнительные настройки параметров безопасности

Помимо дополнительных параметров настройки в разделе **Администратор**, во время работы в режиме администратора сетевого узла (см. Работа в программе в режиме администратор) 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 Client. Если этот

флажок установлен, пароль пользователя хранится в реестре Windows и автоматически подставляется в поле ввода пароля при запуске программы ViPNet Client.

Примечание. Данный параметр задаётся администратором сети ViPNet в программе ViPNet Administrator и передаётся на узел в составе дистрибутива ключей или в составе обновления справочников и ключей. Администратор сетевого узла может изменить состояние флажка **Разрешить сохранение пароля в реестре**, это изменение будет действительно до следующего обновления справочников и ключей. После следующего обновления состояние флажка будет соответствовать настройкам, заданным администратором сети ViPNet.

- **Автоматически входить в ViPNet** — позволяет выполнять вход в ПО ViPNet Client 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 Client 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 сертификатов из хранилища ОС** — позволяет использовать сертификаты не только из личного хранилища (хранилища программы), но также из хранилища операционной системы. Это может понадобиться в том случае, если в ПО ViPNet предполагается использовать криптопровайдер другого производителя (например, КриптоПро), а также сертификаты, изданные внешними Удостоверяющими центрами (вне сети ViPNet).
- **Доверять только сертификатам администраторов УЦ ViPNet** — если этот флажок снят, при проверке сертификата поиск корневого сертификата выполняется не только во внутреннем хранилище ПО ViPNet, но и в системных хранилищах **Доверенные корневые центры сертификации** и **Промежуточные центры сертификации**.
- **Игнорировать отсутствие списков аннулированных сертификатов** — этот флажок следует установить, если в системе используются сертификаты, изданные внешними удостоверяющими центрами, так как в таких сертификатах информация о списках аннулированных сертификатов может отсутствовать.

Изменение способа аутентификации пользователя

Способ аутентификации определяет, какие данные должен предоставить пользователь для входа в программу. Чтобы изменить способ аутентификации:

1 Выполните вход в программу в режиме администратора (см. Работа в программе в режиме администратора).

2 Выберите **Сервис** > **Настройка параметров безопасности** > **Ключи** и нажмите **Изменить**.

3 В окне **Способ аутентификации** выберите один из способов аутентификации. Описание возможных способов аутентификации пользователя приведено в разделе Способы аутентификации пользователя.

Примечание. Способ **Пароль на устройстве** выбрать нельзя, поскольку он перестал отвечать требованиям безопасности.

При выборе способа аутентификации по сертификату подключите внешнее устройство и укажите нужный сертификат в списке сертификатов, обнаруженных на устройстве. При возникновении затруднений в выборе сертификата см. раздел Не удаётся выполнить аутентификацию с помощью сертификата.

При выборе способа аутентификации по персональному ключу подключите внешнее устройство для сохранения на нем персонального ключа пользователя (см. Симметричные ключи в ПО ViPNet). Если вы выбрали способ аутентификации по персональному ключу, также необходимо перенести на это же внешнее устройство ключи подписи пользователя (контейнер ключей). Контейнер ключей можно также перенести из текущей папки в другую папку на диске, но в этом случае каждый раз при подписании и шифровании в стороннем приложении вам потребуется вводить пароль.

Внимание! Если при использовании способа аутентификации **Устройство** внешнее устройство будет отключено, компьютер может быть автоматически заблокирован в соответствии с настройками, заданными в режиме администратора (см. Параметры защиты трафика). При необходимости параметры автоматической блокировки компьютера и IP-трафика могут быть изменены.

---

4 Нажмите **OK**.

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

В сетях ViPNet, управляемых с помощью ПО ViPNet Administrator, способ аутентификации также может изменить администратор сети в программе ViPNet Удостоверяющий и ключевой центр. Если администратор назначает пользователю способ аутентификации по сертификату, то пользователь в данном случае должен предоставить администратору внешнее устройство с сертификатом и закрытым ключом для регистрации. При этом должны быть соблюдены условия, описанные в

примечании в разделе Устройство. После назначения пользователю нового способа аутентификации администратор вышлет обновление ключей узла. Приняв данное обновление ключей, пользователь сможет выполнить аутентификацию на узле только выбранным способом.

Просмотр журнала событий

В журнале событий регистрируются действия по изменению настроек программы ViPNet Client:

- Изменение сетевых фильтров.
- Вход пользователя в программу и его выход.
- Вход в режиме администратора.
- Смена конфигурации.
- Другие события.

Данная информация позволяет администратору контролировать действия пользователя, отслеживать неисправности и попытки нарушения регламента безопасности.

Для просмотра журнала событий:

1 Выполните вход в программу в режиме администратора (см. Работа в программе в режиме администратора).

2 В разделе **Администратор** нажмите **Журнал событий**.

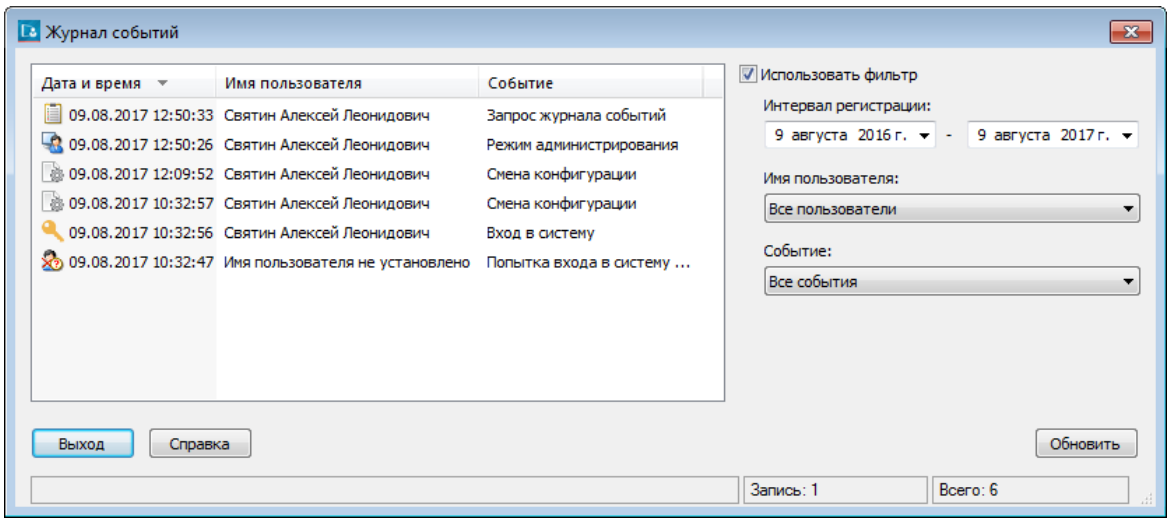


Рисунок 102. Просмотр журнала событий

3 Чтобы отобразить в журнале события определённой даты, связанные с выбранным пользователем или события одного вида, установите флажок **Использовать фильтр.** Затем укажите один или несколько нужных параметров и нажмите **Обновить**.

4 Для просмотра журнала событий в формате HTML или XLS в окне **Журнал событий** щёлкните любую строку правой кнопкой мыши и в контекстном меню выберите **Просмотр в веб-**

браузере или **Просмотр в Excel** (для просмотра журнала в формате XLS на компьютере должна быть установлена программа Microsoft Excel).

Таблица 4. События, фиксируемые в журнале

Столбец	Описание
Дата и время	Когда произошло событие.
Имя пользователя	Кто являлся инициатором события.
Событие	Расшифровка событий: •  Вход в систему. • Выход из системы. •  Режим администратора — при входе в программу с паролем администратора. •  Попытка входа в систему отвергнута (имя пользователя не установлено) — появляется в случае трёхкратного неверного ввода пароля пользователя. •  Попытка входа администратора в систему отвергнута (имя пользователя не установлено) — появляется в случае трёхкратного неверного ввода пароля администратора. •  Технологический перезапуск — перезагрузка программы после принятия файлов обновления. •  Технологический перезапуск — перезагрузка программы после аварийного завершения. •  Смена пользователя — вход в программу другого пользователя, зарегистрированного на данном сетевом узле. •  Смена конфигурации — смена конфигурации программы в разделе **Конфигурации**. •  Изменение фильтра — любые действия по созданию, редактированию или удалению фильтров. •  Отключение защиты трафика. •  Включение функции блокирования всего трафика. •  Разрешение прохождения трафика. •  Включение или выключение опции «Блокировать все протоколы кроме IPv4, ARP» — устанавливается в окне **Настройка** в разделе **Управление трафиком**. •  Включение или выключение функции «Блокировать компьютер» — устанавливается в окне **Настройка** в разделе **Общие** > **Запуск и аварийное завершение**. •  Просмотр журнала событий.

Настройка параметров записи событий в журнал Windows

Если в вашей сети ViPNet развернут программный комплекс ViPNet StateWatcher, вы можете разрешить ПК ViPNet StateWatcher собирать и анализировать дополнительную информацию о событиях на вашем защищённом сетевом узле. В этом случае необходимо включить запись событий, происходящих на сетевом узле ViPNet, в журнал Windows Приложений, так как ПК ViPNet StateWatcher при сборе информации о сетевом узле обращается к журналам событий Windows.

Примечание. Чтобы пользователи ПК ViPNet StateWatcher могли получать оповещения об этих событиях, администратору необходимо создать правило анализа, указав в качестве источника события программное обеспечение ViPNet Client. Подробнее см. «Программный комплекс мониторинга защищённых сетей ViPNet StateWatcher 4. Сервер мониторинга. Руководство администратора».

В программе ViPNet Client предусмотрена запись в журнал Windows блокированных IP-пакетов (см. Блокированные IP-пакеты).

Чтобы включить запись событий в журнал Windows:

1. Войдите в программу в режиме администратора (см. Общие сведения).
2. В разделе **Администратор** в группе **Журнал событий Windows** установите флажок **Дублировать записи о блокированных IP-пакетах**.
3. Нажмите **Применить**.

   События начнут записываться в журнал Windows и в журнал программы ViPNet Client.

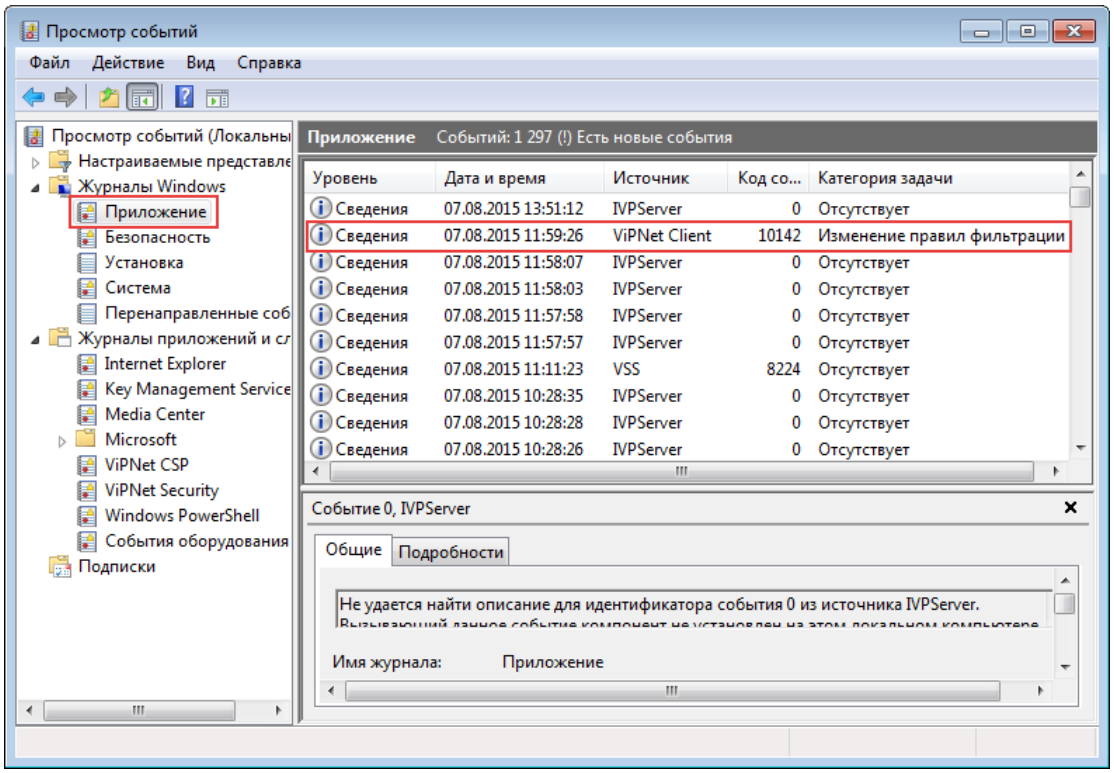


Рисунок 103. Событие узла ViPNet, сохранённое в журнале Windows Приложение

Внимание! В случае если количество записанных событий будет слишком большим и возникнет угроза переполнения журнала Windows, вы можете увеличить его объем с помощью стандартных настроек журнала.

Настройка параметров запуска программы ViPNet Client

Для настройки параметров запуска программы:

1 В меню **Сервис** выберите **Настройка приложения**.

2 В окне **Настройка** на панели навигации выберите раздел **Общие** > **Запуск и аварийное завершение**.

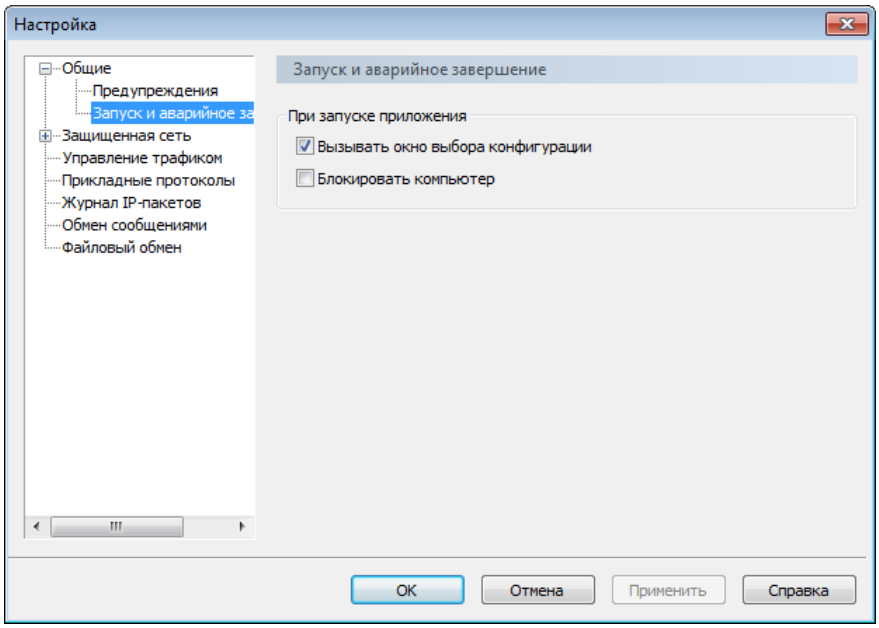


Рисунок 104. Настройка параметров запуска и аварийного завершения работы программы

3 Чтобы при запуске программы не выбирать конфигурацию (см. Управление конфигурациями программы), снимите флажок **Вызывать окно выбора конфигурации**. При этом запуск программы будет происходить в той конфигурации, которая использовалась в последнем сеансе работы.

Если в программе настроена только одна конфигурация, окно выбора появляться не будет независимо от установки флажка.

4 Чтобы при запуске программы блокировать доступ к рабочему столу компьютера, установите флажок **Блокировать компьютер**. Для разблокирования компьютера введите пароль пользователя Windows.

Данная функция полезна для предотвращения несанкционированной работы с компьютером после его перезагрузки, если настроен автоматический вход пользователя Windows в операционную систему. При этом программа ViPNet Client выполняет все функции по защите компьютера.

11

Настройка параметров безопасности

Смена пароля пользователя

Пароль пользователя рекомендуется менять раз в 3 месяца. Как правило, частота смены пароля пользователя определяется регламентом безопасности организации.

Смена текущего пароля пользователя требуется в следующих случаях:

- По истечении срока действия текущего пароля (если этот срок действия ограничен).
- Если из программы ViPNet Удостоверяющий и ключевой центр отправлено обновление с оповещением о смене пароля. При входе появится сообщение «Рекомендуется сменить пароль пользователя», при этом пароль необходимо сменить вручную.
- Если контейнер ключей защищён с использованием персонального ключа пользователя, пароль к контейнеру ключей будет совпадать с паролем пользователя. Поэтому при смене пароля к контейнеру ключей следует сменить пароль пользователя.

Кроме того, рекомендуется менять пароль пользователя при первом входе в программу после установки справочников и ключей. Это повысит надёжность пароля, поскольку он не будет известен администратору.

Для того чтобы сменить пароль пользователя:

1. В окне **Настройка параметров безопасности** откройте вкладку **Пароль**.
2. В группе **Тип пароля** выберите тот тип, которому должен соответствовать новый пароль:
   - **Собственный** — пароль, определяемый пользователем;
   - **Случайный на основе парольной фразы** — пароль, формируемый автоматически на основе парольной фразы по заданным параметрам;
   - **Случайный цифровой** — пароль, формируемый автоматически из заданного числа цифр.
3. Нажмите **Сменить пароль**.
   - Если был выбран тип пароля **Собственный**, задайте и подтвердите пароль. Он должен содержать:
     - от 8 до 31 символа,
     - прописные и строчные буквы английского алфавита (A–Z, a–z),
     - цифры (0–9),
     - спецсимволы (!@#$%^&*()-_+=;:'",.<>/?\|`~[]{}).
   - Если был выбран тип пароля **Случайный на основе парольной фразы** или **Случайный цифровой**, появится автоматически сформированный пароль с парольной фразой или случайный цифровой пароль. При необходимости вы можете создать новый случайный пароль с помощью кнопки **Другой пароль**.
4. Чтобы ограничить срок действия нового пароля установите флажок **Ограничить срок действия пароля** и укажите срок действия.
5. Нажмите **OK**.

Настройка параметров криптопровайдера ViPNet CSP

В состав ViPNet Client включена программа ViPNet CSP. Это криптопровайдер, который позволяет использовать российские криптографические алгоритмы в приложениях Microsoft и других программах, использующих интерфейс Microsoft CryptoAPI 2.0. Кроме этого, ViPNet CSP обеспечивает работу с контейнерами ключей и поддержку различных внешних устройств хранения ключей (см. Внешние устройства).

Чтобы настроить программу ViPNet CSP:

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

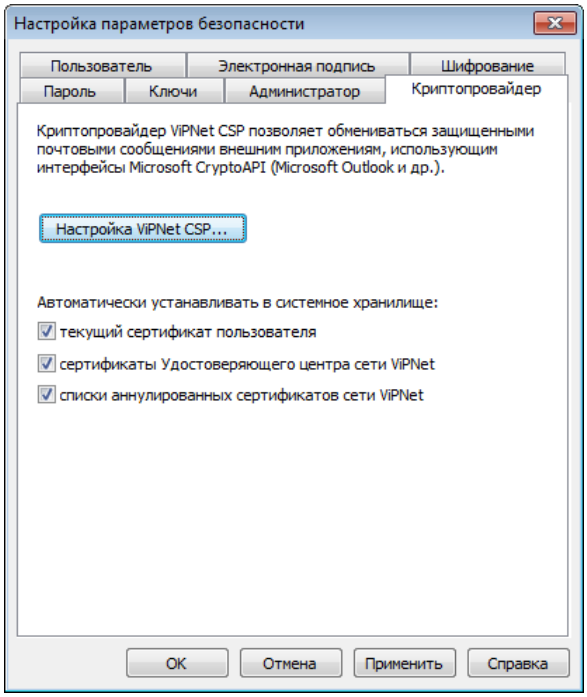


Рисунок 105. Настройка параметров криптопровайдера ViPNet CSP

2 Нажмите **Настройка ViPNet CSP**. Откроется окно **ViPNet CSP**, в котором вы можете:

- Задать необходимые параметры криптопровайдера ViPNet CSP.
- Выполнить операции с контейнерами ключей.
- Настроить параметры использования внешних устройств — задать типы устройств, которые могут использоваться, выполнить инициализацию или изменить ПИН-код.

Подробнее см. документ «ViPNet CSP. Руководство пользователя».

3 Настройте автоматическую установку сертификатов в хранилище:

- **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 в составе обновления ключей;
- **списки аннулированных сертификатов сети ViPNet** — для установки в системное хранилище списков аннулированных сертификатов, получаемых из программы ViPNet Удостоверяющий и ключевой центр в составе обновления ключей.

4 Выполнив необходимые настройки, нажмите **OK**.

12

Работа с сертификатами и ключами

Просмотр сертификатов

Примечание. Описанные в данном разделе возможности доступны, если вы располагаете действительным сертификатом электронной подписи. Для получения сертификата обратитесь к администратору вашего удостоверяющего центра.

Просмотр сертификата может понадобиться для получения информации о его назначении, издателе, составе полей, причине недействительности сертификата и так далее. Подробная информация о сертификатах содержится в разделе Общие сведения о сертификатах ключей проверки электронной подписи.

В программе ViPNet Client можно просматривать следующие типы сертификатов:

- текущий сертификат пользователя (см. Просмотр текущего сертификата пользователя);
- личные сертификаты пользователя (см. Просмотр личных сертификатов пользователя);
- доверенные корневые сертификаты (см. Просмотр доверенных корневых сертификатов);
- изданные сертификаты (см. Просмотр изданных сертификатов).

Основная информация о выбранном сертификате отображается в окне **Сертификат** на вкладке **Общие**:

- назначение сертификата или (для недействительных сертификатов) причина недействительности сертификата;
- имя владельца ключа проверки электронной подписи, которому выдан сертификат;
- имя издателя сертификата;
- срок действия сертификата;
- срок действия ключа электронной подписи, соответствующего данному сертификату (только для сертификатов пользователей);
- информация о политиках применения сертификата, отображаемая при нажатии кнопки **Заявление издателя**.

Примечание. В сертификате пользователя сети ViPNet кнопка **Заявление издателя** доступна только в том случае, если политики применения были присвоены сертификату при его издании в программе ViPNet Удостоверяющий и ключевой центр.

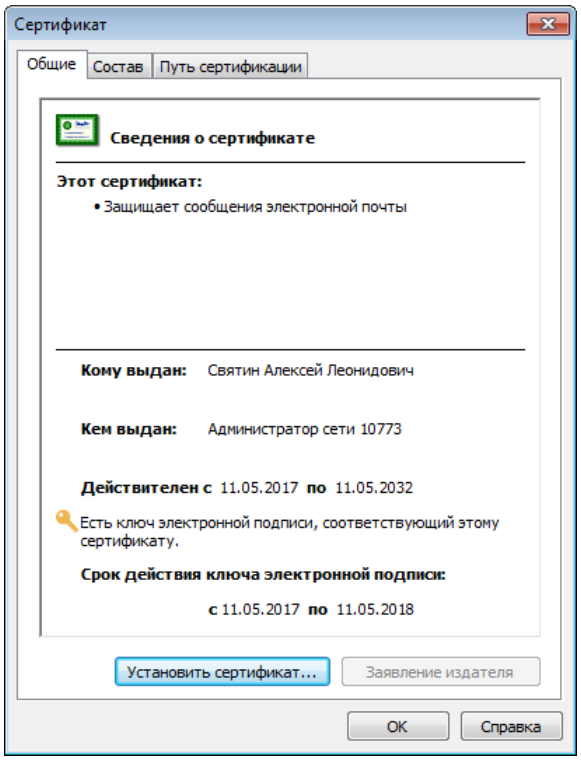


Рисунок 106. Просмотр основной информации о сертификате

Просмотр текущего сертификата пользователя

Для просмотра текущего сертификата пользователя в окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**, после чего нажмите **Подробнее**.

Просмотр личных сертификатов пользователя

Для просмотра личных сертификатов пользователя:

1 В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись** > **Сертификаты**.

Откроется окно **Менеджер сертификатов** с информацией обо всех личных сертификатах пользователя, а также о сертификатах, установленных в хранилище операционной системы. Все данные сертификаты введены в действие.

Примечание. Сертификаты, установленные в хранилище операционной системы, отображаются в том случае, если на вкладке **Администратор** окна **Настройка параметров безопасности** установлен флажок **Разрешить использование сертификатов из хранилища ОС** (см. Дополнительные настройки параметров безопасности).

---

2 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите **Свойства** или дважды щёлкните 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 **Электронная подпись** > **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 **Свойства** или дважды щёлкните этот сертификат.

   Откроется окно **Сертификат** с информацией о выбранном корневом сертификате.

Просмотр изданных сертификатов

Для просмотра сертификатов, которые изданы в программе ViPNet Удостоверяющий и ключевой центр по запросам пользователей или по инициативе администратора УКЦ, но ещё не введены в действие, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись** > **Изданные сертификаты**.

   Откроется окно **Менеджер сертификатов** с информацией об изданных сертификатах.

2 При необходимости просмотра более подробной информации об одном из сертификатов выберите нужный сертификат, после чего нажмите **Свойства** или дважды щёлкните этот сертификат.

   Откроется окно **Сертификат** с информацией о выбранном изданном сертификате.

Просмотр цепочки сертификации

Для просмотра цепочки сертификации определённого 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 **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 определённого 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 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** не отображается в следующих случаях:

- Срок действия сертификата не превышает 15 месяцев, и для хранения ключа электронной подписи используется файл на компьютере, либо внешнее устройство без аппаратной поддержки российских криптографических алгоритмов.
- Срок действия сертификата не превышает 36 месяцев, и для хранения ключа электронной подписи используется файл на компьютере, либо внешнее устройство без аппаратной поддержки российских криптографических алгоритмов.

Срок действия закрытого ключа в данных случаях равен сроку действия сертификата.

- **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 **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 Установка в хранилище вручную
Смена текущего сертификата. Можно выбрать другой сертификат (из числа действительных личных сертификатов пользователя) в качестве текущего.	Смена текущего сертификата
Обновление ключа электронной подписи и сертификата. Можно настроить параметры автоматического оповещения об истечении срока действия текущего сертификата и соответствующего ему ключа электронной подписи, а также, при необходимости, сформировать запрос на обновление этого сертификата и ключа электронной подписи.	Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата Процедура обновления ключа электронной подписи и сертификата
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 в действие автоматически Ввод в действие вручную
Просмотр и удаление запросов на сертификаты. Можно просмотреть состояние запросов на сертификаты, сформированных текущим пользователем, а также удалить ненужные запросы.	Просмотр запроса на сертификат Удаление запроса на сертификат
Экспорт сертификата. В зависимости от целей использования сертификата за пределами ПО ViPNet, сертификат может быть экспортирован в файлы различных форматов.	Экспорт сертификата

Установка сертификатов в хранилище операционной системы

Установка сертификатов в хранилище операционной системы позволяет использовать сертификаты во внешних приложениях (таких как Windows Live Mail, Microsoft Outlook, Microsoft Word и других).

Внимание! Для работы с защищёнными документами, помимо сертификата пользователя, необходимо также установить в хранилище корневой сертификат (издателя) и список аннулированных сертификатов.

Установку можно выполнить автоматически или вручную.

Внимание! Для установки сертификатов в хранилище Windows Server следует запускать программу ViPNet Client от имени администратора.

Установка в хранилище автоматически

Установка сертификатов запускается автоматически при соблюдении следующих условий:

- сертификаты (текущий сертификат пользователя, корневой сертификат и списки аннулированных сертификатов) ещё не были установлены 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 и списков аннулированных сертификатов в хранилище текущего пользователя.

Если необходимо обеспечить автоматическое обновление списков аннулированных сертификатов в хранилище локального компьютера, выполните следующие действия:

- Предварительно вручную установите в это хранилище соответствующие корневой сертификат и список аннулированных сертификатов (см. Установка в хранилище вручную).
- Убедитесь, что установлен компонент программы ViPNet CSP «Поддержка работы ViPNet CSP через MS CryptoAPI». Подробнее см. документ «ViPNet CSP. Руководство пользователя» раздел «Добавление, удаление и восстановление компонентов программы».
- Для запуска программы ViPNet Client используйте учётную запись, обладающую правами администратора.

Для автоматической установки текущего сертификата пользователя и списков аннулированных сертификатов (при соблюдении приведённых выше условий) не требуется никаких дополнительных действий со стороны пользователя.

Для установки корневого сертификата необходимо подтверждение этого действия пользователем в окне **Установка корневого сертификата**. Данное окно появляется тогда, когда корневой сертификат отсутствует в хранилище сертификатов Windows. Это может произойти в следующих случаях:

- При первичном запуске ПО ViPNet после развёртывания сетевого узла.
- Если совместно с обновлением текущего сертификата пользователя получен новый корневой сертификат.

Для подтверждения автоматической установки корневого сертификата выполните следующие действия:

1 При появлении окна **Установка корневого сертификата**:

- чтобы выполнить автоматическую установку сертификата, нажмите **ОК**;
- если автоматическая установка корневого сертификата и других сертификатов не требуется, установите флажок **Отключить автоматическую установку сертификатов**, после чего нажмите **ОК**.

Примечание. В окне **Настройка параметров безопасности** на вкладке **Криптопровайдер** флажки группы **Автоматически устанавливать в системное хранилище** будут также сняты.

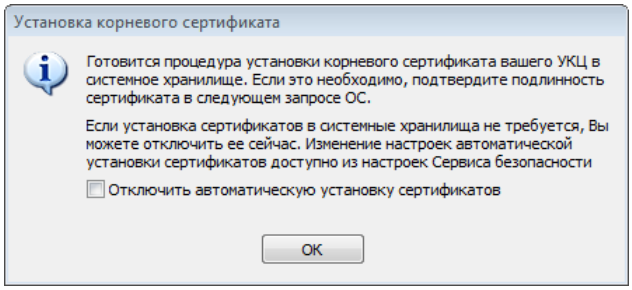


Рисунок 107. Установка корневого сертификата

2 Если автоматическая установка сертификатов не была прервана, в окне запроса на добавление сертификата в хранилище проверьте подлинность сертификата, после чего нажмите **Да**.

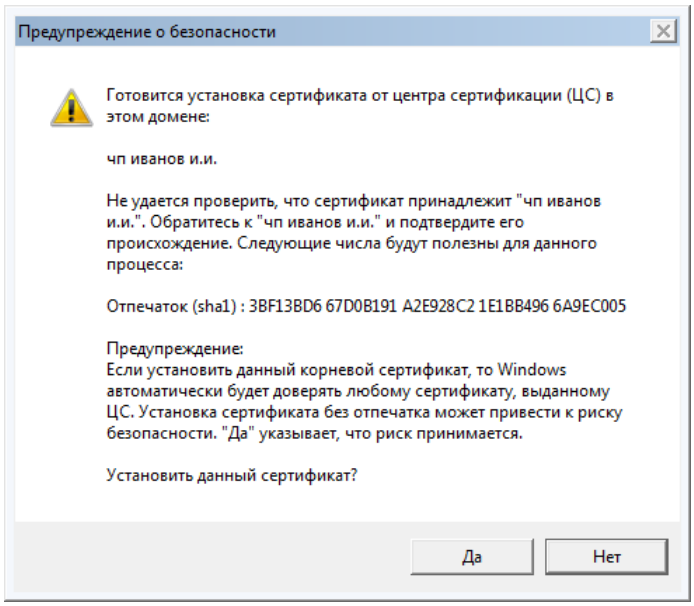


Рисунок 108. Подтверждение подлинности корневого сертификата

Следует иметь в виду, что пауза перед автоматической установкой корневого сертификата может занимать продолжительное время в зависимости от используемой программы ViPNet:

- В программе ViPNet Client опрос параметров выполняется через 5 минут после запуска и далее с 2-часовым интервалом. При открытом окне **Настройка параметров безопасности** интервал опроса сокращается до 10–15 минут.
- В программе ViPNet Деловая почта опрос параметров выполняется через 5 минут после запуска программы, а затем с интервалом 60 минут.

Корневой сертификат установлен в хранилище сертификатов текущего пользователя.

Установка в хранилище вручную

Если изданный сертификат пользователя не был установлен в хранилище автоматически (см. Установка в хранилище автоматически), вы можете установить его в хранилище и сопоставить с ключом электронной подписи вручную. Также совместно с сертификатом пользователя вы можете установить в хранилище операционной системы сертификат издателя и список аннулированных сертификатов (CRL).

Для установки сертификата пользователя, а также сертификата издателя и CRL в хранилище операционной системы выполните следующие действия:

1. Вызовите окно **Сертификат** для того сертификата, который необходимо установить в хранилище (см. Просмотр сертификатов).
2. Нажмите **Установить сертификат**.
3. На странице приветствия мастера установки сертификатов нажмите **Далее**.

4 На странице **Выбор хранилища сертификатов** выполните следующие действия:

- Укажите, в какое хранилище будет установлен ваш сертификат.
- Если на сетевой узел кроме сертификата пользователя также поступили сертификаты издателей и CRL, для их установки установите соответствующие флажки.

Нажмите **Далее**.

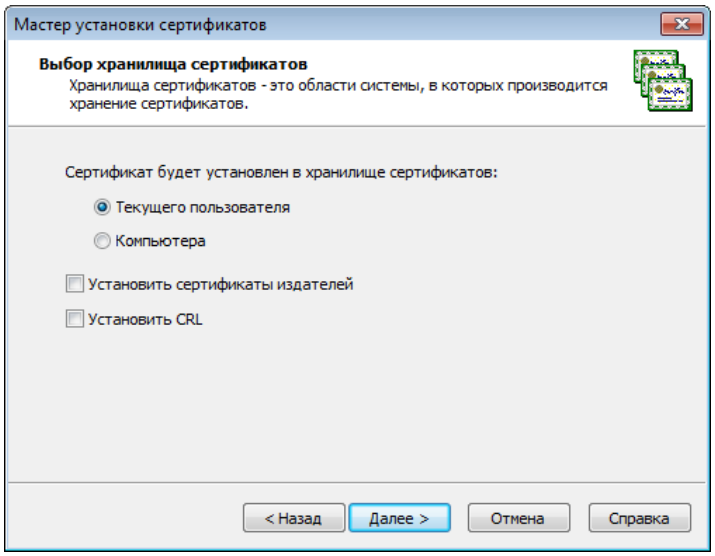


Рисунок 109. Выбор хранилища сертификатов

Примечание. Сертификат следует устанавливать в хранилище текущего пользователя для целей шифрования, расшифрования и подписания файлов, а также для доступа к защищённым ресурсам через веб-браузер. В хранилище компьютера следует устанавливать сертификаты, которые будут использоваться службами данного компьютера, и сертификаты для аутентификации в программе ViPNet.

Сертификат следует устанавливать в хранилище компьютера при использовании ViPNet Client на веб-сервере для организации доступа к защищённым ресурсам.

Если возможность установки сертификата в хранилище компьютера недоступна, запустите программу ViPNet от имени 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.

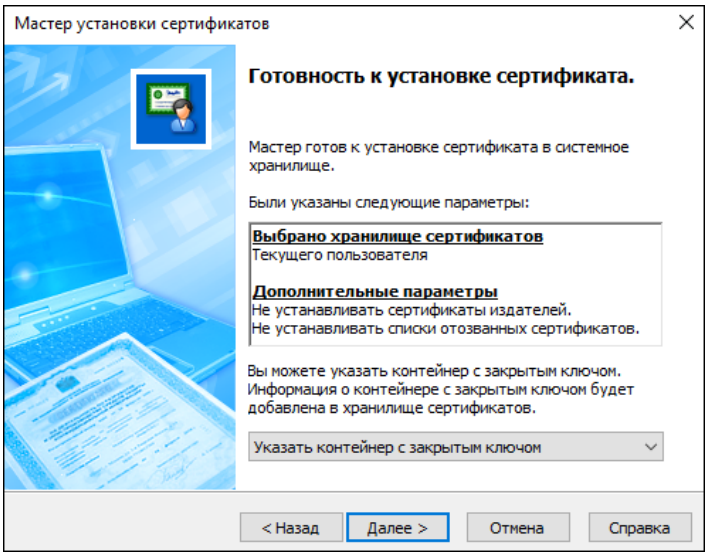


Рисунок 110. Сертификат готов к установке

- Для сопоставления сертификата пользователя с ключом электронной подписи установите флажок **Указать контейнер с ключом электронной подписи**.
- Нажмите **Далее**.

6 Если флажок **Указать контейнер с ключом электронной подписи** установлен и контейнер не найден либо недоступен, в появившемся окне **ViPNet CSP – инициализация контейнера ключей** укажите расположение контейнера ключей:

- папку на диске;
- устройство (с указанием его ПИН-кода).

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства.

После этого нажмите **OK**.

7 В окне подтверждения нажмите **Да**, чтобы добавить сертификат в контейнер ключей, или **Нет**, чтобы оставить сертификат в виде отдельного файла.

8 Если появилось окно **ViPNet CSP – пароль контейнера ключей**, то в поле **Пароль** введите пароль доступа к контейнеру, после чего нажмите **OK**.

Совет. Сохранение сертификата в одном контейнере с ключом электронной подписи удобно, если контейнер планируется переносить и устанавливать на другом компьютере.

Примечание. Окно **ViPNet CSP – пароль контейнера ключей** отображается в следующих случаях:

- контейнер, в котором находится сертификат, сформирован с помощью программы ViPNet CSP или ViPNet Registration Point;
- если ранее при сохранении пароля не был установлен флажок **Сохранить пароль**.

9 На странице **Завершение работы мастера установки сертификата** нажмите **Готово**.

Сертификат установлен в выбранное хранилище сертификатов. Если в процессе установки сертификата ему не был сопоставлен ключ электронной подписи, вы можете вручную установить сертификат в контейнер ключей (см. Установка сертификата в контейнер ключей).

Обновление ключа электронной подписи и сертификата

Сертификат ключа проверки электронной подписи и ключ электронной подписи имеют ограниченный срок действия, поэтому их требуется регулярно обновлять. При обновлении сертификата также обновляется ключ электронной подписи.

Обновление требуется в следующих случаях:

- Истёк срок действия сертификата. Срок действия сертификата может составлять до 5 лет.
- Истёк срок действия ключа электронной подписи. Если ключ электронной подписи хранится в файле на компьютере или на внешнем устройстве без аппаратной поддержки российских криптографических алгоритмов, то его срок действия составляет 15 месяцев (если срок действия сертификата превышает 15 месяцев) или равен сроку действия сертификата (если срок действия сертификата меньше 15 месяцев).

  Если ключ электронной подписи хранится на внешнем устройстве с аппаратной поддержкой российских криптографических алгоритмов, то его срок действия составляет 36 месяцев (если срок действия сертификата превышает 36 месяцев) или равен сроку действия сертификата (если срок действия сертификата меньше 36 месяцев).
- Требуется получить сертификат, в котором будут изменены данные о его владельце (должность, подразделение и другие) или добавлены дополнительные атрибуты, расширения. Например, для использования сертификата в системах документооборота в него могут быть добавлены нужные политики применения.

Обновить сертификат и ключ электронной подписи вы можете не только в программе ViPNet Client (из окна **Настройка параметров безопасности**), но и с помощью её компонента — программы ViPNet CSP (см. документ «ViPNet CSP. Руководство пользователя»).

Таблица 5. Последовательность действий при обновлении ключа электронной подписи и сертификата

	Действие	Ссылка
☐	Проверьте настройки обновления сертификатов. При необходимости настройте автоматическую установку сертификатов в хранилище и их автоматический ввод в действие	Установка в хранилище автоматически Ввод в действие автоматически
☐	Создайте запрос на сертификат. Дождитесь, пока сертификат будет издан в УКЦ и передан на ваш узел	Процедура обновления ключа электронной подписи и сертификата
☐	Установите сертификат в контейнер ключей и в системное хранилище, если не было настроено автоматическое выполнение этих действий	Установка в хранилище вручную
☐	При необходимости сделайте полученный сертификат текущим	Смена текущего сертификата
☐	Введите сертификат в действие, если не было настроено автоматическое выполнение этого действия	Ввод в действие вручную

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

Примечание. Если истёк срок действия ключа электронной подписи, но при этом сертификат ключа проверки электронной подписи остаётся действительным, можно создать запрос на обновление сертификата. Запрос будет подписан ключом электронной подписи, но электронная 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 истёк срок действия и ключа электронной подписи и сертификата, запрос на обновление создать невозможно. Новый сертификат в этом случае может быть издан только по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр.

В случае отсутствия ключа электронной подписи создать запрос на сертификат также невозможно.

Настройка оповещения об истечении срока действия ключа электронной подписи и сертификата

По умолчанию программа ViPNet Client начинает выдавать предупреждения за 15 дней до истечения срока действия сертификата или ключа электронной подписи.

Чтобы изменить настройки оповещения, выполните следующие действия:

1 В окне **Настройка параметров безопасности** перейдите на вкладку **Электронная подпись**.

В поле **Информация о текущем сертификате** указан срок действия сертификата и ключа электронной подписи.

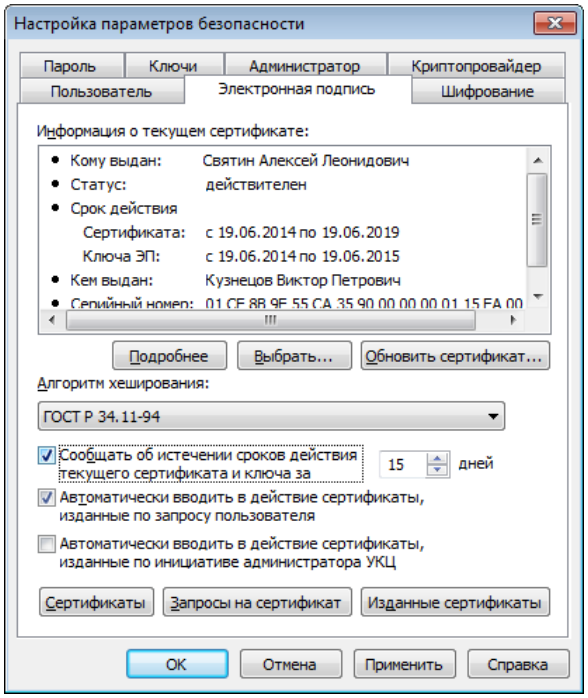


Рисунок 111. Просмотр информации о текущем сертификате и настройка параметров оповещения об истечении сроков действия ключа электронной подписи и сертификата

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 ключа электронной подписи и сертификата

За несколько дней до истечения срока действия сертификата или ключа электронной подписи требуется выполнить следующие действия:

- Если включено оповещение об истечении срока действия сертификата и ключа электронной подписи:
  - Когда до истечения срока остаётся заданное количество дней, программа ViPNet Client выдаст соответствующее сообщение.

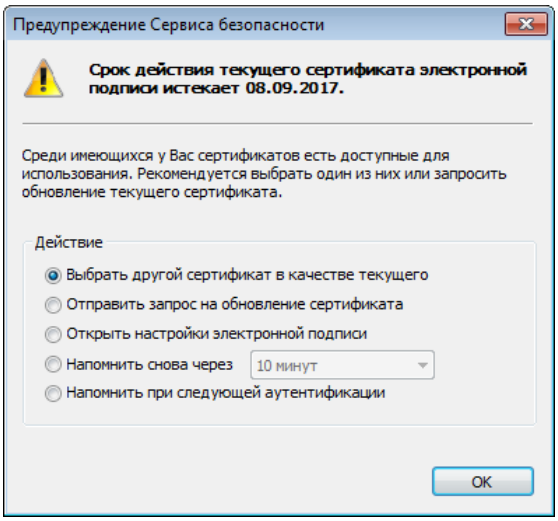


Рисунок 112. Предупреждение о скором истечении срока действия сертификата и ключа электронной подписи

- Если истекает срок действия сертификата, в окне сообщения выберите **Отправить запрос на обновление сертификата**, после чего нажмите **OK**. Будет запущен **Мастер обновления сертификата**.

Примечание. Можно также открыть окно настройки параметров электронной подписи, отложить отправку запроса на обновление сертификата или выбрать другой сертификат при его наличии.

- Если истекает срок действия ключа электронной подписи, в окне сообщения выберите **Открыть настройки электронной подписи**, после чего нажмите **OK**. В появившемся окне **Настройка параметров безопасности** на вкладке **Электронная подпись** нажмите **Обновить сертификат**.

- Если оповещение об истечении срока действия сертификата и ключа электронной подписи отключено:
  - В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**.
  - На вкладке **Электронная подпись** нажмите **Обновить сертификат**. Будет запущен **Мастер обновления сертификата**.

Чтобы сформировать и отправить запрос на обновление сертификата и ключа электронной подписи с помощью мастера:

1 На первой странице мастера обновления сертификата нажмите **Далее**.

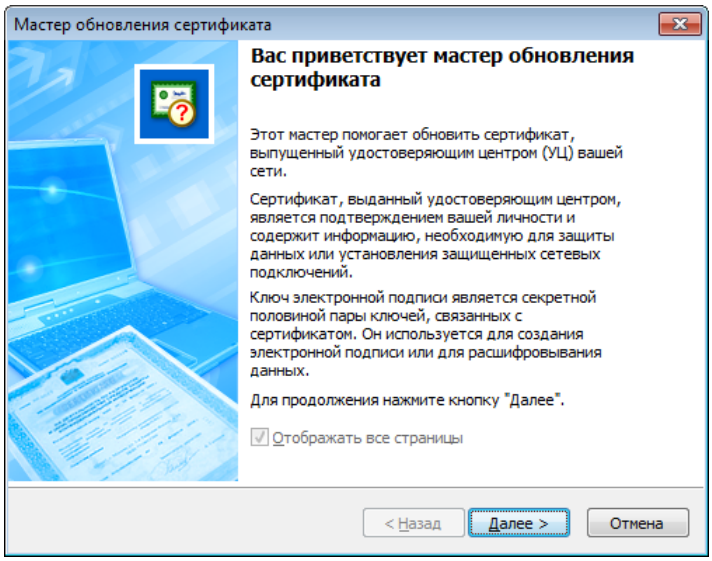


Рисунок 113. Стартовая страница мастера обновления сертификата

2 На странице **Ключ электронной подписи** выполните следующие действия:

2.1 Укажите назначение ключа и сертификата:

- если предполагается их использовать только для подписи — значение **Электронная подпись**;
- если предполагается их использовать как для подписи, так и для шифрования — значение **Электронная подпись и шифрование**.

2.2 Задайте алгоритм формирования ключа и параметры алгоритма в соответствии с приведённой ниже таблицей:

Таблица 6. Характеристики алгоритмов

Алгоритм и его описание	Параметры алгоритма	Длина ключа проверки электронной подписи
ГОСТ Р 34.10-2012/512 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 256 бит OID «1.2.643.7.1.1.1.1»	ГОСТ Р 34.10 - 2001 Параметры по умолчанию (рекомендуется) OID «1.2.643.2.2. 35.1» ГОСТ Р 34.10 - 2001 Параметры подписи B OID «1.2.643.2.2. 35.2» ГОСТ Р 34.10 - 2001 Параметры подписи C OID «1.2.643.2.2. 35.3»	512

Алгоритм и его описание	Параметры алгоритма	Длина ключа проверки электронной подписи
	Примечание. Параметры ГОСТ Р 34.10 - 2001 используются для двух алгоритмов: ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012/512, поскольку стандарт ГОСТ-2001 идентичен ГОСТ-2012 для ключей 256 бит.	
ГОСТ Р 34.10-2012/1024 Новый стандарт электронной подписи от 2012 года с длиной ключа электронной подписи 512 бит OID «1.2.643.7.1.1.1.2»	ГОСТ Р 34.10 - 2012/1024 Набор параметров A ГОСТ Р 34.10 - 2012/1024 Набор параметров B	1024

Совет. Рекомендуется использовать параметры алгоритма, предлагаемые по умолчанию. Данные параметры характеризуются наибольшей скоростью вычисления и проверки электронной подписи, шифрования и расшифрования.

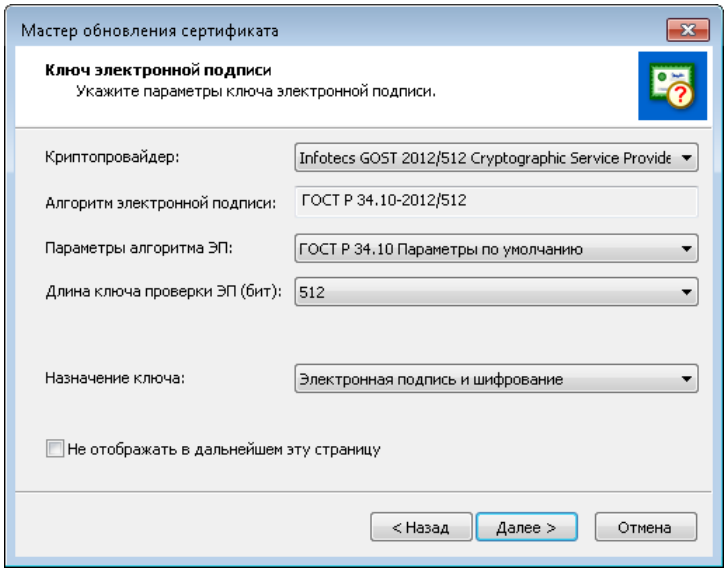


Рисунок 114. Выбор алгоритма и его параметров

2.3 Нажмите **Далее**.

3 На странице **Контейнер с ключом электронной подписи** укажите место хранения контейнера:

- папку на диске,
- устройство с указанием его параметров и ПИН-кода.

Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства.

После этого нажмите **Далее**.

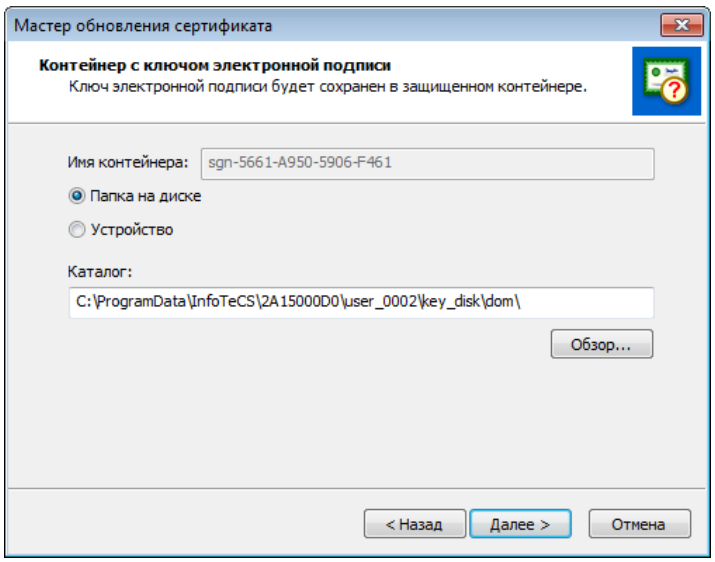


Рисунок 115. Указание места хранения контейнера ключей

4 На странице **Срок действия сертификата** задайте желаемый срок действия обновляемого сертификата удобным для вас способом, после чего нажмите **Далее**.

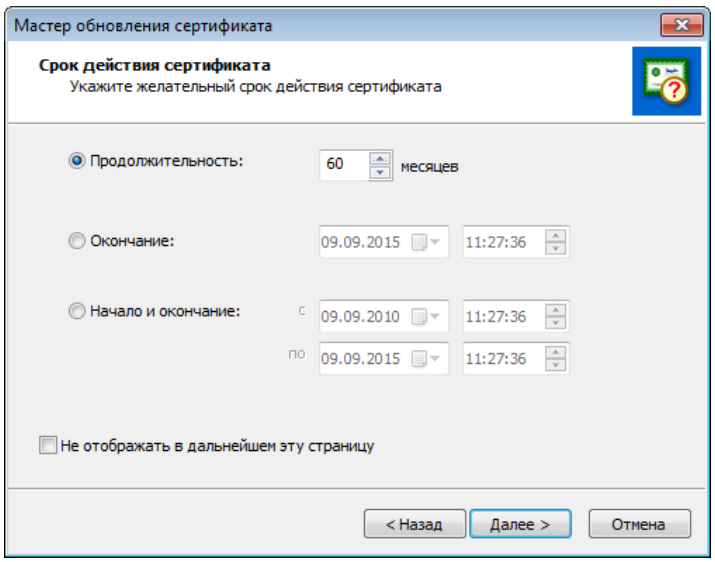


Рисунок 116. Указание желаемого срока действия сертификата

5 На странице **Готовность к созданию запроса на сертификат**:

- Убедитесь в правильности параметров, заданных на предыдущих страницах мастера. При необходимости изменения параметров вернитесь на нужную страницу с помощью кнопки **Назад**.

- При необходимости печати информации о запросе на принтере, используемом по умолчанию на данном сетевом узле, убедитесь в том, что установлен флажок **Печатать информацию о запросе**. В противном случае снимите флажок.

После этого нажмите **Далее**.

6 При появлении электронной рулетки следуйте указаниям окна.

Примечание. В случае если в рамках текущей сессии электронная рулетка уже была запущена, данное окно не появится.

---

7 На странице **Завершение работы мастера обновления сертификата** нажмите **Готово**.

В результате запрос на обновление сертификата будет передан в программу ViPNet Удостоверяющий и ключевой центр.

Примечание. Время ожидания ответа от программы ViPNet Удостоверяющий и ключевой центр может значительно варьироваться в зависимости от параметров настройки этой программы. Если программа ViPNet Удостоверяющий и ключевой центр настроена на автоматическую обработку запросов на сертификаты, время ожидания ответа не превышает 5 минут. Если обработка запросов в программе ViPNet Удостоверяющий и ключевой центр осуществляется вручную, время ожидания ответа не ограничено. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Если запрос на обновление сертификата в программе ViPNet Удостоверяющий и ключевой центр будет удовлетворён, на сетевой узел поступит обновлённый сертификат. Если изданный сертификат был введён в действие и назначен текущим автоматически (см. Ввод в действие автоматически), в окне **Менеджер сертификатов** для запроса, по которому был издан сертификат, будет отображаться статус **сертификат введён в действие** (см. Просмотр запроса на сертификат).

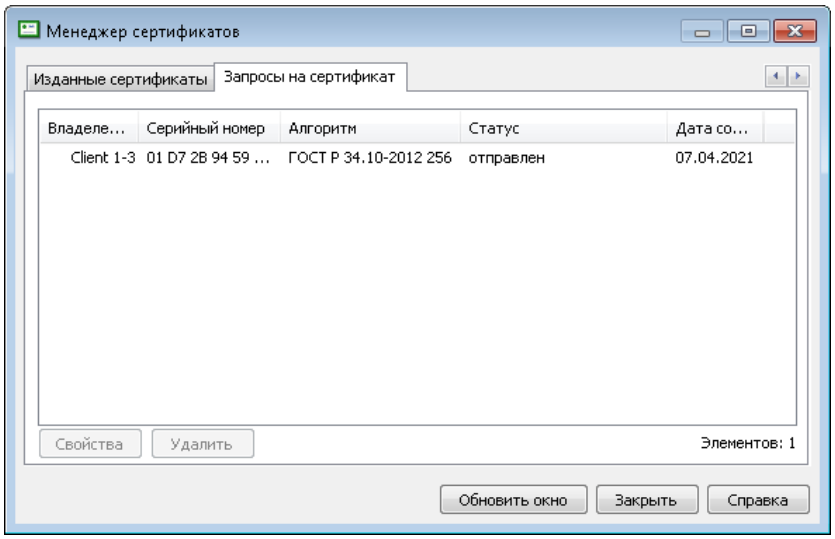


Рисунок 117. Статус запроса в случае ввода сертификата в действие

Если сертификат был получен, но не введён в действие автоматически, для запроса, по которому он был издан, будет отображаться статус **удовлетворён**. Выполните в данном случае ввод сертификата в действие вручную (см. Ввод в действие вручную).

Если запрос на обновление сертификата в программе ViPNet Удостоверяющий и ключевой центр будет отклонён, сертификат не будет издан. Запрос на сертификат будет иметь статус **отклонён**. Обратитесь к администратору программы ViPNet Удостоверяющий и ключевой центр для уточнения причин отклонения запроса.

Ввод сертификата в действие

Для того чтобы использовать сертификат, полученный из программы ViPNet Удостоверяющий и ключевой центр, необходимо ввести этот сертификат в действие. При этом сертификат сопоставляется с закрытым ключом и устанавливается в контейнер.

Ввод в действие автоматически

Для того чтобы ввод в действие сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр, выполнялся автоматически, убедитесь в том, что в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** установлен флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**, а также флажок **Автоматически вводить в действие сертификаты, изданные по инициативе администратора УКЦ**.

При наличии данных флажков сертификаты будут вводиться в действие автоматически в течение часа с момента их получения. Сертификаты, изданные по вашим запросам, смогут вводиться в действие автоматически только в том случае, если доступны контейнеры с соответствующими ключами электронной подписи. В противном случае они могут быть введены в действие только вручную (см. Ввод в действие вручную).

Внимание! Если контейнер с ключом электронной подписи хранится в папке на диске, то он доступен всегда. Если контейнер хранится на внешнем устройстве, то он будет доступен, если устройство подключено и сохранен ПИН-код к нему или ПИН-код уже вводился в рамках текущей сессии.

При вводе в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр, появится окно **Предупреждение сервиса безопасности** с соответствующим сообщением (см. Сертификат, изданный по инициативе администратора, введён в действие).

Ввод в действие вручную

Ввод сертификатов, полученных из программы ViPNet Удостоверяющий и ключевой центр, в действие вручную требуется выполнять в следующих случаях:

- Если не установлены флажки, позволяющие выполнять автоматический ввод сертификатов в действие.
- При автоматическом вводе сертификата в действие был недоступен контейнер с соответствующим ключом электронной подписи.

Чтобы вручную ввести в действие полученный сертификат, выполните следующие действия:

1 В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**, после чего нажмите **Изданные сертификаты**.

2 В окне **Менеджер сертификатов** на вкладке **Изданные сертификаты** выберите полученный сертификат, который необходимо ввести в действие, после чего нажмите **Ввести в действие**.

В результате введённый 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).

Смена текущего сертификата

Если у вас есть несколько действительных личных сертификатов, вы можете использовать любой из них в качестве текущего. Текущий сертификат используется программой ViPNet Client по умолчанию при подписании письма или зашифровании файла.

Внимание! Если при обновлении сертификата новый сертификат, изданный по запросу пользователя, передан на сетевой узел в составе ключей, для его использования необходимо назначить этот сертификат текущим. Чтобы делать это автоматически, в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** установите флажок **Автоматически вводить в действие сертификаты, изданные по запросу пользователя**. При этом новый сертификат станет текущим только в том случае, если старый сертификат недействителен.

Для выбора действительного личного сертификата в качестве текущего:

1 В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**, после чего нажмите **Выбрать**.

Если у вас есть хотя бы один действительный личный сертификат, появится окно **Назначение сертификата текущим** 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 сертификатов из хранилища ОС** (см. Дополнительные настройки параметров безопасности).

Если не найден ни один действительный личный сертификат, появится окно с сообщением «Нет действительных сертификатов с действительным ключом электронной подписи».

2 В окне **Назначение сертификата текущим** выберите нужный сертификат, при необходимости воспользовавшись кнопкой **Свойства** для просмотра подробной информации о сертификате, после чего нажмите **OK**.

Примечание. В качестве текущего допускается использовать сертификат, который введён в действие. Изданный, но не введённый в действие личный сертификат необходимо сначала ввести в действие (см. Ввод сертификата в действие), а затем назначить текущим.

При успешном выполнении описанных действий выбранный сертификат назначается текущим. При этом на вкладке **Ключи** в группе **Электронная подпись** меняется информация о контейнере ключей, с которым сопоставлен выбранный сертификат.

Работа с запросами на сертификаты

Работа с запросами на сертификаты выполняется в окне **Менеджер сертификатов** на вкладке **Запросы на сертификат**.

Для вызова окна **Менеджер сертификатов**:

1 В окне **Настройка параметров безопасности** откройте вкладку **Электронная подпись**.

2 Нажмите **Запросы на сертификат**.

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 **Свойства** или дважды щёлкните 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**.

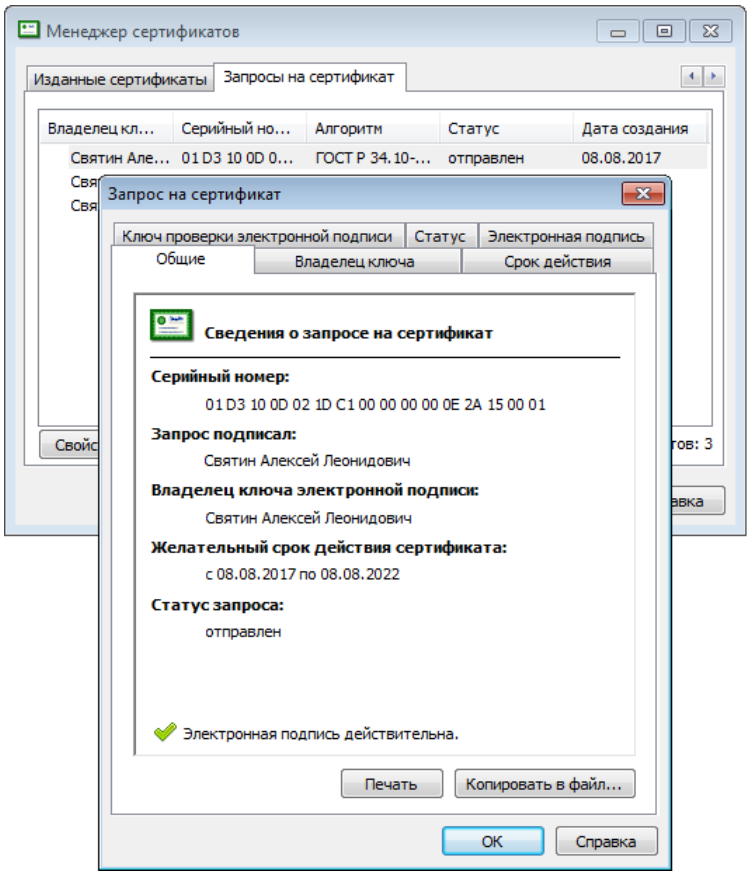


Рисунок 118. Просмотр подробной информации о запросе на сертификат

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 **Удалить**.

2 В окне подтверждения нажмите **Да**.

Информация о запросе будет удалена. Удалённый запрос не будет отображаться на вкладке **Запросы на сертификат**, при этом сертификат, изданный по этому запросу, сохранится.

Экспорт сертификата

В программе ViPNet можно выполнить экспорт сертификата пользователя в различные форматы. Выбор формата экспорта зависит от целей, для которых проводится данный экспорт.

Экспорт сертификата может понадобиться для выполнения следующих задач:

- архивирование сертификата;
- копирование сертификата для использования на другом компьютере;

- отправка сертификата другому пользователю для организации обмена зашифрованными сообщениями;
- просмотр сертификата в удобной форме.

Для экспорта сертификата в файл определённого формата:

1 Вызовите окно **Сертификат** для того сертификата, который необходимо экспортировать (см. Просмотр сертификатов).

2 Откройте вкладку **Состав**, после чего нажмите **Копировать в файл**.

3 На начальной странице мастера экспорта сертификатов нажмите **Далее**.

Совет. Если при последующих запусках мастера желательно пропускать первую страницу, установите на ней флажок **Не отображать в дальнейшем эту страницу**.

---

4 На странице **Формат экспортируемого файла** выберите один из предлагаемых форматов (см. Форматы экспорта сертификатов), после чего нажмите **Далее**.

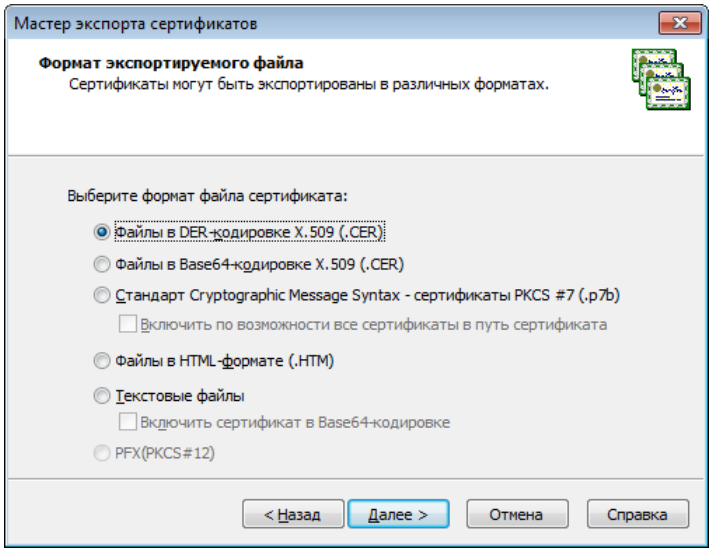


Рисунок 119. Выбор формата файла

5 На странице **Имя файла экспорта** укажите полный путь к создаваемому файлу, после чего нажмите **Далее**.

6 На странице **Завершение работы мастера экспорта сертификатов** убедитесь в правильности параметров экспорта, заданных на предыдущих страницах мастера, после чего нажмите **Готово**.

7 В окне с сообщением об успешном экспорте нажмите **OK**.

Форматы экспорта сертификатов

При выборе формата экспорта сертификата следует руководствоваться перечисленными положениями.

- При экспорте сертификатов для импорта на компьютер с ОС Windows предпочтительный формат экспорта — PKCS #7, поскольку этот формат обеспечивает сохранение цепочки центров сертификации (пути сертификации). Некоторые приложения требуют при импорте сертификата из файла представления в виде DER или Base64. Поэтому формат экспорта необходимо выбирать в соответствии с требованиями приложения или системы, в которую этот сертификат предполагается импортировать.
- Для просмотра сертификата и вывода его на печать используются текстовый и HTML-форматы.

Ниже приведена подробная информация о каждом из форматов экспорта сертификатов, поддерживаемых ПО ViPNet.

- **Стандарт Cryptographic Message Syntax (PKCS #7)**

  Формат PKCS #7 позволяет передавать сертификат и все сертификаты в цепочке сертификации с одного компьютера на другой или с компьютера на внешнее устройство. Файлы PKCS #7 обычно имеют расширение `.p7b` и совместимы со стандартом ITU-T X.509. Формат PKCS#7 разрешает такие атрибуты, как удостоверяющие подписи, связанные с обычными подписями. Для таких атрибутов, как метка времени, можно выполнить проверку подлинности вместе с содержимым сообщения. Дополнительные сведения о формате PKCS#7 см. на веб-сайте RSA Laboratories.

- **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, определённый 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).

- **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, что обеспечивает целостность информации при её передаче по сети. Протокол S/MIME обеспечивает работу некоторых криптографических служб безопасности для приложений электронной почты, включая механизм неотрекаемости (с помощью электронных подписей), секретность и безопасность данных (с помощью

кодирования, процесса проверки подлинности и целостности сообщений). Файлы сертификатов Base64 имеют расширение `.cer`.

MIME (Multipurpose Internet Mail Extensions, спецификация RFC 1341 и последующие) определяет механизмы кодирования произвольных двоичных данных для передачи по электронной почте.

Дополнительные сведения см. в документе «RFC 2633 S/MIME Version 3 Message Specification, 1999» на веб-узле Internet Engineering Task Force (IETF).

- **Файлы в HTML-формате**

  Файлы для просмотра и печати в любом веб-браузере, а также в офисных и других программах, поддерживающих язык разметки гипертекста HTML.

- **Текстовые файлы**

  Файлы в кодировке ANSI для просмотра в любом текстовом редакторе и вывода на печать.

- **Файлы в формате PFX (PKCS #12)**

  Формат PFX (PKCS#12) поддерживает безопасное хранение сертификата и закрытого ключа, соответствующего сертификату пользователя, может содержать все сертификаты в цепочке доверия от сертификата пользователя до корневого сертификата удостоверяющего центра и CRL.

Работа с контейнером ключей

Контейнер ключей содержит ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи, если он установлен в контейнер.

В программе ViPNet Client вы можете выполнять следующие операции с контейнером ключей:

- Установка (см. Установка контейнера ключей).

  Установка нового контейнера ключей указанным способом требуется в том случае, если у вас есть новый контейнер ключей, и вы хотите его использовать.

  Вы также можете установить контейнер ключей с помощью программы ViPNet CSP, входящей в состав ViPNet Client. Но при этом использовать ключ и сертификат из такого контейнера ключей вы сможете только в том случае, если вам разрешено использование внешних сертификатов (см. Дополнительные настройки параметров безопасности). В противном случае, они будут вам недоступны, даже если контейнер ключей будет установлен.

- Смена и удаление сохранённого пароля к контейнеру (см. Смена пароля к контейнеру).

  Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль. Удаление сохранённого пароля может потребоваться, если изменился регламент безопасности вашей организации и хранение пароля на компьютере стало недопустимым.

- Изменение расположения контейнера (см. Перенос контейнера ключей).

  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 электронной 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).

Внимание! В сети ViPNet, управляемой с помощью ПО ViPNet Administrator, выполнять различные операции с контейнером ключей может только пользователь, который обладает правом подписи. Такое право предоставляется пользователям сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

Для работы с контейнером ключей:

1 Откройте вкладку **Ключи**.

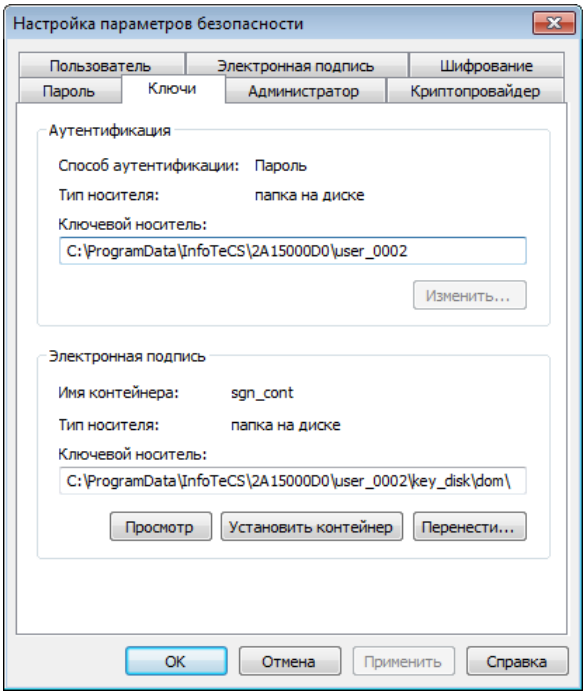


Рисунок 120. Работа с контейнером ключей

2 В группе **Электронная 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);
  - удаления пароля (см. Удаление сохранённого на компьютере пароля к контейнеру ключей);
  - проверки соответствия ключа электронной подписи сертификату (см. Проверка контейнера ключей);
  - удаления ключа электронной подписи.
- **Установить контейнер** — для установки нового контейнера ключей (см. Установка контейнера ключей).
- **Перенести** — для изменения расположения контейнера ключей (см. Перенос контейнера ключей).

Примечание. В группе **Электронная подпись** отображается информация о ключе электронной подписи, соответствующем текущему сертификату.

Смена пароля к контейнеру

Заданный пароль к контейнеру ключей рекомендуется использовать в течение 1 года. По истечении этого срока следует задать новый пароль. Описанный ниже сценарий смены пароля к контейнеру ключей применяется только для контейнеров, которые были созданы в программе ViPNet Registration Point, либо были перенесены из папки ключей пользователя (по умолчанию `C:\ProgramData\InfoTeCS\ViPNet Registration Point\Mftp_Transport\<идентификатор пользователя>\key_disk\dom`) в другую папку. В остальных случаях смена пароля к контейнеру предполагает смену пароля пользователя ViPNet (см. Смена пароля пользователя).

Для смены пароля к контейнеру ключей:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите **Просмотр**.

2 В окне **Свойства контейнера ключей** нажмите **Сменить пароль**.

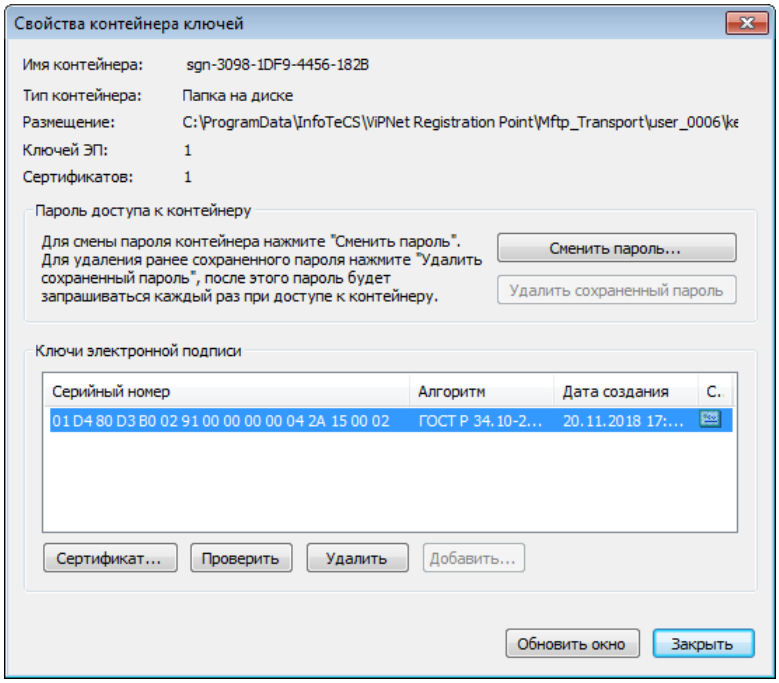


Рисунок 121. Смена пароля к контейнеру ключей

3 При появлении сообщения «Для данного контейнера смена пароля возможна только в настройке безопасности приложений ViPNet» нажмите **OK**, после чего завершите работу с окном **Свойства контейнера ключей** и измените пароль пользователя (см. Смена пароля пользователя).

4 В окне **Пароль** введите текущий пароль доступа к контейнеру ключей и нажмите **OK**.

Примечание. Если ранее был установлен режим **Сохранить пароль**, то окно **Пароль** не появится.

---

5 В окне **ViPNet CSP - смена пароля контейнера ключей** укажите текущий пароль, задайте и подтвердите новый пароль. Нажмите **OK**.

Внимание! Запрещается вводить пароль при помощи операций копирования и вставки через буфер обмена.

Чтобы сохранить пароль для последующих обращений к контейнеру ключей, установите флажок **Сохранить пароль**.

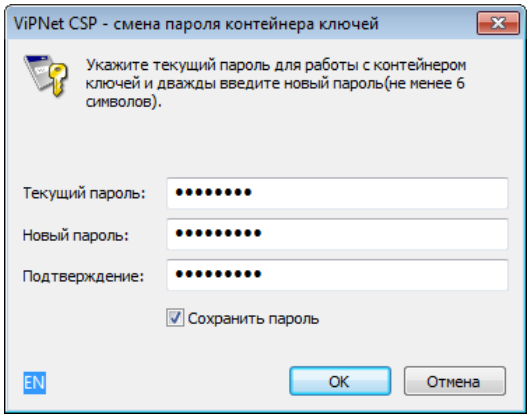


Рисунок 122. Смена пароля доступа к контейнеру ключей

Внимание! Не создавайте пароль длиной в 32 символа и более. Пароли с такой длиной не могут использоваться в текущих версиях приложений ViPNet. Данное ограничение связано с существующим алгоритмом передачи пароля в криптопровайдер. В соответствии с этим алгоритмом длина пароля не должна превышать 31 символ.

Удаление сохранённого на компьютере пароля к контейнеру ключей

Удаление сохранённого пароля к контейнеру ключей может потребоваться, если изменились условия эксплуатации пароля или регламент вашей организации, вследствие чего хранение пароля на компьютере стало недопустимым.

Для удаления сохранённого пароля к контейнеру ключей и отображения окна ввода пароля при доступе к контейнеру:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите **Просмотр**.
2. В окне **Свойства контейнера ключей** нажмите **Удалить сохранённый пароль**.

Сохранённый пароль будет удалён. Теперь пароль необходимо вводить всякий раз при доступе к контейнеру ключей.

Проверка контейнера ключей

Проверка контейнера ключей позволяет убедиться, что файл контейнера не повреждён, хранящиеся в контейнере сертификат и ключ электронной подписи соответствуют друг другу и могут быть использованы для работы с защищёнными документами.

Чтобы проверить контейнер ключей:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите **Просмотр**.

2 В окне **Свойства контейнера ключей** нажмите **Проверить**.

Программа сформирует фрагмент данных, который будет подписан с помощью ключа электронной подписи. После чего будет выполнена проверка электронной подписи. Таким образом, можно выяснить пригодность ключа электронной подписи и его соответствие сертификату ключа проверки электронной подписи, хранящемуся в контейнере.

Примечание. Проверка возможна только в том случае, если в контейнере ключей есть сертификат, соответствующий ключу электронной подписи. Сертификат может отсутствовать в контейнере ключей, если он размещён 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 ключа электронной подписи проверка действительности сертификата (срок его действия, отсутствие в списках аннулированных сертификатов и прочее) не выполняется.

Установка контейнера ключей

Если у вас есть контейнер ключей с сертификатом, который вы хотите использовать в программе ViPNet Client, то вы можете его установить в окне **Настройка параметров безопасности** на вкладке **Ключи**. Данная ситуация может возникнуть в следующих случаях:

- Вы переносите контейнер ключей с другого компьютера.
- Вы сформировали запрос на сертификат (см. Процедура обновления ключа электронной подписи и сертификата) и получили на него сертификат из программы ViPNet Удостоверяющий и ключевой центр не по сети, а в отдельном файле.
- У вас есть контейнер ключей, сформированный с помощью ViPNet CSP (см. Криптопровайдер ViPNet CSP). О том, как сформировать контейнер ключей в ViPNet CSP, см. в документе «ViPNet CSP. Руководство пользователя».

Внимание! Нельзя установить контейнер ключей, сформированный в ПО ViPNet версии ниже 3.2.x.

Вы также можете установить контейнер ключей с помощью программы ViPNet CSP, входящей в состав ViPNet Client. Но при этом использовать ключ и сертификат из такого контейнера ключей вы сможете только в том случае, если вам разрешено использование внешних сертификатов (см. Дополнительные настройки параметров безопасности). В противном случае, они будут недоступны вам, даже если контейнер ключей будет установлен.

Для установки контейнера ключей выполните следующие действия:

1 В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите **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.

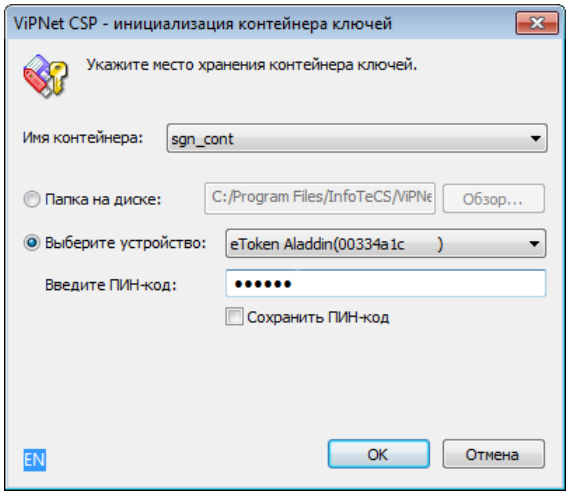


Рисунок 123. Установка контейнера ключей

Нажмите **OK**.

3 В окне **Назначение сертификата текущим** выберите соответствующий сертификат и нажмите **OK**.

В результате ключ электронной подписи и сертификат, которые хранятся в выбранном контейнере, будут назначены текущими. Информация о сертификате, который хранится в установленном контейнере, отобразится на вкладке **Электронная подпись**.

Перенос контейнера ключей

Перенос текущего контейнера ключей может потребоваться для изменения расположения контейнера, например, если хранение контейнера по прежнему пути было признано небезопасным.

Примечание. Перенести можно только контейнер с ключами, сформированными в ПО ViPNet версии не ниже 3.2.x.

Не рекомендуется переносить контейнер вручную, меняя его расположение на диске. Если это произошло, выполните установку контейнера (см. Установка контейнера ключей).

Не поддерживается перенос контейнера ключей на устройства с аппаратной реализацией криптографических функций.

Для того чтобы поменять расположение контейнера ключей:

1. В окне **Настройка параметров безопасности** на вкладке **Ключи** нажмите **Перенести**.
2. В окне **ViPNet CSP – инициализация контейнера ключей** укажите новое место хранения контейнера ключей:
   - папку на диске;
   - устройство с указанием его параметров и ПИН-кода.

   Примечание. Для использования какого-либо внешнего устройства необходимо подключить это устройство и установить для него драйверы. Перечень поддерживаемых устройств хранения данных и полезная информация об использовании устройств содержится в разделе Внешние устройства).

   Укажите пароль для доступа к контейнеру ключей, если появилось соответствующее сообщение.

Контейнер ключей будет перенесён по указанному пути.

Установка сертификата в контейнер ключей

Если по каким-то причинам ваш сертификат не находится в контейнере ключей, вы можете установить его в контейнер ключей вручную. Установить сертификат в контейнер можно как в программе ViPNet CSP, так и в окне **Настройка параметров безопасности**. При этом в обоих случаях контейнер ключей должен быть установлен в программу.

Совет. Сохранение сертификата в одном контейнере с ключом электронной подписи удобно, если контейнер планируется переносить и устанавливать на другом компьютере.

Установка сертификата в контейнер с помощью программы ViPNet CSP описана в документе «ViPNet CSP. Руководство пользователя». Чтобы установить сертификат в контейнер ключей в окне **Настройка параметров безопасности**, выполните следующие действия:

1. Перейдите на вкладку **Ключи**.
2. Установите контейнер ключей, если он не установлен (см. Установка контейнера ключей).
3. Перейдите в свойства контейнера с помощью кнопки **Просмотр**.
4. В окне **Свойства контейнера ключей** нажмите **Добавить**.
5. Укажите файл сертификата, который соответствует ключу электронной подписи, находящемуся в контейнере. Если будет установлено, что указанный сертификат соответствует ключу электронной подписи, он будет добавлен в контейнер. В противном случае, появится соответствующее сообщение.

A

Возможные неполадки

Сбор диагностической информации при возникновении неполадок

При обращении в службу поддержки ИнфоТеКС потребуется предоставить информацию о компьютере, на котором установлено ПО ViPNet. На основе этой информации сотрудники смогут выявить причины неполадок и определить способы их устранения.

Информацию о компьютере вы можете получить с помощью утилиты lumpdiag, встроенной в ПО ViPNet Client. Утилита собирает информацию о компьютере (например, информацию о системе, криптографическом окружении и так далее) независимо от работоспособности ПО ViPNet Client.

Примечание. В процессе работы утилиты сбор вашей конфиденциальной информации не производится. Компания ИнфоТеКС ответственно подходит к защите вашей личной информации и принимает все меры для предотвращения несанкционированного доступа или разглашения информации, которую вы нам предоставляете.

С помощью утилиты вы можете собрать необходимую информацию либо в архив, либо в папку `\SysEnv`, которая автоматически создаётся в папке установки ПО ViPNet Client.

Для работы с утилитой запустите командную строку от имени администратора и перейдите в папку установки ПО ViPNet Client.

Для получения справки по утилите в командной строке введите: `lumpdiag -h`, где `h` — ключ, который вызывает справку. Если утилита вызвана без указания каких-либо ключей, считается, что она вызвана с данной опцией.

Для сбора информации в командной строке введите:

`lumpdiag -a [<archive file>]`, где:

- `-a` — ключ, который запускает процесс сбора информации на компьютере;
- `<archive file>` — путь к архиву, в который будут упакованы файлы, собранные в результате работы утилиты.

  Если при сборе информации параметр `<archive file>` не был указан, то собранная информация будет сохранена в папке `\SysEnv` папки установки ПО ViPNet Client (по умолчанию: `c:\Program Files (Program Files (x86))\InfoTeCS\ViPNet Client`). Если папка `\SysEnv` уже существует, то утилита запросит у вас разрешение на перезапись содержимого папки.

Возможные неполадки

Невозможно установить или обновить программу

Установку, обновление или удаление ViPNet Client может блокировать:

- программа Kaspersky;
- программа 360 Total Security.

Установку блокирует программа Kaspersky

Функция самозащиты программы Kaspersky может заблокировать установку или обновление ViPNet Client.

Для установки ViPNet Client выполните одно из действий:

- отключите самозащиту Kaspersky (может быть заблокировано политикой безопасности, принятой в вашей организации);
- запросите в службе поддержки Kaspersky патч 3140 (подходит для ПО Kaspersky Endpoint Security), установите патч и перезагрузите компьютер.

Внимание! Если вы приостановите антивирусную защиту или выйдете из программы Kaspersky, проблема не будет решена. Необходимо отключить самозащиту описанным ниже способом.

Чтобы временно отключить самозащиту Kaspersky:

1. В окне программы Kaspersky Anti-Virus или Endpoint Security выберите **Настройка**.
2. На странице **Настройка** выберите раздел **Дополнительно** и затем **Самозащита**.
3. В **Параметрах самозащиты** снимите флажок **Включить самозащиту**.
4. В окне подтверждения нажмите **Продолжить**.

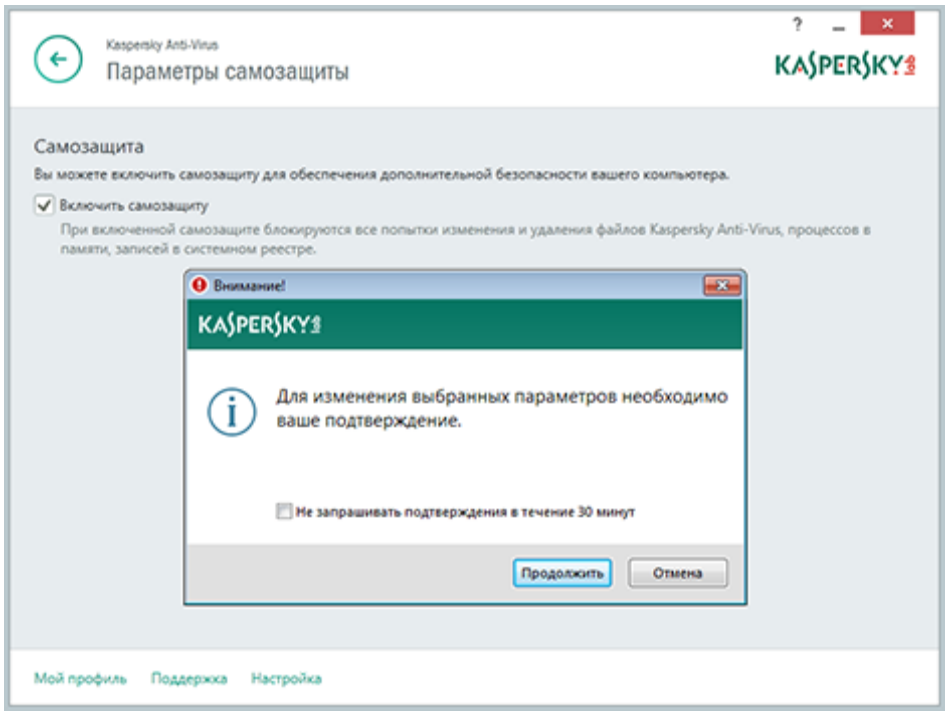


Рисунок 124. Отключение самозащиты в антивирусе Касперского

После отключения самозащиты Kaspersky заново начните установку ViPNet Client. Отключение самозащиты требуется только на время установки.

Установку блокирует программа 360 Total Security

Функция защиты реестра и файловой системы программы 360 Total Security может заблокировать установку ViPNet Client.

Чтобы установить программу ViPNet Client, временно отключите защиту:

1. В программе 360 Total Security щёлкните значок  в верхнем левом углу программы.
2. На верхней панели нажмите **Настройка**.
3. Выберите режим защиты **Настраиваемый**.
4. Отключите функции **Защита реестра** и **Файл защиты системы**.

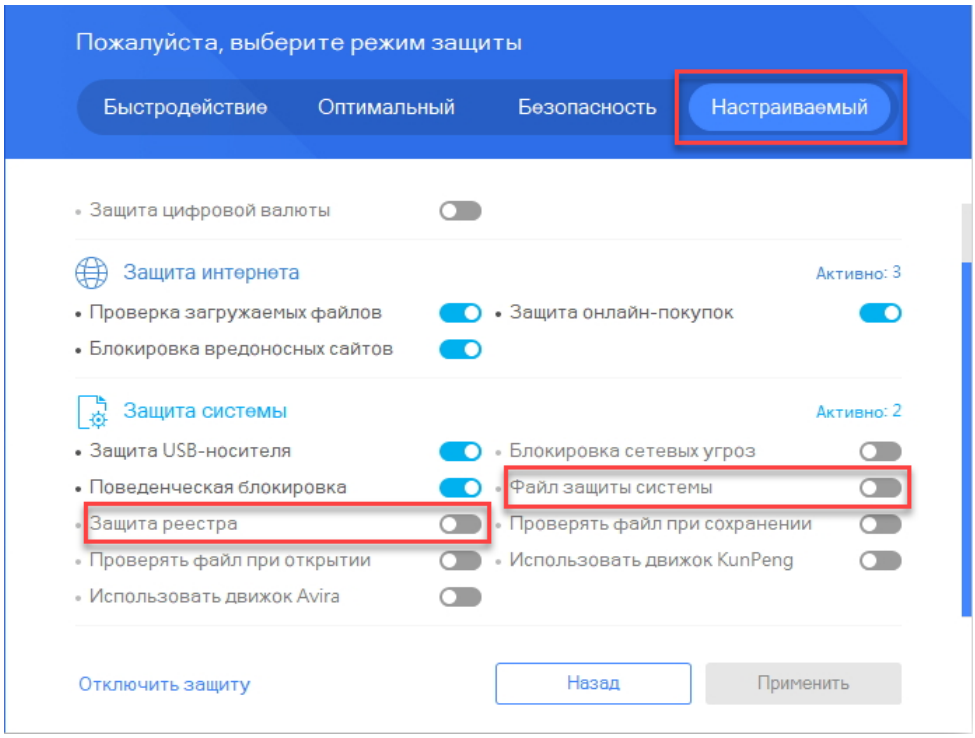


Рисунок 125. Настройка 360 Total Security

5 Установите программу ViPNet Client и файл ключей и справочников DST.

6 Включите функции **Защита реестра** и **Файл защиты системы** в программе 360 Total Security.

После обновления не работает обмен межсетевой информацией

Возможные причины:

- В доверенных сетях на узлах с ViPNet ЦУС установлена старая версия ViPNet Client.
- В доверенных сетях на узлах с центром управления ViPNet Prime установлена старая версия ViPNet Client 5.

Чтобы обмен межсетевой информацией работал, попросите администраторов доверенных сетей обновить ViPNet Client на этих узлах до версии:

- ViPNet Client for Windows 4.5.3 hotfix 7 и выше
  или ViPNet Client for Windows 4.5.5 hotfix 9 и выше,
- ViPNet Client 5 for Windows 5.1 и выше,
- ViPNet Client 5 for Linux 5.0.0 или 5.1.3 и выше.

Не применяется обновление ПО, отправленное из ViPNet ЦУС

Причины неудачного обновления ПО могут быть следующими:

- Программе установки не удалось завершить работу всех компонентов ПО ViPNet (например, какие-то компоненты ПО ViPNet были запущены в сессии другого пользователя).

  Для решения проблемы завершите работу всех компонентов ПО ViPNet или перезагрузите компьютер.

- Установку блокирует антивирусная программа. Для решения проблемы перейдите к разделу Kaspersky или 360 Total Security.
- Возникли проблемы совместимости ПО ViPNet с вашим компьютером.

Для решения проблемы совместимости:

1. Убедитесь, что компьютер удовлетворяет системным требованиям для установки ПО ViPNet.
2. Перезагрузите компьютер, на котором не удалось обновить ПО ViPNet.

   Затем отправьте обновление из программы ViPNet Центр управления сетью и примите его на узле (см. Обновление, отправленное из ViPNet Центр управления сетью).
3. Запустите установку программы из установочного EXE-файла на каком-либо сетевом узле. Если при установке будут обнаружены проблемы совместимости, выполните предложенные рекомендации для всех компьютеров, на которые устанавливается ViPNet Client.

   Затем отправьте обновление из программы ViPNet Центр управления сетью и примите его на узле.
4. Если установить обновление не удалось, обратитесь в службу поддержки ИнфоТеКС (см. Сбор диагностической информации при возникновении неполадок).

Невозможно запустить ViPNet Client

Возможны следующие ситуации:

- Программа ViPNet Client была удалена с компьютера либо были удалены файлы, необходимые для её работы. Переустановите программу, либо обратитесь за помощью к администратору.
- Если на сетевом узле одновременно установлены программы ViPNet Registration Point и ViPNet Client и срок действия лицензии на роль «VPN-клиент» истёк, дальнейшая работа с программой ViPNet Registration Point будет невозможна. Для продолжения работы с программой ViPNet Registration Point необходимо обновить лицензию в программе ViPNet Центр управления сетью (см. документ «ViPNet Центр управления сетью. Руководство администратора», раздел «Обновление лицензии»).

- Если для входа в программу вы используете внешнее устройство, то отключите в программе ViPNet CSP все неиспользуемые устройства для аутентификации. Подробнее см. «ViPNet CSP 4.4. Руководство пользователя», раздел «Настройка списка опрашиваемых устройств».

ViPNet Client не запускается после загрузки Windows

Если на вашем компьютере работает несколько пользователей и компьютер находится не в домене, то после входа в Windows программа ViPNet Client может не запускаться автоматически.

Для исправления проблемы выполните следующие настройки:

Для Windows 10 версии 1709 и выше:

1 В меню **Пуск** выберите **Параметры** > **Учетные записи** > **Параметры входа**.

2 В разделе **Конфиденциальность** включите параметр **Использовать мои данные для входа, чтобы автоматически завершить настройку устройства после обновления**.

Для Windows 10 версии 1703 и ниже:

1 В меню **Пуск** выберите **Параметры** > **Обновление и безопасность** > **Центр обновления Windows** > **Дополнительные параметры**.

2 В разделе **Параметры обновления** установите флажок **Использовать мои данные для входа, чтобы автоматически завершить настройку устройства после обновления**.

Совет. Чтобы узнать версию Windows 10, в меню **Пуск** введите команду `winver` и нажмите клавишу **Enter**.

Невозможно произвести авторизацию пользователя ViPNet

При появлении такой ошибки:

1 Загрузите компьютер в безопасном режиме.

2 В меню **Пуск** выберите **ViPNet** > **Настройка компонентов ViPNet Client**.

3 На странице **Управление составом ViPNet Client** выберите **Восстановить**.

После восстановления программы запустите компьютер в обычном режиме.

Если приведённые действия не помогли войти в программу ViPNet, обратитесь в службу поддержки ИнфоТеКС.

Не найдены ключи пользователя или неверный пароль

В этом случае программа выдаёт следующее сообщение:

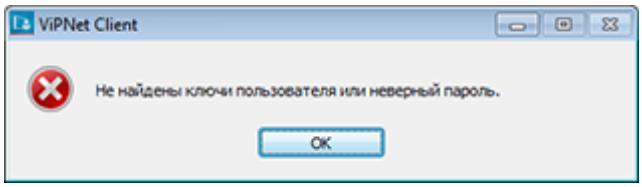


Рисунок 126. Сообщение о неверном пароле

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 ещё раз внимательно наберите пароль.
- Возможно, ключи пользователя установлены в папку, которая отличается от папки ключей пользователя по умолчанию.

  В этом случае в окне ввода пароля щёлкните значок  справа от кнопки **Настройка**, в меню выберите **Папка ключей пользователя** и укажите путь к папке ключей пользователя.

  Если операционная система ещё не загружена, в окне ввода пароля ViPNet нажмите **Отмена**. После загрузки операционной системы запустите ViPNet Client и укажите путь к папке ключей пользователя.

Ошибка при повторном разворачивании DST

Если пароль для входа в программу ViPNet Client сохранен в реестре, то после установки нового дистрибутива ключей при запуске программы может появиться сообщение об ошибке. В этом случае для первого входа в программу введите пароль. При последующих запусках программы ввод пароля не потребуется.

Не удаётся выполнить аутентификацию с помощью сертификата

Если вам не удаётся войти в программу ViPNet Client, используя для аутентификации сертификат и соответствующий ему ключ электронной подписи, которые хранятся на внешнем устройстве, это может быть вызвано одной из следующих причин:

- Внешнее устройство не обеспечивает аппаратную поддержку алгоритмов ГОСТ.
- Внешнее устройство хранения данных не поддерживает стандарт PKCS#11. Проверить, поддерживает ли ваше устройство этот стандарт, можно в разделе Внешние устройства.
- Срок действия выбранного сертификата истёк. При выборе недействительного сертификата появится соответствующее сообщение. В этом случае следует передать сертификат администратору вашего удостоверяющего центра для обновления.
- Выбранный сертификат присутствует в списке аннулированных сертификатов, который установлен в хранилище данного узла. При выборе аннулированного сертификата появится соответствующее сообщение. В этом случае следует обратиться к администратору вашего удостоверяющего центра.
- Выбранный сертификат не имеет назначения «Шифрование ключей». Это расширение должно отображаться в окне **Сертификат**, на вкладке **Состав**, в поле **Использование ключа**. В этом случае следует обратиться к администратору вашего удостоверяющего центра для переиздания сертификата.
- Вы используете внешнее устройство JaCarta с апплетом PKI. Запрос на сертификат для этого устройства следует создавать в ПО «Единый клиент JaCarta» версии 2.12 и выше, поскольку только в этом ПО возможна запись открытого ключа на устройство. Если использование «Единого клиента» невозможно, передайте устройство производителю для записи на него открытого ключа.

После обновления программы наблюдаются перебои в работе защищённой сети

После обновления ПО ViPNet Client на сетевых узлах могут не передаваться обновления справочников и ключей или письма Деловой почты. Это может быть связано с тем, что на некоторых сетевых узлах в настройках модуля MFTP указан канал SMTP/POP3, а новая версия программы не поддерживает передачу конвертов по этому каналу.

Для решения проблемы выполните следующие действия:

- По возможности обновите программу на всех сетевых узлах с ОС Windows до версии 4.5.1 или выше.

- На сетевых узлах Windows с прежней версией программы или программных координаторах на ОС Linux и ПАКах в настройках модуля MFTP замените канал SMTP/POP3 на MFTP

Подробнее для ПО Windows см. документ «ViPNet MFTP. Руководство администратора», раздел «Управление каналами передачи конвертов».

Подробнее для ПО Linux и ПАКов см. документ «Настройка с помощью командной строки», раздел «Выбор канала передачи конвертов».

Невозможно сохранить пароль

Сохранение пароля в реестре может противоречить регламенту безопасности вашей организации. Эта возможность определяется настройками программы ViPNet:

- в режиме работы администратора программы ViPNet Client (см. Дополнительные настройки параметров безопасности);
- в программе ViPNet Administrator.

Если вам необходимо сохранить пароль, обратитесь к администратору сетевого узла или администратору сети ViPNet.

Невозможно установить соединение с одним из защищённых узлов

Возможные причины:

- Сетевой узел выключен или на нем не запущена программа ViPNet Client.
- Нет ключей, необходимых для связи с сетевым узлом. Обратитесь к администратору сети ViPNet.
- Ваш компьютер физически не подключён к сети или не имеет выхода в интернет.

Невозможно подключиться к ресурсам в интернете

Возможные причины:

- Соединение с ресурсами интернета заблокировано фильтрами открытой сети или заблокирован IP-трафик компьютера. Убедитесь, что настроены сетевые фильтры, разрешающие соединение с требуемыми адресами (см. Создание фильтров для открытой

сети), а также в том, что IP-трафик компьютера не заблокирован (об этом свидетельствует, например, наличие в меню **Файл** > **Конфигурации** команды **Блокировать IP-трафик**).

- На компьютере установлена версия антивируса Avast, конфликтующая с ПО ViPNet. Обновите Avast до актуальной версии.

Медленное соединение с ресурсами в интернете

Если вы используете ПО Kaspersky и после установки программы ViPNet Client соединение с сайтами в интернете происходит очень медленно, выполните следующие настройки:

1 В программе Kaspersky Total Security нажмите **Настройка**, затем выберите раздел **Дополнительно** > **Сеть**.

2 На странице **Параметры сети** снимите флажок **Внедрять в трафик скрипт взаимодействия с веб-страницами**.

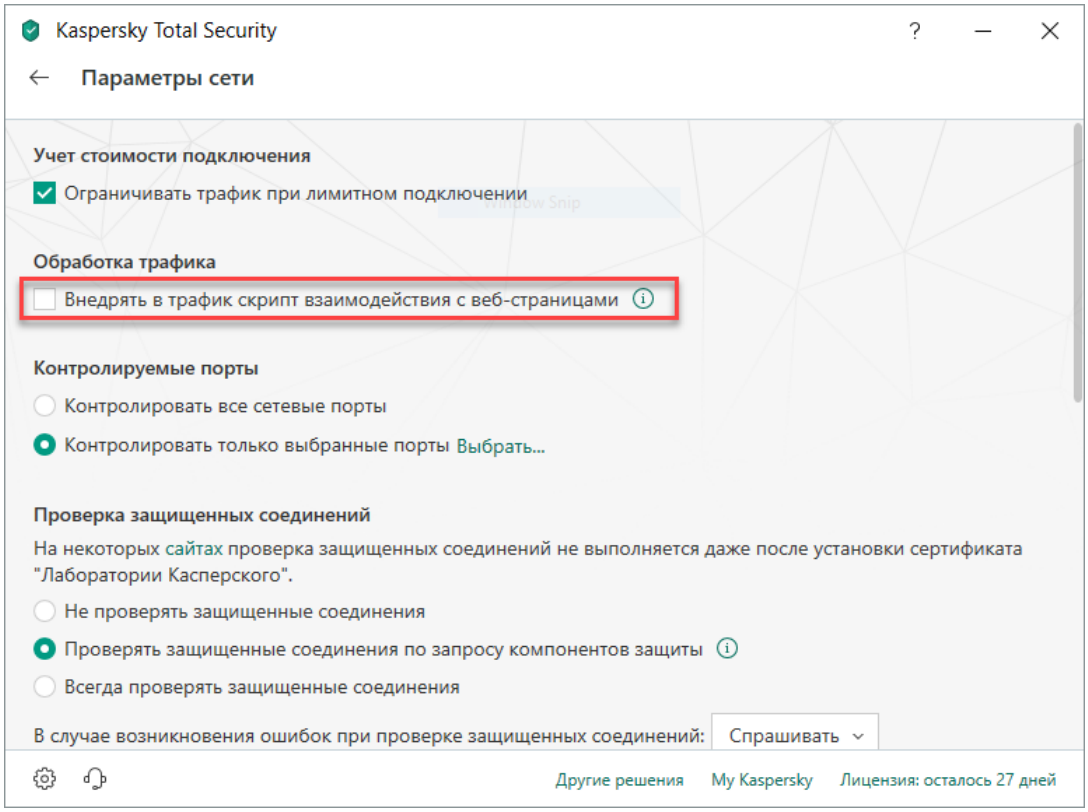


Рисунок 127. Отключение скрипта взаимодействия с веб-страницами

Невозможно подключиться к ресурсам по доменному имени

Проблема может появиться, если вы используете антивирус Avast или AVG Internet Security. При этом других неполадок в работе сети нет. Для решения проблемы выполните следующие действия:

1. В главном окне программы Avast или AVG выберите **Меню** > **Настройки** > **Компоненты**.
2. В программе AVG в разделе **Компоненты** отключите компоненты **Усиленный (Улучшенный) брандмауэр** и **Защита от поддельных сайтов**.
3. В программе Avast в разделе **Безопасность** отключите компоненты **Брандмауэр** и **Подлинные сайты**.

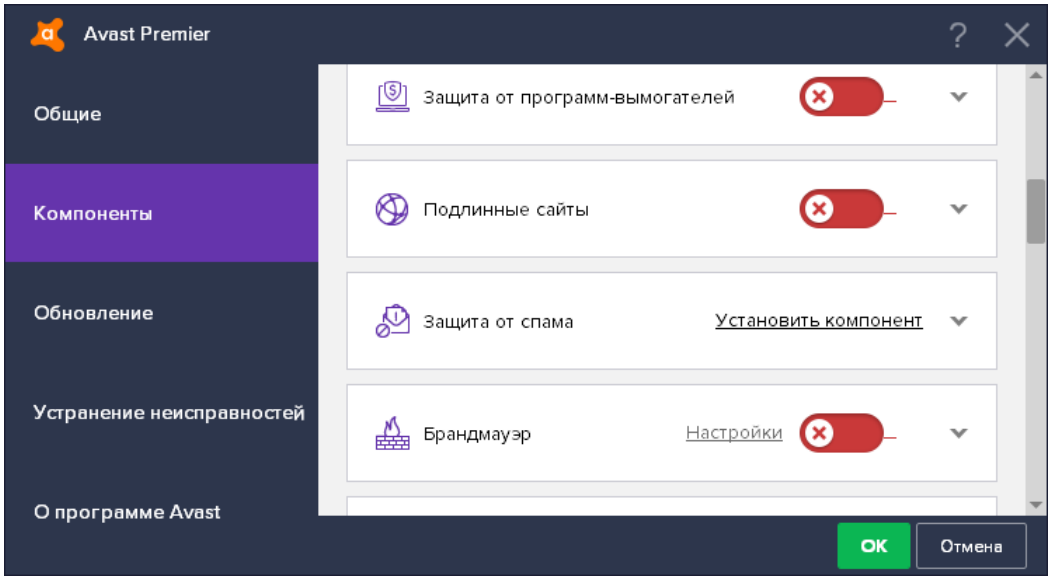


Рисунок 128. Отключение брандмауэра и защиты сайтов в Avast

Невозможно получить и отправить сообщения по электронной почте

Проблема может появиться, если вы используете антивирус Avast или AVG Internet Security. При этом других неполадок в работе сети нет. Для решения проблемы воспользуйтесь одним из способов:

- Отключите сетевое перенаправление портов для почтовых клиентов.

  Для этого в главном окне программы Avast или AVG выберите **Меню** > **Настройки** > **Устранение неисправностей**. Затем в разделе **Настройки перенаправления** удалите все записи с номерами портов.

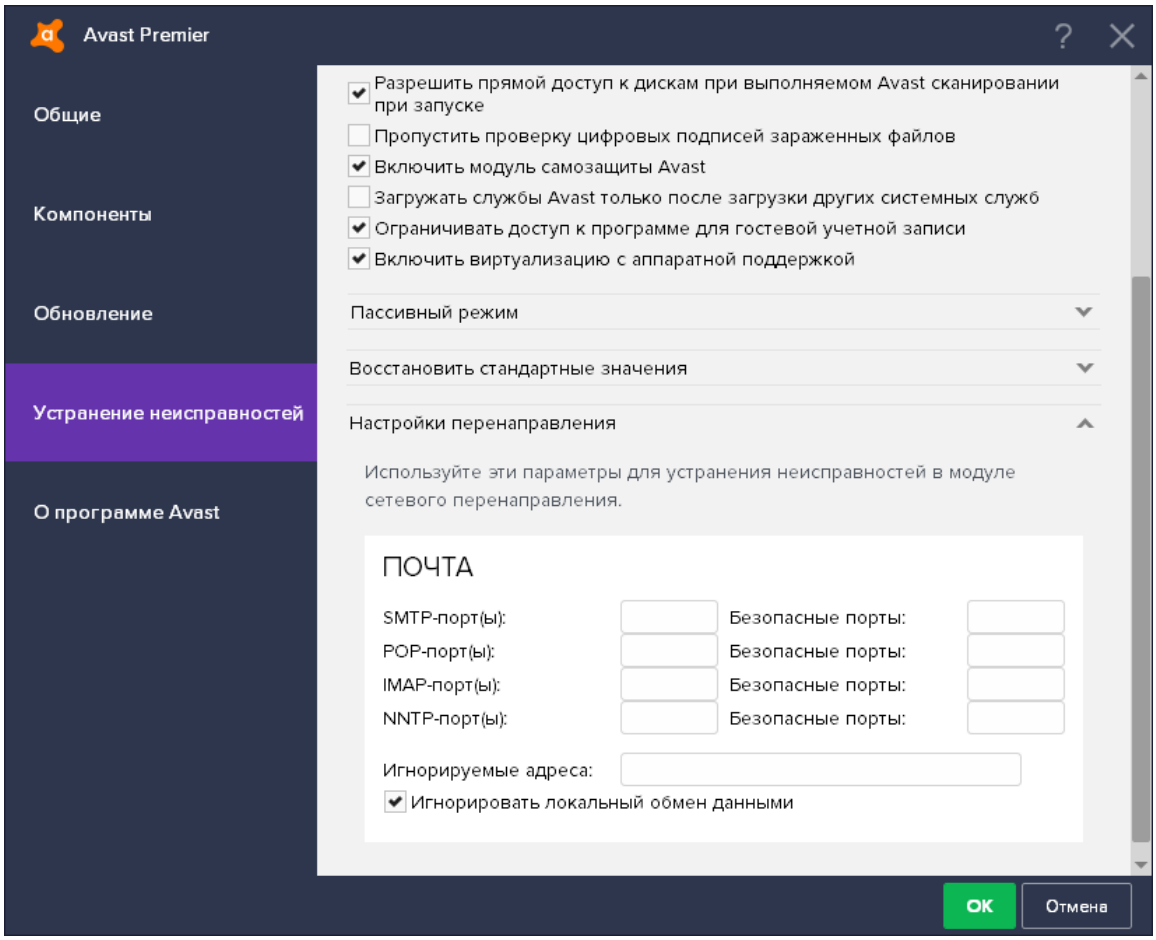


Рисунок 129. Удаление записи о портах в Avast

- Отключите защиту почты и защиту от спама.

Для этого в главном окне программы Avast или AVG выберите **Меню** > **Настройки** > **Компоненты**. Затем в разделе **Безопасность** отключите компоненты **Защита почты** и **Защита от спама**.

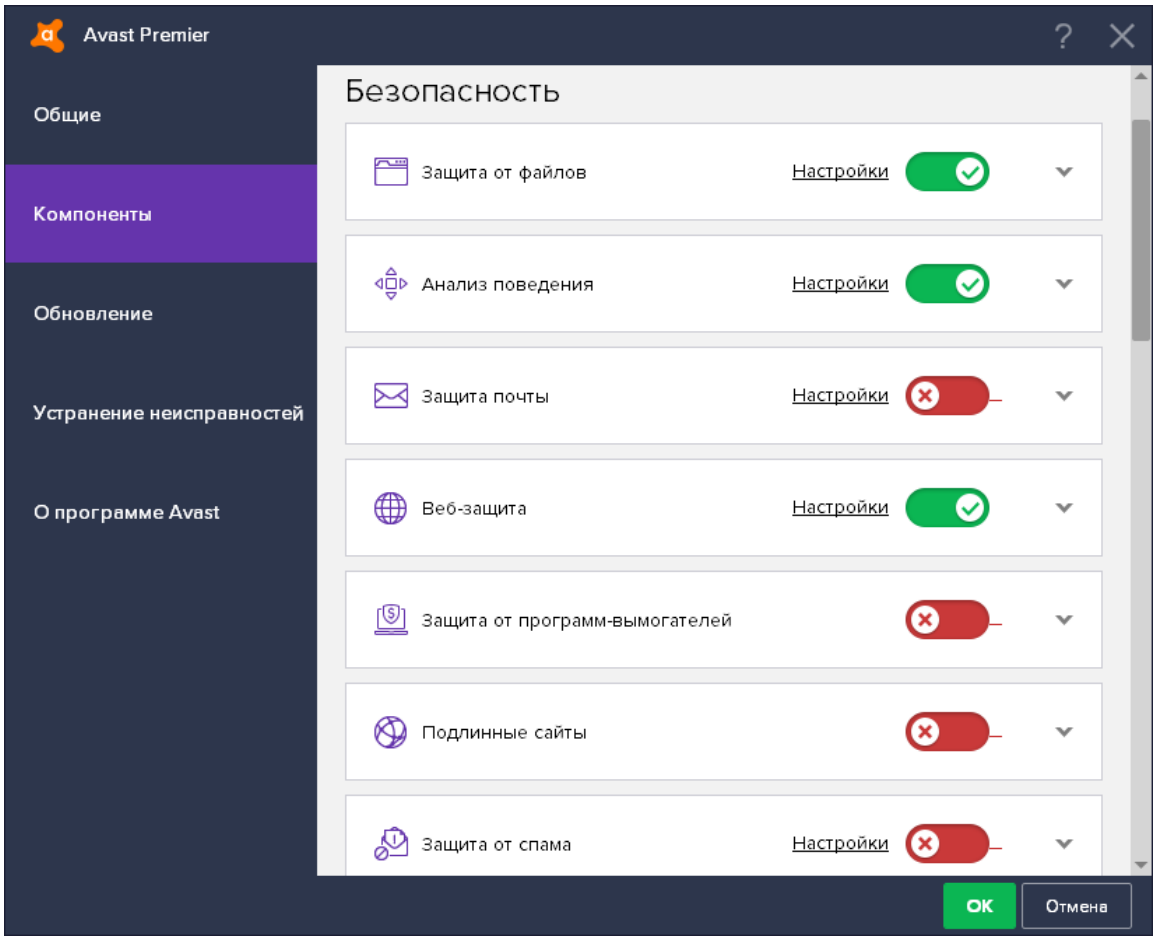


Рисунок 130. Отключение почтовой защиты в Avast

Если перечисленные способы не помогли восстановить работу почты, воспользуйтесь рекомендациями на сайте Microsoft.

Невозможно обратиться к узлам домена по доменному имени

Если в сети ViPNet вашей организации используется служба Active Directory и при этом контроллеры домена с DNS-серверами, которые в рамках домена синхронизируются между собой, находятся на разных узлах ViPNet или туннелируются разными координаторами, то могут возникнуть проблемы разрешения IP-адресов при обращении к ним с других защищённых узлов. В этом случае выполните указания раздела Использование DNS-серверов на контроллерах домена.

Невозможно получить удалённый доступ к защищённым узлам по доменному имени

При совместной установке на компьютер ПО ViPNet Client и ESET NOD32 Smart Security возможны проблемы с установлением соединения между защищёнными узлами и доступом к ресурсам интернета. Чтобы обеспечить на компьютере совместное функционирование программ ViPNet Client и ESET NOD32 Smart Security, в программе ESET NOD32 Smart Security создайте правила, разрешающие обмен данными по протоколу 241 (см. Протоколы соединений в защищённой сети) и использование компонента `Itcsnatproxy.exe`.

Выполните следующие действия:

1. Откройте главное окно программы ESET NOD32 Smart Security и выберите вкладку **Настройка**.
2. В правой части окна щёлкните ссылку **Сеть** и в открывшемся окне щёлкните ссылку **Настроить правила и зоны**.
3. В окне **Настройка зон и правил** нажмите **Создать**.
4. В окне **Новое правило** выберите вкладку **Общие** и в группе **Общая информация об этом правиле** укажите название разрешающего правила для протокола 241.

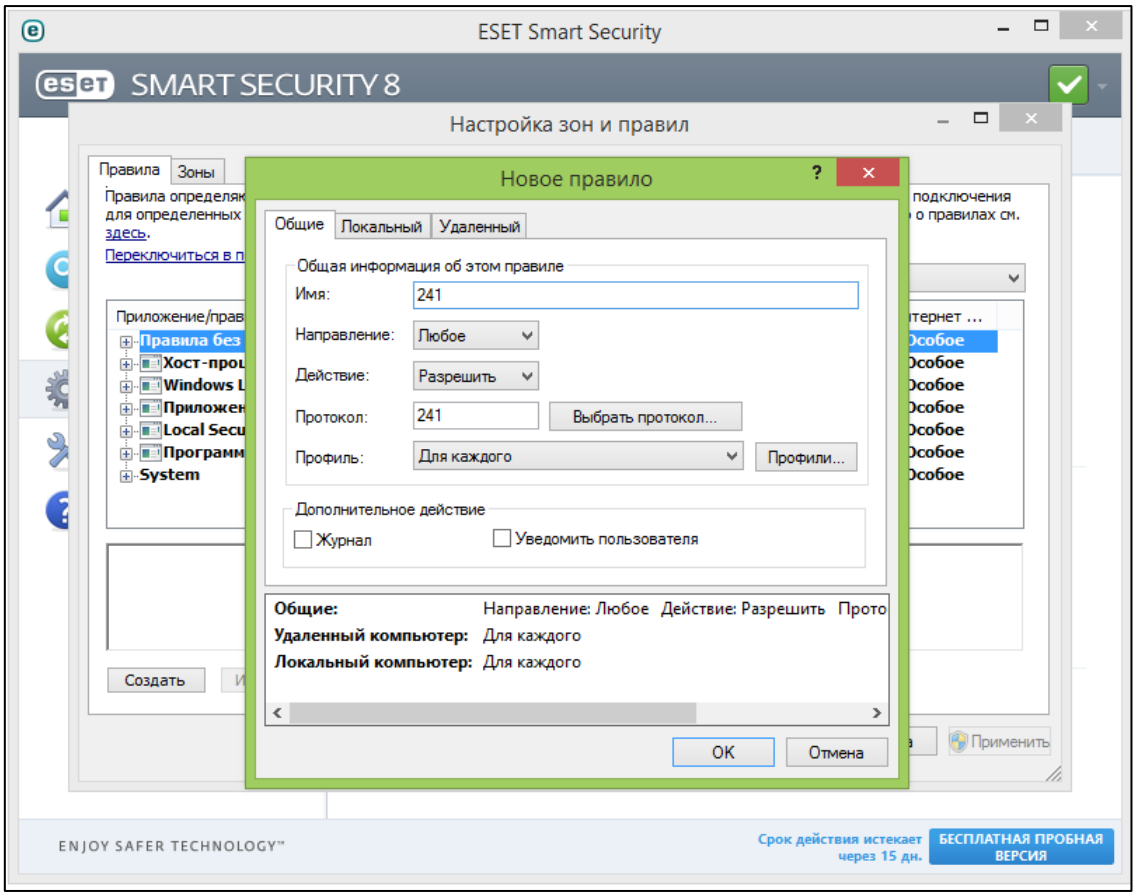


Рисунок 131. Создание правила в ESET NOD32 Smart Security для протокола 241

5. Нажмите **Выбрать протокол** и выберите протокол 241.

6 Нажмите **OK**, чтобы сохранить правило.

7 В окне **Настройка зон и правил** нажмите **Создать**, чтобы создать правило для компоненты `Itcsnatproxy.exe`.

8 В окне **Новое правило** на вкладке **Общие** в группе **Общая информация об этом правиле** укажите название разрешающего правила.

9 Перейдите на вкладку **Локальный** и в группе **Приложение** укажите путь к файлу `Itcsnatproxy.exe`. Например,

`C:\Program Files (x86)\InfoTeCS\ViPNet Client\Itcsnatproxy.exe`

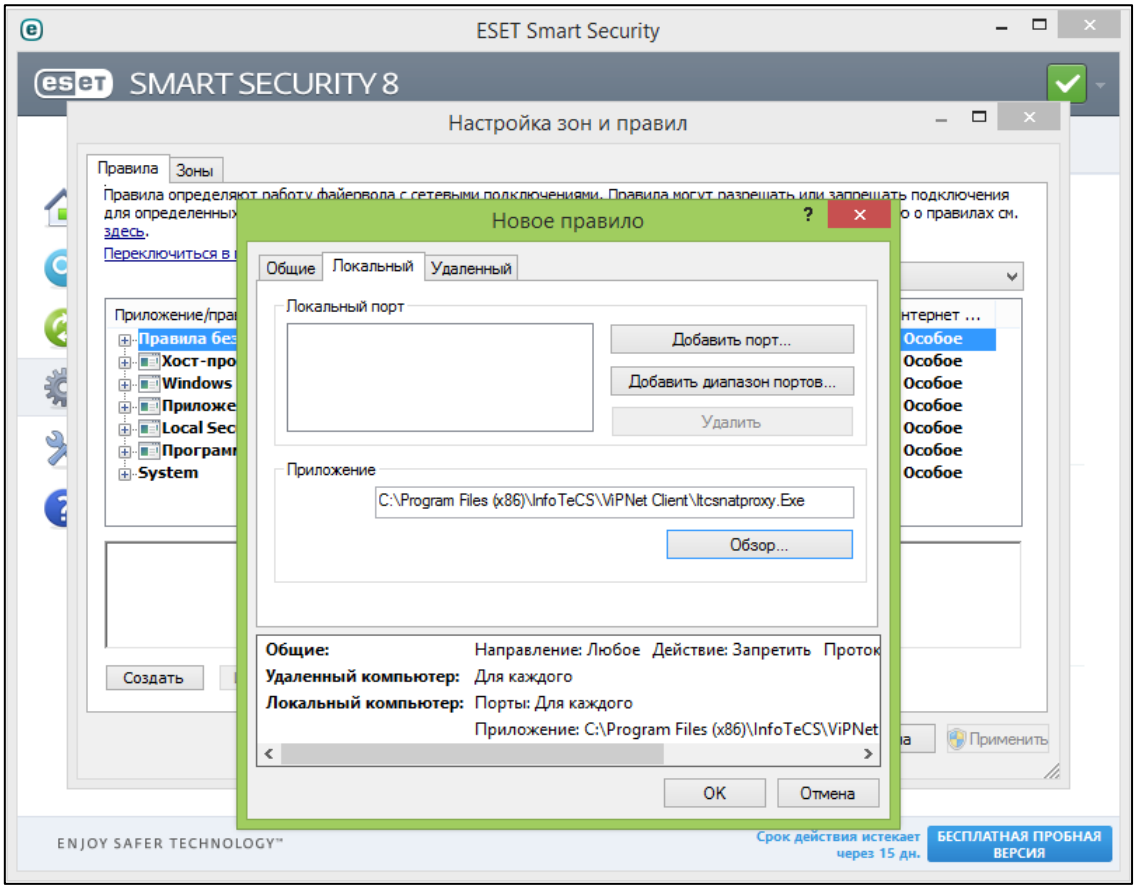


Рисунок 132. Создание правила в ESET NOD32 Smart Security для компоненты Itcsnatproxy.exe

10 Нажмите **OK**, чтобы сохранить правило.

11 В окне **Настройка зон и правил** нажмите **Применить**. Соединение между защищёнными узлами и доступ к ресурсам интернет будут восстановлены.

Невозможно установить соединение с открытым узлом в локальной сети

Возможные причины:

- IP-адрес открытого узла присутствует в списке защищённых узлов. В этом случае ViPNet-драйвер пытается послать зашифрованный пакет на открытый компьютер, установить соединение не удаётся. Для устранения данной проблемы необходимо удалить адрес открытого узла из списка адресов защищённых узлов.
- Неправильно настроены фильтры для работы с открытой сетью. Для нормальной работы в сетях Microsoft убедитесь, что включены и настроены нужные фильтры открытой сети (см. Общие сведения о сетевых фильтрах).

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.

Невозможно установить соединение по протоколу PPPoE

Соединение по протоколу PPPoE может быть заблокировано программой ViPNet Client. Для решения данной проблемы выполните следующие действия:

1. В окне программы ViPNet Client в меню **Сервис** выберите **Настройка приложения**.
2. В окне **Настройка** откройте раздел **Управление трафиком**.
3. Снимите флажок **Блокировать все протоколы, кроме IPv4, ARP**.
4. Нажмите **OK**.

После копирования файла по сети пропадает соединение с сетью

Если после копирования файла из сетевого расположения пропадает соединение с сетью, это может быть связано с настройкой сетевого адаптера Intel(R) Ethernet Connection. Для устранения проблемы:

1 Войдите в Windows под учётной записью администратора.

2 Щёлкните значок **Сеть** в левом нижнем углу панели задач Windows и щёлкните ссылку **Параметры сети и Интернет (Центр управления сетями и общим доступом)**.

3 В окне управления сетями щёлкните ссылку **Настройка (Изменение) параметров адаптера**.

4 В окне **Сетевые подключения** щёлкните правой кнопкой мыши значок сетевого адаптера Intel и в контекстном меню выберите **Свойства**.

Затем в окне свойств сетевого адаптера снимите флажок **Intel(R) Technology Access Filter Driver**.

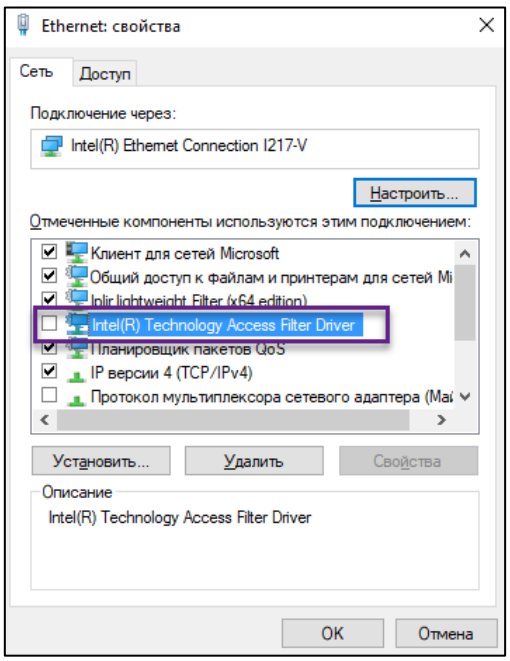


Рисунок 133. Настройка адаптера Intel для работы в сети ViPNet

5 Если вы используете другой сетевой адаптер, то в контекстном меню выберите **Отключить**, затем **Включить**. Дождитесь, когда соединение с сетью восстановится.

В сети зарегистрирован узел с таким же идентификатором, как у вашего узла

В этом случае:

- В журнале событий регистрируется событие с номером 95 (см. Блокированные IP-пакеты).
- Полностью блокируется весь IP-трафик.
- В программе ViPNet Client появляется следующее сообщение:

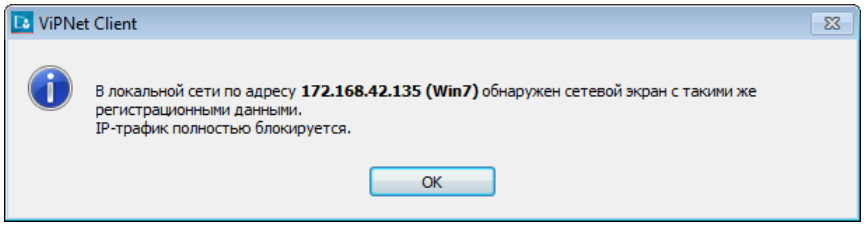


Рисунок 134. Сообщение о том, что в сети обнаружен узел с таким же идентификатором

Для устранения данной проблемы требуется удалить дубликат вашего узла из сети ViPNet (удалить на нем текущие ключи или установить новые ключи). После этого требуется перезагрузить ваш компьютер.

Обнаружен конфликт IP-адресов или доменных имён

При добавлении IP-адреса или DNS-имени в процессе настройки доступа к защищённому или туннелируемому узлу может оказаться, что он совпадает с IP-адресом или DNS-именем, заданным ранее для другого узла. Тогда появится следующее сообщение:

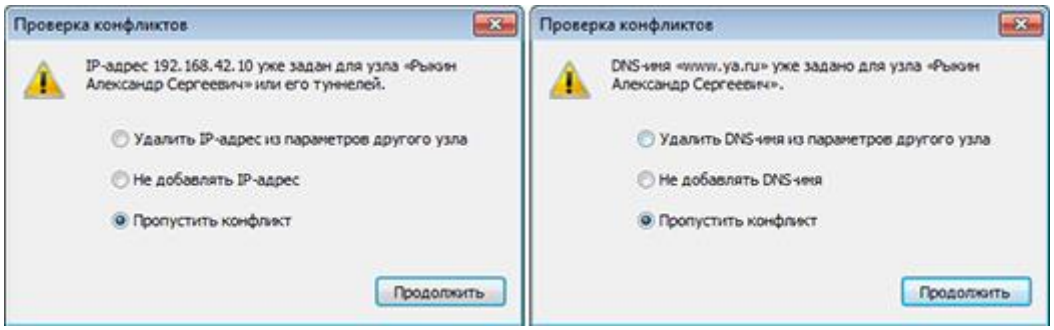


Рисунок 135. Действия при обнаружении пересечения IP-адресов или DNS-имён

Конфликт IP-адресов и DNS-имён также может быть обнаружен в ходе их проверки с помощью кнопки **Проверить конфликты**  . В этом случае появится такое сообщение:

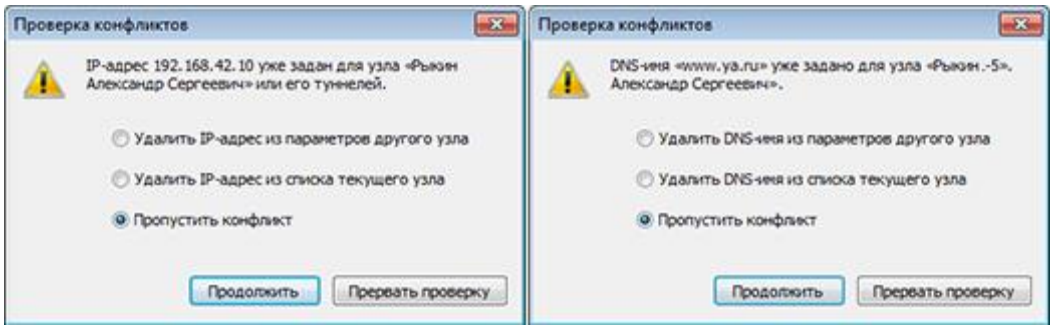


Рисунок 136. Действия при обнаружении пересечения IP-адресов или DNS-имён

Для устранения конфликта IP-адресов или DNS-имён вы можете:

- удалить повторяющийся IP-адрес или DNS-имя из параметров другого узла;
- не добавлять IP-адрес или DNS-имя в первом случае, удалить IP-адрес или DNS-имя из списка текущего узла — во втором.

Кроме этого, вы можете не учитывать возникший конфликт (в первом случае будет добавлен указанный IP-адрес или DNS-имя), а также во втором случае прервать проверку.

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 изменить настройки в ViPNet Client

Изменение настроек программы ViPNet Client может быть невозможно по одной из следующих причин:

- На сетевом узле ограничены полномочия пользователя. Изменить настройки программы ViPNet Client может только пользователь с максимальным уровнем полномочий. Обратитесь к администратору сети ViPNet с просьбой повысить уровень полномочий в программе ViPNet Центр управления сетью.
- Установлены ограничения интерфейса в режиме администратора (см. Работа в программе в режиме администратора). Обратитесь к администратору сети ViPNet с просьбой снять ограничение.

Не удаётся 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:
   - `accord` — Аккорд-АМДЗ.
   - `sobol` — электронный замок «Соболь».
   - `bio` — электронная рулетка (используется в программном обеспечении ViPNet по умолчанию).
   - `tokenJava` — eToken PRO (Java).
   - `ruToken` — Rutoken ЭЦП.
4. Сохраните созданный файл, затем измените его имя и расширение на `csp_config.ini`.

   При следующем вызове датчика случайных чисел будет использоваться указанный датчик.

SIP-клиент Zoiper сбрасывает входящие звонки

Если на компьютере с ПО ViPNet также установлена программа Zoiper, в настройках которой задано использование протокола TCP, то входящие звонки сбрасываются через 30 секунд после принятия вызова.

Для устранения этой проблемы в настройках программы Zoiper включите использование протокола UDP вместо протокола TCP:

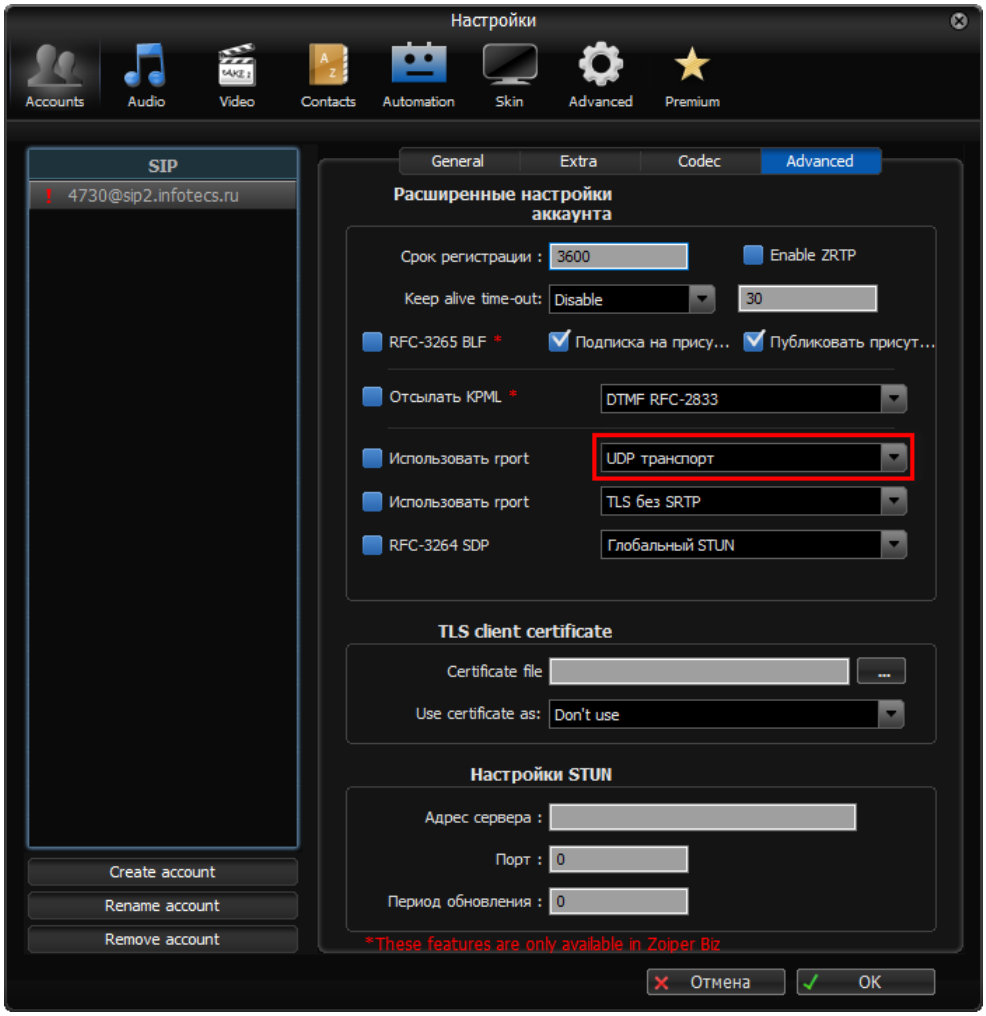


Рисунок 137. Настройка транспорта UDP в программе Zoiper

Не удаётся зарегистрировать в сети клиент Cisco

Если в рамках защищённой сети ViPNet развёрнута сеть IP-телефонии Cisco, включая клиенты (как аппаратные, так и программные) и серверы (Cisco CallManager - CCM, Cisco Unified Communications Manager - CUCM), то для серверов Cisco необходимо настроить видимость в сети по их реальным

IP-адресам (см. Настройка доступа к туннелируемым узлам). Видимость по реальным IP-адресам необходимо включить как на защищённых сетевых узлах с установленным ПО ViPNet Client, так и на координаторах (для туннелируемых сетевых узлов). Если же для CCM (CUCM) вы настроите видимость по виртуальным адресам (например, в случае конфликта адресов), то соединение между клиентами и серверами Cisco не будет установлено.

ViPNet Client невозможно установить на сервер HP с включённым NIC Teaming

Если вы устанавливаете программу ViPNet Client на сервер HP с включённым режимом объединения сетевых интерфейсов (NIC Teaming), то в процессе установки могут возникнуть неполадки. Это происходит в том случае, если сервер работает под управлением ОС Windows Server 2008 R2, и режим NIC Teaming настроен с помощью утилиты HP Network Configuration Utility. Так как Windows Server 2008 R2 не поддерживает режим NIC Teaming, то для решения проблемы обновите ОС до Windows Server 2016 и выше и настройте режим NIC Teaming средствами системы.

Не найден ключ для подписи запроса

При обновлении сертификата появляется следующее сообщение:

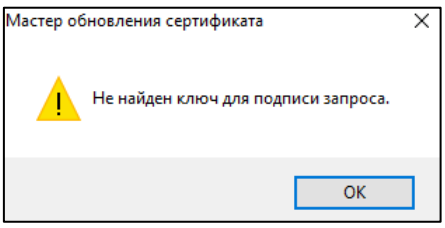


Рисунок 138. Ошибка обновления сертификата

Данная ошибка может возникать после смены мастер-ключей в вашей сети ViPNet. Для решения проблемы выберите в качестве текущего сертификат (см. Смена текущего сертификата), выпущенный вместе с новыми ключами. Как правило, это сертификат с самой поздней датой выпуска. Если подходящего сертификата нет, обратитесь к администратору вашей сети ViPNet.

Не найден резервный набор персональных ключей (РНПК)

При первом запуске программы ViPNet появляется сообщение о необходимости указать расположение резервного набора персональных ключей или о том, что РНПК не найден. Данная ошибка может возникать после смены мастер-ключей в вашей сети ViPNet. Для решения проблемы выполните следующие действия:

1. Получите файл РНПК у администратора вашей сети или подключите внешнее устройство, на котором находится РНПК (файл `AAAA.pk`, где `AAAA` — идентификатор пользователя).
2. Укажите путь к файлу РНПК или поместите его в папку `d_station\abn_AAAA`, расположенную в папке ключей пользователя, по умолчанию:

   `C:\ProgramData\Infotecs\ID_Узла\d_station\abn_AAAA`.

После этого запустите ViPNet Client и выполните вход в программу.

ViPNet Client не позволяет войти в Windows

Если из-за сбоя в программе ViPNet Client невозможно войти в Windows и другие способы восстановления входа не применимы, удалите программу ViPNet Client в безопасном режиме. Для этого:

1. Загрузите компьютер в безопасном режиме.
2. Войдите в систему, используя учётную запись администратора Windows.
3. Запустите файл `SafeModeUninstall.bat` из папки установки программы ViPNet Client.

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.

4. Дождитесь запуска службы «Windows Installer» («Установщик Windows»).
5. Удалите программу ViPNet Client (см. Удаление ПО ViPNet Client).
6. Перезагрузите компьютер в обычном режиме.
7. Убедитесь, что ваш компьютер соответствует системным требованиям.
8. Установите программу ViPNet Client или обратитесь службу поддержки ИнфоТеКС (см. Сбор диагностической информации при возникновении неполадок).

Блокируется соединение с координатором своей сети ViPNet

Проверьте, что для IP-адреса сетевого интерфейса, на котором указан шлюз по умолчанию, задано `SkipAsSource=False`. Иначе ViPNet Client будет блокировать соединение с координатором своей сети ViPNet и в журнале IP-пакетов зарегистрируется событие 115 (см. Блокированные IP-пакеты).

Если в ViPNet Client нужно использовать несколько IP-адресов, то для соединения с координатором:

1. Назначьте все IP-адреса на один сетевой интерфейс.

2 Для IP-адреса, с которого планируется подключение к координатору, задайте `SkipAsSource=False`.

Срок действия лицензии заканчивается или закончился

При появлении такого сообщения обратитесь к администратору вашей сети ViPNet для обновления лицензии. Подробнее см. раздел Лицензирование программы ViPNet Client.

ViPNet Client постоянно требует перезагрузки

Если после перезагрузки компьютера снова появляется сообщение о перезагрузке, подождите 5-10 минут, пока загрузятся все компоненты ПО ViPNet Client. После этого выполните перезагрузку компьютера.

Обнаружена исключительная ситуация в модуле Monitor

Если вы не используете внешние устройства, то после появления ошибки повторно выполните вход в программу ViPNet Client и передайте администратору сети файл `C:\ProgramData\InfoTeCS\Monitor.err`.

Восстановление программы при изменении её конфигурации

При автоматической установке обновлений ОС Windows в некоторых случаях возможно нарушение конфигурации программы ViPNet CSP из состава ViPNet Client. Для решения этой проблемы запустите восстановление программы через меню **Пуск** > **ViPNet** > **Настройка компонентов ViPNet Client**, затем выберите **Восстановить**.

Информация для администратора сети ViPNet

Если политика безопасности вашей организации не позволяет запустить функцию восстановления программы на компьютере пользователя, вы можете восстановить программу удалённо одним из способов:

- Отправка обновления из программы ViPNet Центр управления сетью в виде файла `*.lzh`.

- Отправка и запуск исполняемого файла `*.bat` на компьютере пользователя через групповые политики или вручную.

В зависимости от выбранного способа восстановления запросите в службе поддержки ИнфоТеКС нужный файл и восстановите конфигурацию программы на всех компьютерах с ограниченной политикой безопасности.

На терминальный сервер не приходят обновления

Информация для администратора сети ViPNet

Если на терминальном сервере с ViPNet Client одновременно работают более десяти пользователей, то для правильной отправки обновлений из ЦУСа выберите одно из действий:

- перед оправкой обновлений отключите сессии пользователей, чтобы их осталось не более десяти;
- выполняйте обновление локально, с помощью файла дистрибутива ключей и справочников. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора», раздел «Создание дистрибутивов ключей».
- перенесите терминальный сервер в туннель ViPNet Coordinator и удалите ViPNet Client. Подробнее о создании туннелей см. документацию для того координатора, который используется в вашей сети.

Не появляется окно входа в программу при работе на Hyper-V

Если вы работаете на сервере виртуализации Hyper-V, то после перезагрузки может не появиться окно входа в программу ViPNet Client. Чтобы решить проблему, отключите настройку Allow enhanced session mode:

1. Запустите консоль управления Hyper-V Manager.
2. Откройте настройки сервера **Hyper-V Settings**.
3. Перейдите в раздел **Enhanced Session Mode Policy**.
4. Снимите флажок **Allow enhanced session mode**.

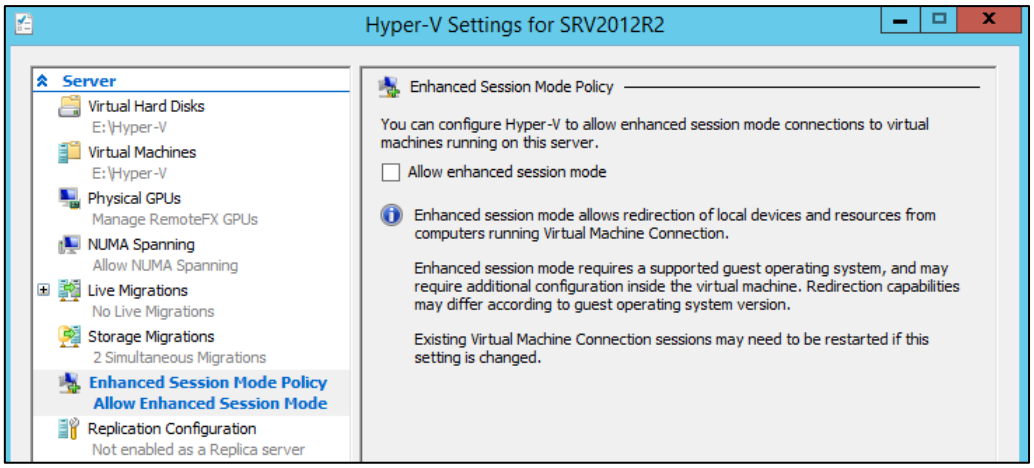


Рисунок 139. Отключение Allow enhanced session mode

Предупреждения сервиса безопасности

Предупреждения сервиса безопасности предназначены для своевременного информирования пользователя о таких событиях, как истечение сроков действия пароля, текущего сертификата, ключа электронной подписи и списка аннулированных сертификатов, а также ввод в действие сертификата, изданного по инициативе администратора программы ViPNet Удостоверяющий и ключевой центр.

Проверка статуса пароля, текущего сертификата и ключа электронной подписи выполняется каждые 5 минут.

Срок действия пароля истёк

Окно с сообщением об истечении срока действия пароля пользователя появляется в следующих случаях:

- Если в окне **Настройка параметров безопасности** на вкладке **Пароль** установлен флажок **Ограничить срок действия пароля** и задан срок действия пароля.

  Появление окна свидетельствует о том, что указанный срок подошёл 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).

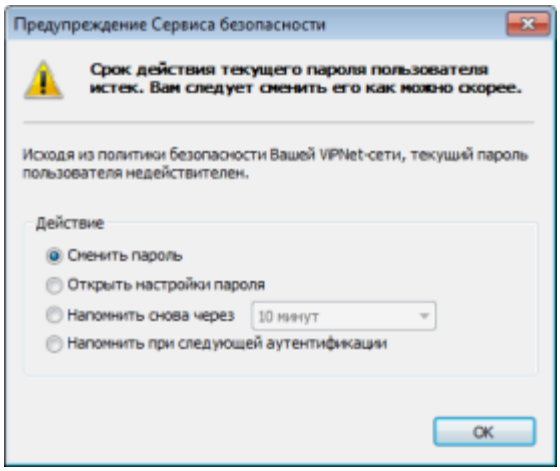


Рисунок 140. Предупреждение об истечении срока действия пароля пользователя

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**;
- **Открыть настройки пароля** — для вызова окна **Настройка параметров безопасности** на вкладке **Пароль**, с помощью которой можно сначала 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 **OK**.

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 введён в действие новый сертификат, подписание электронных документов невозможно.

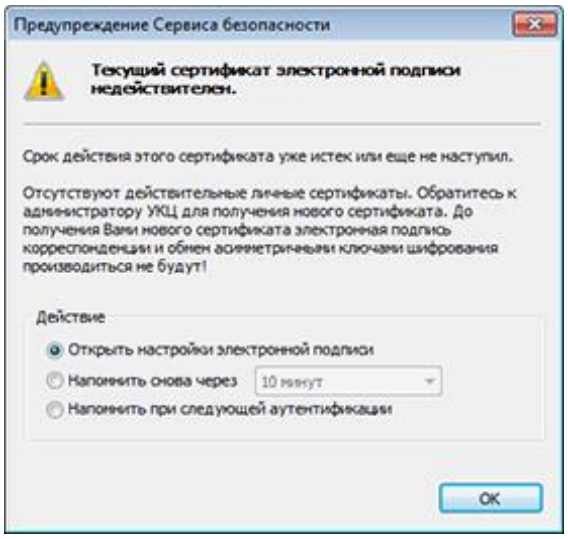


Рисунок 141. Предупреждение о том, что текущий сертификат недействителен

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 **Назначение сертификата текущим**.

Примечание. Данное положение переключателя отображается в окне предупреждения в случае, если в хранилище пользователя найдены другие действительные личные сертификаты.

- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная 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 **OK**.

Срок действия текущего ключа электронной подписи или соответствующего сертификата близок к концу

Предупреждение о скором истечении срока действия ключа электронной подписи или соответствующего ему сертификата появляется в следующих случаях:

- Если срок действия ключа электронной подписи или сертификата близок к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворён, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае Вы можете сформировать запрос на обновление сертификата (см. Процедура обновления ключа электронной подписи и сертификата). Для этого:

  - если истекает срок действия сертификата, выберите **Отправить запрос на обновление сертификата**;
  - если истекает срок действия ключа электронной подписи, выберите **Открыть настройки подписи**, затем в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** нажмите **Обновить сертификат**.

- Если срок действия ключа электронной подписи или сертификата близок к концу, при этом последний запрос на обновление текущего сертификата либо отклонён, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте ещё один запрос на обновление текущего сертификата.

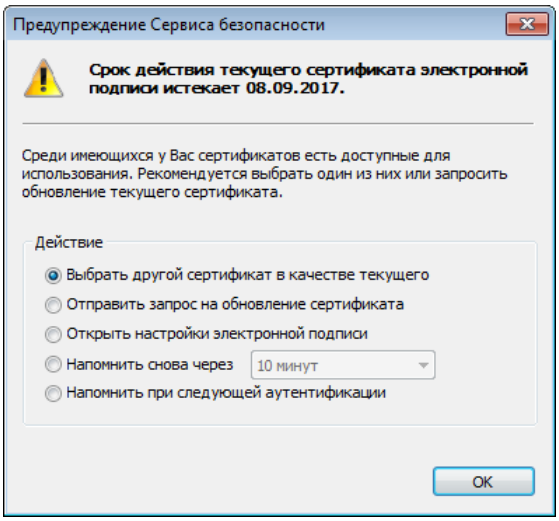


Рисунок 142. Предупреждения о скором истечении срока действия сертификата и ключа электронной подписи

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 Н**азначение сертификата текущим**.
- **Отправить запрос на обновление сертификата** — для формирования запроса на обновление текущего сертификата с помощью мастера обновления сертификатов (см. Процедура обновления ключа электронной подписи и сертификата).
- **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная 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 **OK**.

Срок действия текущего ключа электронной подписи уже истёк

Предупреждение об истечении срока действия ключа электронной подписи появляется в следующих случаях:

- Если срок действия ключа электронной подписи подошёл к концу, при этом не найдено запросов на обновление текущего сертификата (или последний запрос на обновление удовлетворён, однако соответствующий сертификат не может быть назначен текущим).

  В этом случае вы можете открыть вкладку **Электронная подпись** окна **Настройка параметров безопасности**, выбрав **Открыть настройки подписи**. С помощью соответствующей кнопки на вкладке **Электронная подпись** вы можете обновить текущий сертификат (см. Процедура обновления ключа электронной подписи и сертификата). 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 ключа электронной подписи, 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).

- Если срок действия ключа электронной подписи подошёл к концу, при этом последний запрос на обновление текущего сертификата либо отклонён, либо находится в состоянии обработки в программе ViPNet Удостоверяющий и ключевой центр.

  В этом случае обратитесь к администратору вашей сети ViPNet и, при необходимости, создайте ещё один запрос на обновление текущего сертификата.

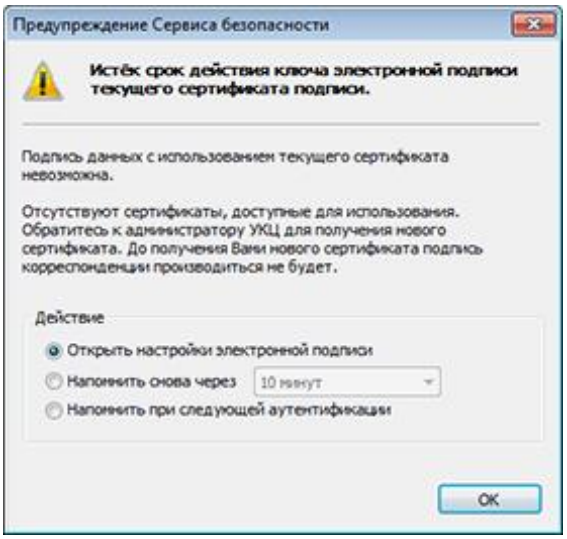


Рисунок 143. Предупреждение о том, что истёк срок действия ключа электронной подписи

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

   - **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная 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 **OK**.

Действительный список аннулированных сертификатов не найден

Предупреждение о том, что действительный список аннулированных сертификатов не найден, появляется при выполнении следующих условий:

- если список аннулированных сертификатов не обнаружен в хранилище пользователя или срок его действия истёк;
- если в окне **Настройка параметров безопасности** на вкладке **Администратор** снят флажок **Игнорировать отсутствие списков аннулированных сертификатов** (см. Дополнительные настройки параметров безопасности).

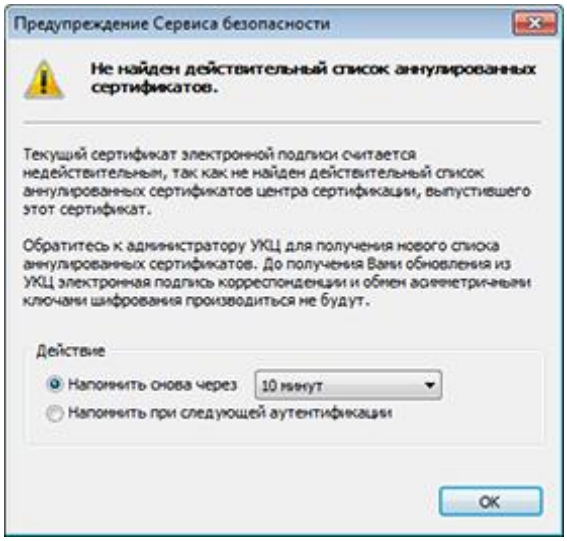


Рисунок 144. Предупреждение о том, что действительный список аннулированных сертификатов не найден

При появлении окна с таким предупреждением:

- Обратитесь к администратору вашей сети ViPNet для получения нового списка аннулированных 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 **OK**.

Сертификат, изданный по инициативе администратора, введён в действие

Предупреждение о том, что введён 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 **Электронная подпись** 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 ключ электронной подписи.

При появлении окна с таким предупреждением:

1 Выберите одно из предложенных действий:

   - **Открыть настройки электронной подписи** — для вызова окна **Настройка параметров безопасности** на вкладке **Электронная подпись**, 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 ключа электронной подписи и сертификата).

     Отправлять запрос на обновление сертификата следует в том случае, если политика безопасности вашей организации запрещает использовать ключ электронной подписи, сформированный не вами лично, а на сетевом узле администратора. В результате обновления вам будет доставлен сертификат, который будет соответствовать ключу электронной подписи, сформированному на вашем компьютере.

2 Нажмите **ОК**.

Истекает срок действия текущего сертификата аутентификации

Если пользователь выбрал способ аутентификации в ПО ViPNet Client при помощи сертификата на устройстве, за 45 дней до истечения срока действия этого сертификата появится соответствующее предупреждение сервиса безопасности. Вид предупреждения зависит от того, хранятся ли на внешнем устройстве другие сертификаты, подходящие для аутентификации.

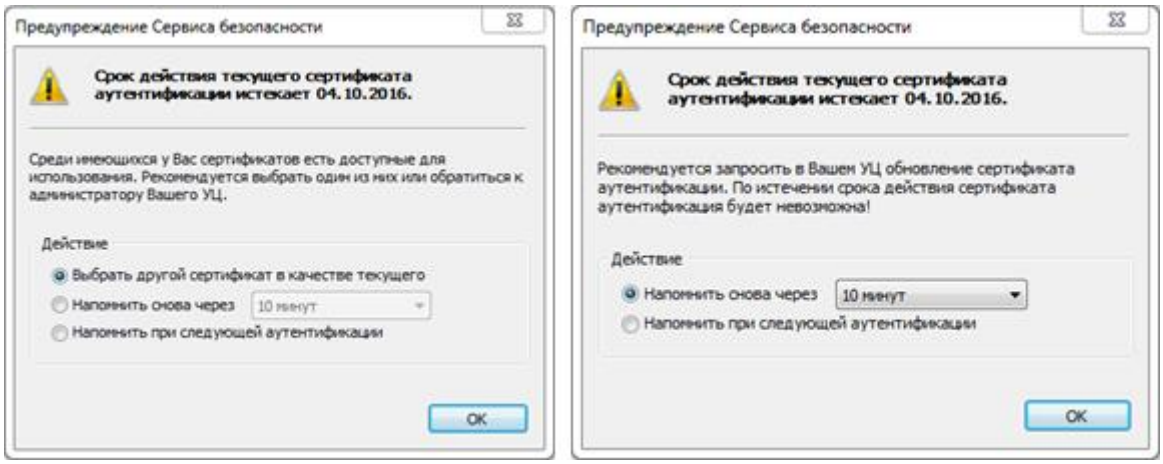


Рисунок 145. Предупреждения о скором истечении срока действия сертификата, используемого при аутентификации

Выполните следующие действия:

- Если на внешнем устройстве найдены другие сертификаты, подходящие для аутентификации, и соответствующие им списки аннулированных сертификатов установлены в хранилище и являются действительными, выберите одно из предложенных действий:
  - **Выбрать другой сертификат в качестве текущего** — для назначения другого сертификата для аутентификации с помощью окна Выбор сертификата.
  - **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 ПО ViPNet Client.
- Если на внешнем устройстве нет других подходящих для аутентификации сертификатов, выберите одно из двух действий, чтобы настроить напоминание, и затем получите новый сертификат для аутентификации (см. Особенности аутентификации с помощью сертификата).

Если на внешнем устройстве есть другие подходящие для аутентификации сертификаты, но соответствующие им CRL просрочены либо не установлены, выберите одно из двух действий, чтобы настроить напоминание, и затем обратитесь к администратору вашей сети ViPNet для получения соответствующего списка аннулированных сертификатов. После обновления CRL или

установки его в хранилище при следующей проверке появится окно предупреждения о скором истечении срока действия сертификата, в котором вы сможете выбрать действие **Выбрать другой сертификат в качестве текущего**.

Внимание! Если вы используете программу ViPNet Деловая почта, необходимо заменить сертификат, используемый для аутентификации, до истечения его срока действия, чтобы не выполнять повторную установку ключей. В противном случае после повторной установки ключей будет потерян доступ к зашифрованным письмам программы ViPNet Деловая почта (в том числе в архивах).

Текущий сертификат аутентификации недействителен

Если срок действия сертификата, используемого при аутентификации, истёк, появится соответствующее предупреждение сервиса безопасности.

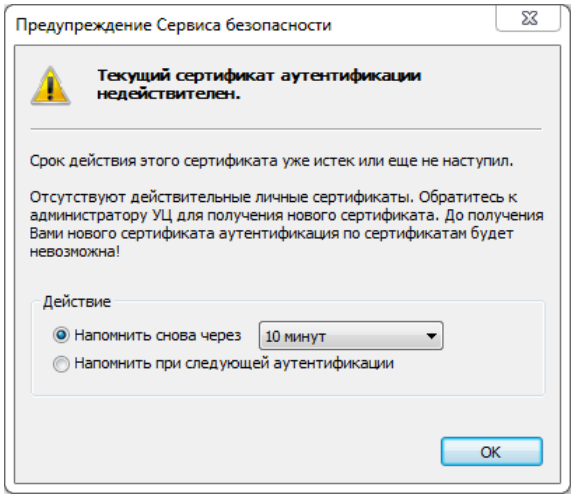


Рисунок 146. Предупреждение об истечении срока действия сертификата, используемого при аутентификации

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий, чтобы настроить напоминание.
2. Получите новый сертификат для аутентификации (см. Особенности аутентификации с помощью сертификата).

Кроме того, предупреждение о недействительном сертификате аутентификации появляется в случае, когда сертификат издателя не установлен в системное хранилище **Доверенные корневые сертификаты**.

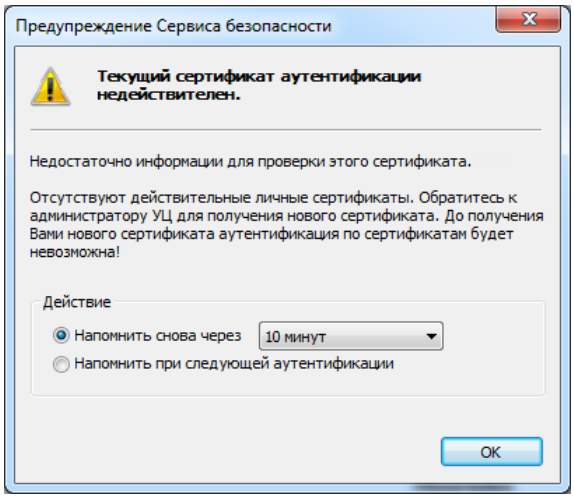


Рисунок 147. Предупреждение о недействительном сертификате, используемом при аутентификации

При появлении окна с таким предупреждением:

1. Выберите одно из предложенных действий, чтобы настроить напоминание.
2. Обратитесь к администратору вашей сети ViPNet, чтобы получить сертификат издателя и затем установите его в системное хранилище **Доверенные корневые сертификаты**. Для этого дважды щёлкните по сертификату и следуйте указаниям мастера установки сертификатов (см. Установка в хранилище вручную).

Текущий сертификат аутентификации не найден

Если устройство, используемое для аутентификации с помощью сертификата, не подключено, появится соответствующее предупреждение.

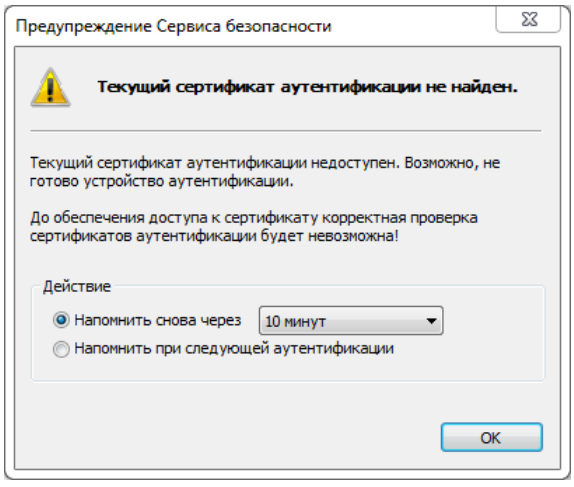


Рисунок 148. Предупреждение о ненайденном сертификате, используемом при аутентификации

1. Выберите одно из предложенных действий, чтобы настроить напоминание.
2. Подключите внешнее устройство с сертификатом, который используется для аутентификации.

Предупреждения об угрозах

Предупреждения об угрозах предназначены для своевременного информирования пользователя о снижении уровня безопасности сетевого узла.

Нарушена целостность файла

Для обеспечения безопасности сетевого узла каждый раз при запуске программы ViPNet Client выполняется проверка целостности всех модулей и компонентов ПО. При обнаружении неполадок, появится сообщение о нарушении целостности файла. Программа ViPNet Client будет переведена в аварийный режим работы, при котором:

- заблокирован доступ к ресурсам защищённой сети;
- разрешён доступ к открытой сети в соответствии с настроенными сетевыми фильтрами.

Восстановление работы ПО ViPNet Client выполняется в ручном режиме. Для этого воспользуйтесь одним из способов:

- выполните восстановление программы (см. Добавление, удаление и восстановление компонентов;
- обратитесь к администратору сети ViPNet за обновлением программы (см. Обновление, отправленное из ViPNet Центр управления сетью);
- проведите обновление самостоятельно (см. Обновление с помощью установочного файла).

Обнаружена попытка нарушения сетевых фильтров

Для безопасной работы в сети необходимы корректно настроенные правила фильтрации трафика. Если по какой-то причине сетевые фильтры будут искажены, появится соответствующее сообщение. При этом фильтры заменяются на предустановленные. Чтобы при нарушении целостности фильтров автоматически блокировать трафик, выполните необходимые настройки в режиме администратора (см. Параметры защиты трафика).

B

Общие сведения о сертификатах и ключах

Основы криптографии

Криптография используется для решения трёх 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 упрощённое описание алгоритмов с симметричным ключом, с асимметричным ключом, электронной подписи, а также приводятся примеры использования этих алгоритмов в информационных системах (приведённые 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 изображён процесс симметричного зашифрования и расшифрования.

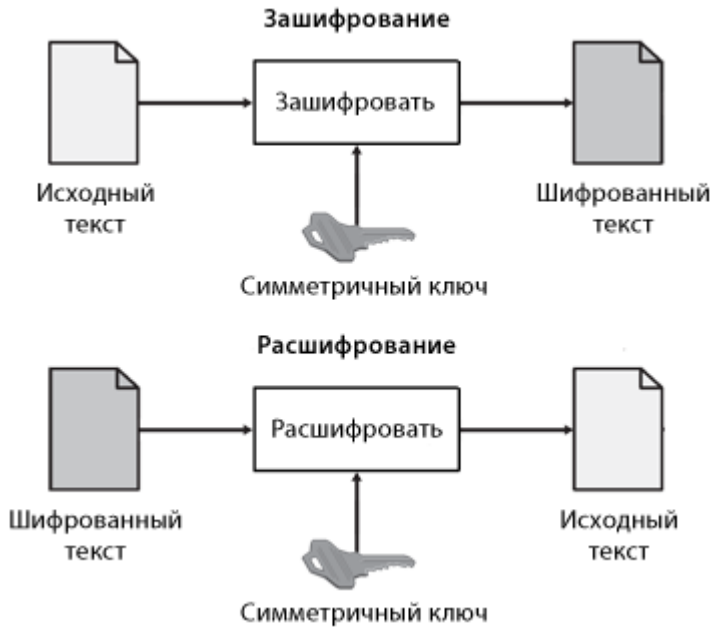


Рисунок 149. Зашифрование и расшифрование на симметричном ключе

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 надёжным способом. Обычно создаётся симметричный ключ парной связи, который передаётся получателю лично. Затем для шифрования используются случайные (сессионные) симметричные ключи, которые зашифровываются на ключе парной связи и в таком виде передаются 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 создаёт 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.

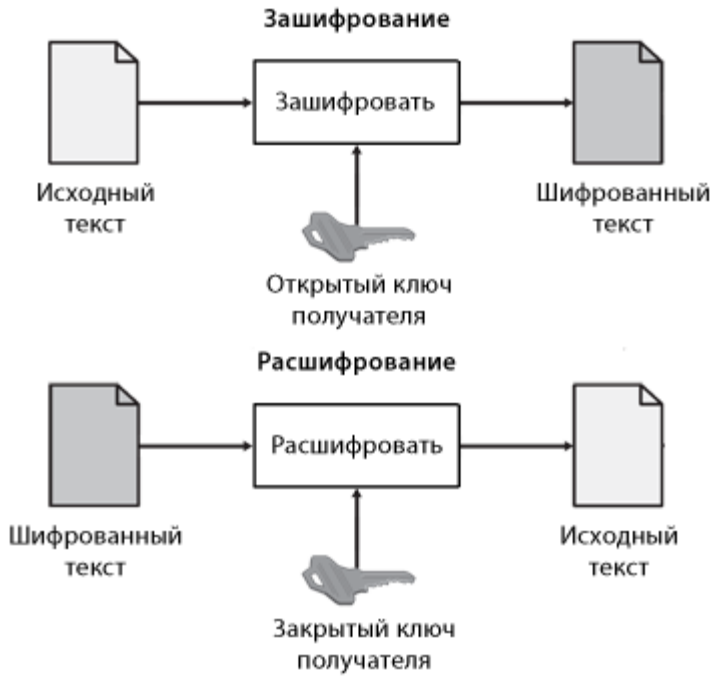


Рисунок 150. Зашифрование и расшифрование на асимметричном ключе

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).

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 изображён процесс шифрования с помощью комбинированного алгоритма.

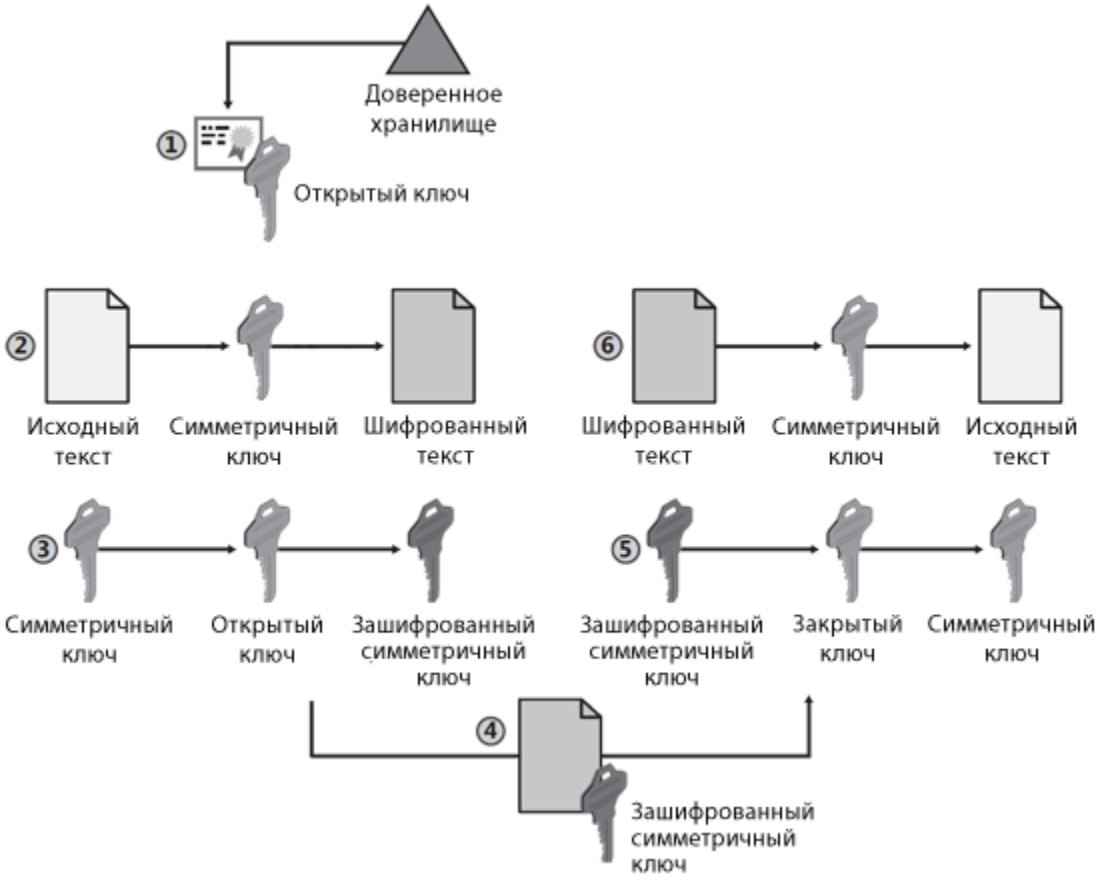


Рисунок 151. Шифрование с помощью комбинированного алгоритма

1 Отправитель запрашивает открытый ключ получателя из доверенного хранилища.

2 Отправитель создаёт 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 ключом электронной подписи, 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.

Приведённая ниже схема иллюстрирует применение хэш-функции и асимметричного алгоритма в электронной подписи.

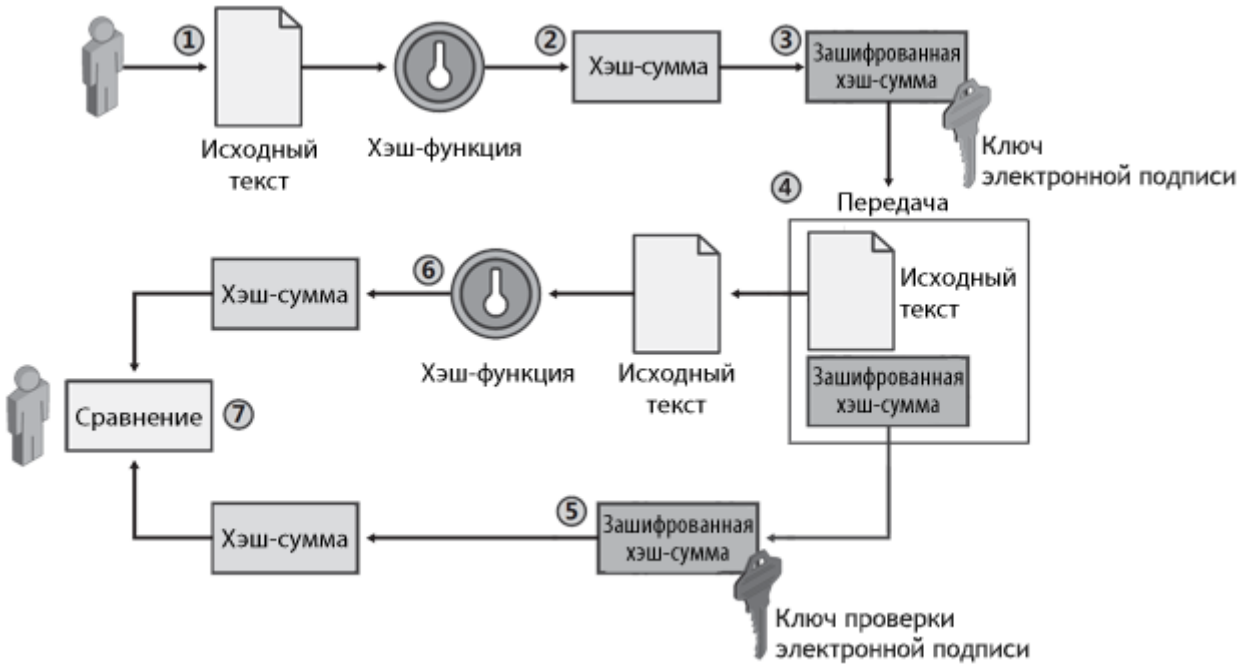


Рисунок 152. Применение хэш-функции и асимметричного криптографического алгоритма в электронной подписи

1 Отправитель создаёт файл с исходным сообщением.

2 Программное обеспечение отправителя вычисляет хэш-сумму исходного сообщения.

3 Полученная хэш-сумма зашифровывается с помощью ключа электронной подписи 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 ключа проверки электронной подписи отправителя. Ключ проверки электронной подписи может быть передан вместе с сообщением или получен из доверенного хранилища.

6 Получатель использует ту же хэш-функцию, что и отправитель, чтобы вычислить хэш-сумму полученного сообщения.

7 Вычисленная хэш-сумма сравнивается с хэш-суммой, полученной от отправителя. Если эти хэш-суммы различаются между собой, то сообщение или хэш-сумма были изменены при передаче.

Общие сведения о сертификатах ключей проверки электронной подписи

Определение и назначение

Сертификат ключа проверки электронной подписи является одним из объектов криптографии с ключом проверки электронной подписи, в которой для прямого и обратного преобразований используются разные ключи:

- Ключ электронной подписи — для формирования электронной подписи и расшифрования сообщения. Ключ электронной подписи хранится в тайне и не подлежит распространению.
- Ключ проверки электронной подписи — для проверки электронной подписи и зашифрования сообщения. Ключ проверки электронной подписи известен всем участникам информационного обмена и может передаваться по незащищённым каналам связи.

Таким образом, криптография с ключом проверки электронной подписи позволяет выполнять следующие операции:

- Подписание сообщения — формирование электронной подписи, прикрепление её к сообщению и проверка электронной подписи на стороне получателя;
- Шифрование — зашифрование документа с возможностью расшифрования на стороне получателя.

Ключи электронной подписи и проверки электронной подписи являются комплементарными по отношению друг к другу — только владелец ключа электронной подписи может подписать данные, а также расшифровать данные, которые были зашифрованы ключом проверки электронной подписи, соответствующим ключу электронной подписи владельца. Простой аналогией может служить почтовый ящик: любой может кинуть письмо в почтовый ящик («зашифровать»), но только владелец секретного ключа (ключа электронной подписи) может извлечь письма из ящика («расшифровать»).

Поскольку ключ проверки электронной подписи распространяется публично, существует опасность того, что злоумышленник, подменив ключ проверки электронной подписи одного из пользователей, может выступать от его имени. Для обеспечения доверия к ключам проверки электронной подписи создаются удостоверяющие центры (согласно Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года), которые играют роль доверенной третьей стороны и заверяют ключи проверки электронной подписи каждого из пользователей своими электронными подписями — иначе говоря, сертифицируют эти ключи.

Сертификат ключа проверки электронной подписи (далее — сертификат) представляет собой цифровой документ, заверенный электронной подписью удостоверяющего центра и призванный подтверждать принадлежность ключа проверки электронной подписи определённому пользователю.

Примечание. Несмотря на то, что защита сообщений выполняется фактически с помощью ключа проверки электронной подписи, в профессиональной речи используются выражения «подписать сертификатом (с помощью сертификата)», «зашифровать на сертификате (с помощью сертификата)».

Сертификат включает ключ проверки электронной подписи и список дополнительных атрибутов, принадлежащих пользователю (владельцу сертификата). К таким атрибутам относятся: имена владельца и издателя сертификата, номер сертификата, время действия сертификата, предназначение ключа проверки электронной подписи (электронная подпись, шифрование) и так далее. Структура и протоколы использования сертификатов определяются международными стандартами.

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 ключа электронной подписи, соответствующего этому сертификату.
- Корневой сертификат — самоподписанный сертификат издателя, являющийся главным из вышестоящих сертификатов. Корневой сертификат не может быть проверен с помощью другого сертификата, поэтому пользователь должен безусловно доверять источнику, из которого получен данный сертификат.
- Кросс-сертификат — это сертификат администратора удостоверяющего центра, изданный администратором другого удостоверяющего центра. Таким образом, для кросс-сертификата значения полей «Издатель» и «Субъект» различны и определяют разные удостоверяющие центры. С помощью кросс-сертификатов устанавливаются доверительные отношения между различными удостоверяющими центрами. В зависимости от модели доверительных отношений, установленной между удостоверяющими центрами (см. PKI и асимметричная криптография), может использоваться либо как сертификат издателя (в иерархической модели), либо для проверки сертификатов пользователей другой сети (в распределённой модели).

Рисунок 153. 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 аннулирован, то сертификат считается действительным. Документы, подписанные действительным сертификатом и не изменявшиеся с момента их подписания, также считаются действительными.

Таким образом, криптография с ключом проверки электронной подписи и инфраструктура обмена сертификатами ключей проверки электронной подписи (см. PKI и асимметричная криптография) позволяют выполнять шифрование сообщений, а также предоставляют возможность подписывать сообщения с помощью электронной подписи.

Посредством шифрования конфиденциальная информация может быть передана по незащищённым каналам связи. В свою очередь, электронная подпись позволяет обеспечить:

- Подлинность (аутентификация) — возможность однозначно идентифицировать отправителя. Если сравнивать с бумажным документооборотом, то это аналогично собственноручной подписи отправителя.
- Целостность — защиту информации от несанкционированной модификации как при хранении, так и при передаче.
- Неотрекаемость — невозможность для отправителя отказаться от совершенного действия. Если сравнивать с бумажным документооборотом, то это аналогично предъявлению отправителем паспорта перед выполнением действия.

Структура

Чтобы сертификат можно было использовать, он должен обладать доступной универсальной структурой, позволяющей извлечь из него нужную информацию и легко её 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 определён в рекомендациях Международного Союза по телекоммуникациям (International Telecommuncations Union, ITU) X.509 | ISO/IEC 9594–8 и документе RFC 3280 Certificate & CRL Profile Организации инженерной поддержки интернета (Internet Engineering Task Force, IETF). В настоящее время наиболее распространенной версией X.509 является версия 3, позволяющая задать для сертификата расширения, с помощью которых можно разместить в сертификате дополнительную информацию (о политиках безопасности, использовании ключа, совместимости и так далее).

Сертификат содержит элементы данных, сопровождаемые электронной подписью издателя сертификата. В сертификате имеются обязательные и дополнительные поля.

К обязательным полям относятся:

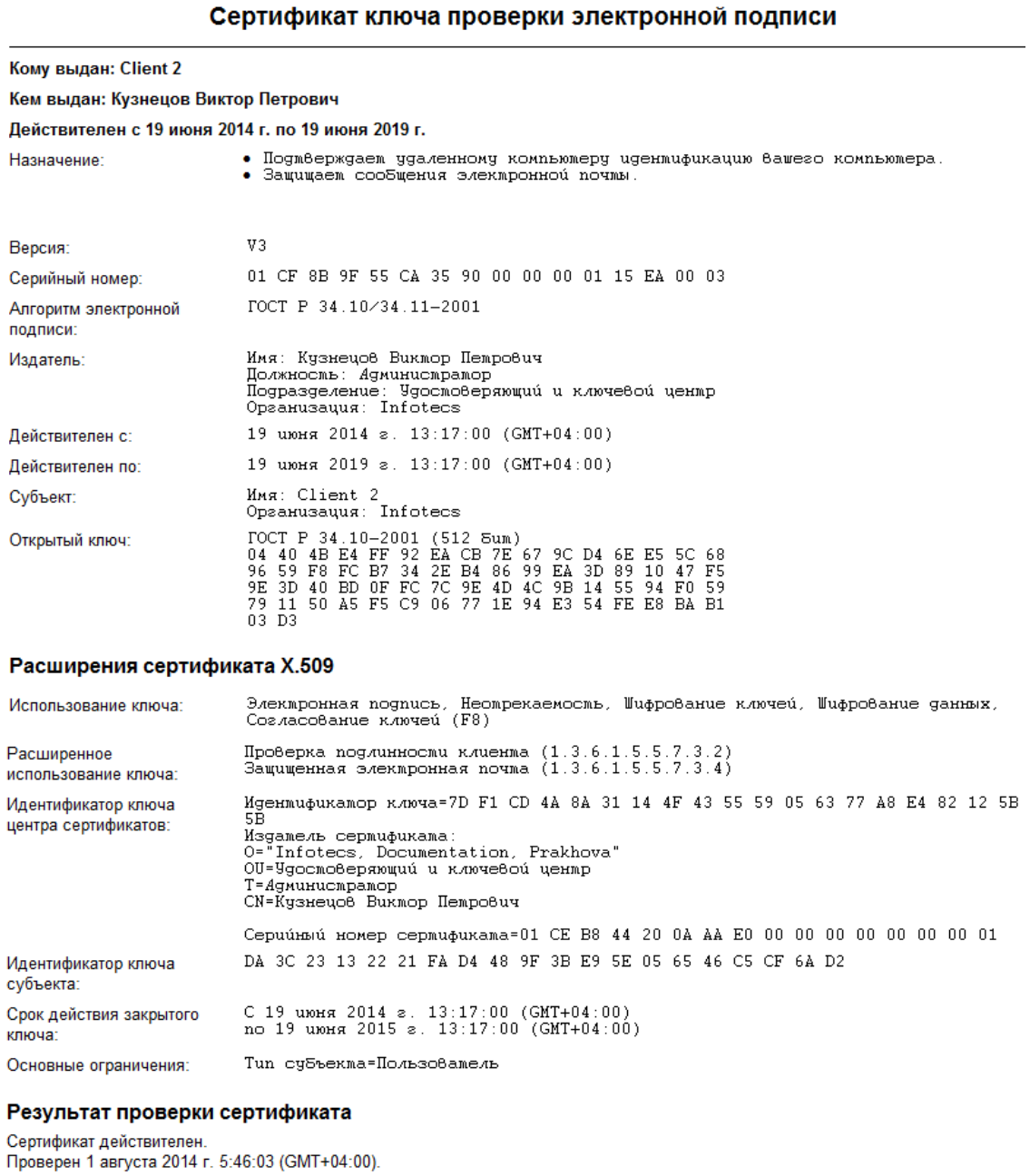
- номер версии стандарта X.509,
- серийный номер сертификата,
- идентификатор алгоритма подписи издателя,
- идентификатор алгоритма подписи владельца,
- имя издателя,
- период действия,
- ключ проверки электронной подписи владельца,
- имя владельца сертификата.

Примечание. Под владельцем понимается сторона, контролирующая ключ электронной подписи, соответствующий данному ключу проверки электронной подписи. Владельцем сертификата может быть конечный пользователь или удостоверяющий центр.

К необязательным полям относятся:

- уникальный идентификатор издателя,
- уникальный идентификатор владельца,
- расширения сертификата.

Рисунок 154. Структура сертификата, соответствующего стандарту X.509 версий 1, 2 и 3



Сертификат ключа проверки электронной подписи

Кому выдан: Client 2

Кем выдан: Кузнецов Виктор Петрович

Действителен с 19 июня 2014 г. по 19 июня 2019 г.

Назначение:	• Подтверждает удаленному компьютеру идентификацию вашего компьютера. • Защищает сообщения электронной почты.
Версия:	V3
Серийный номер:	01 CF 8B 9F 55 CA 35 90 00 00 00 01 15 EA 00 03
Алгоритм электронной подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: Кузнецов Виктор Петрович Должность: Администратор Подразделение: Удостоверяющий и ключевой центр Организация: Infotecs
Действителен с:	19 июня 2014 г. 13:17:00 (GMT+04:00)
Действителен по:	19 июня 2019 г. 13:17:00 (GMT+04:00)
Субъект:	Имя: Client 2 Организация: Infotecs
Открытый ключ:	ГОСТ Р 34.10-2001 (512 Бит) 04 40 4B E4 FF 92 EA CB 7E 67 9C D4 6E E5 5C 68 96 59 F8 FC B7 34 2E B4 86 99 EA 3D 89 10 47 F5 9E 3D 40 BD 0F FC 7C 9E 4D 4C 9B 14 55 94 F0 59 79 11 50 A5 F5 C9 06 77 1E 94 E3 54 FE E8 BA B1 03 D3

Расширения сертификата X.509

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)
Идентификатор ключа центра сертификатов:	Идентификатор ключа=7D F1 CD 4A 8A 31 14 4F 43 55 59 05 63 77 A8 E4 82 12 5B 5B Издатель сертификата: O="Infotecs, Documentation, Prakhova" OU=Удостоверяющий и ключевой центр T=Администратор CN=Кузнецов Виктор Петрович Серийный номер сертификата=01 CE B8 44 20 0A AA E0 00 00 00 00 00 00 00 01
Идентификатор ключа субъекта:	DA 3C 23 13 22 21 FA D4 48 9F 3B E9 5E 05 65 46 C5 CF 6A D2
Срок действия закрытого ключа:	С 19 июня 2014 г. 13:17:00 (GMT+04:00) по 19 июня 2015 г. 13:17:00 (GMT+04:00)
Основные ограничения:	Тип субъекта=Пользователь

Результат проверки сертификата

Сертификат действителен.
Проверен 1 августа 2014 г. 5:46:03 (GMT+04:00).

Рисунок 155. Пример сертификата ViPNet, соответствующего стандарту X.509 версии 3

PKI и асимметричная криптография

Одной из реализаций инфраструктуры, позволяющей управлять сертификатами ключей проверки электронной подписи, является технология PKI (инфраструктура открытых ключей). PKI обслуживает жизненный цикл сертификата: издание сертификатов, хранение, резервное копирование, печать, взаимную сертификацию, ведение списков аннулированных сертификатов (CRL), автоматическое обновление сертификатов после истечения срока их действия.

Основой технологии PKI являются отношения доверия, а главным управляющим компонентом — удостоверяющий центр. Удостоверяющий центр предназначен для регистрации пользователей, выпуска сертификатов, их хранения, выпуска CRL и поддержания его в актуальном состоянии. В сетях ViPNet удостоверяющий центр издаёт 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 создаётся несколько удостоверяющих центров. Доверительные отношения между этими удостоверяющими центрами могут выстраиваться по распределённой или иерархической модели.

- В иерархической модели доверительных отношений удостоверяющие центры объединяются в древовидную структуру, в основании которой находится головной удостоверяющий центр. Головной удостоверяющий центр выдаёт кросс-сертификаты подчинённым ему центрам, тем самым обеспечивая доверие к ключам проверки электронной подписи этих центров. Каждый удостоверяющий центр вышестоящего уровня аналогичным образом делегирует право выпуска сертификатов подчинённым ему центрам. В результате доверие к сертификату каждого удостоверяющего центра основано на заверении его ключом вышестоящего центра. Сертификат головного удостоверяющего центра (корневой сертификат) является самоподписанным. В остальных удостоверяющих центрах администраторы не имеют собственных корневых сертификатов и для установления доверительных отношений формируют запросы на кросс-сертификат к своим вышестоящим удостоверяющим центрам.

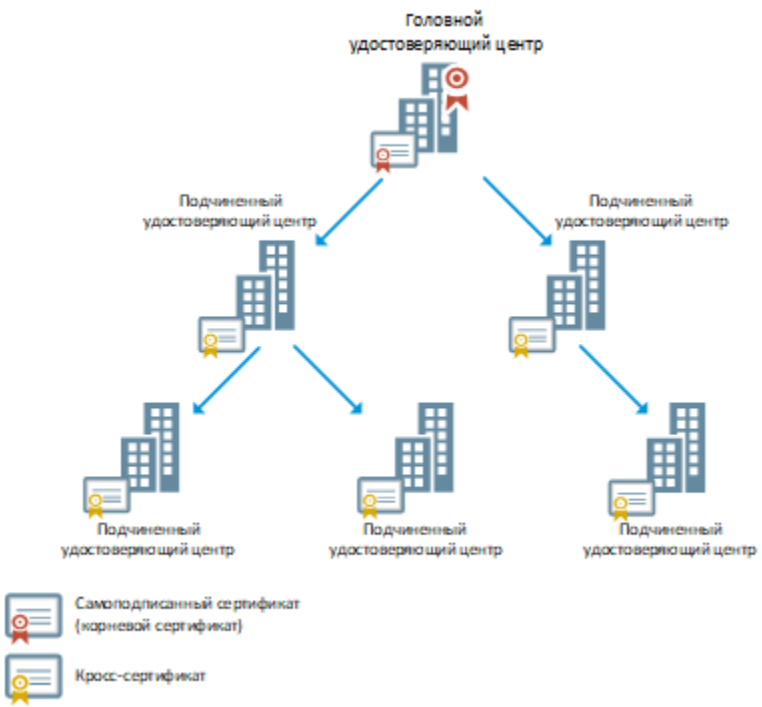


Рисунок 156. Иерархическая модель доверительных отношений

- В распределённой модели доверительных отношений все удостоверяющие центры равнозначны: в каждом удостоверяющем центре администратор имеет свой корневой

(самоподписанный) сертификат. Доверительные отношения между удостоверяющими центрами в этой модели устанавливаются обычно путём двусторонней кросс-сертификации, когда два удостоверяющих центра издают кросс-сертификаты друг для друга. Взаимная кросс-сертификация проводится попарно между всеми удостоверяющими центрами. В результате в каждом удостоверяющем центре в дополнение к корневому сертификату имеются кросс-сертификаты, изданные для администраторов в других удостоверяющих центрах.

Для подписания сертификатов пользователей каждый удостоверяющий центр продолжает пользоваться своим корневым сертификатом, а кросс-сертификат, изданный для другого удостоверяющего центра, использует для проверки сертификатов пользователей другой сети. Это возможно в силу того, что кросс-сертификат для доверенного удостоверяющего центра издаётся на базе его корневого сертификата и содержит сведения о его ключе проверки электронной подписи. Поэтому в сети, отправившей запрос, нет необходимости переиздавать сертификаты пользователей.

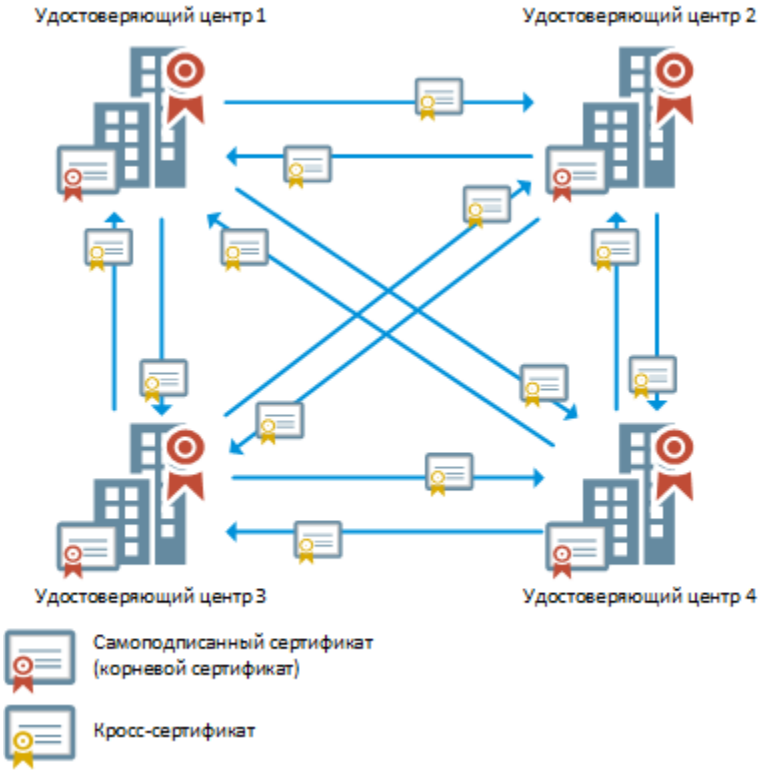


Рисунок 157. Распределённая модель доверительных отношений

Зная иерархию и подчинённость удостоверяющих центров друг другу, можно всегда точно установить, является ли тот или иной пользователь владельцем данного ключа проверки электронной подписи.

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 создаёт 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.

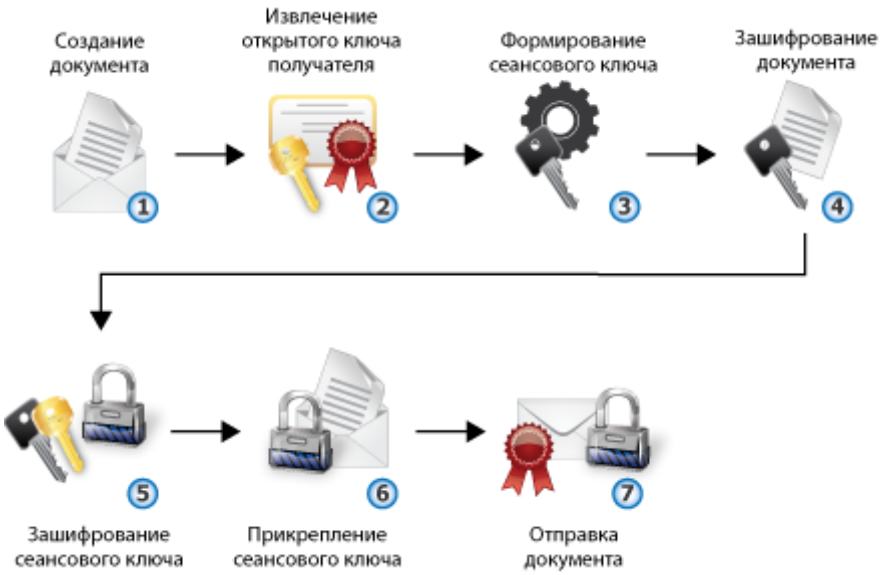


Рисунок 158. Зашифрование электронного документа

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 159. Расшифрование электронного документа

Использование сертификатов для подписания электронных документов

Когда отправитель подписывает документ, он использует ключ электронной подписи, соответствующий ключу проверки электронной подписи, который хранится в сертификате. Когда получатель проверяет электронную подпись сообщения, он извлекает ключ проверки электронной подписи из сертификата отправителя.

Подписание

1 Пользователь создаёт 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 Ключ электронной подписи отправителя извлекается из контейнера ключей.

4 С использованием ключа электронной подписи отправителя на основе значения хэш-функции формируется электронная подпись.

5 Электронная подпись прикрепляется к документу.

6 Зашифрованный документ отправляется.

Рисунок 160. 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 Ключ проверки электронной подписи отправителя извлекается из сертификата отправителя.

5 Электронная подпись расшифровывается с использованием ключа проверки электронной подписи 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 изменён с момента подписания), электронная подпись документа считается недействительной. Электронная подпись считается недействительной также в том случае, если сертификат

отправителя просрочен, аннулирован, искажён или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

Рисунок 161. Процесс проверки электронной подписи документа

Использование сертификатов для подписания и шифрования электронных документов

Подписание и зашифрование

1 Пользователь создаёт электронный документ.

2 Вычисляется значение хэш-функции документа.

3 Ключ электронной подписи отправителя извлекается из контейнера ключей.

4 Открытый ключ получателя извлекается из сертификата получателя.

5 С использованием ключа электронной подписи 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 открытого ключа получателя.

10 Зашифрованный сеансовый ключ прикрепляется к зашифрованному документу.

11 Документ отправляется.

Рисунок 162. 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 Ключ проверки электронной подписи отправителя извлекается из сертификата отправителя.

9 Электронная подпись расшифровывается с использованием ключа проверки электронной подписи 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 изменён с момента подписания), электронная подпись документа считается недействительной. Подпись считается недействительной также в том случае, если сертификат отправителя просрочен,

аннулирован, искажён или подписан удостоверяющим центром, с которым не установлены доверительные отношения.

12 Расшифрованный документ доступен получателю.

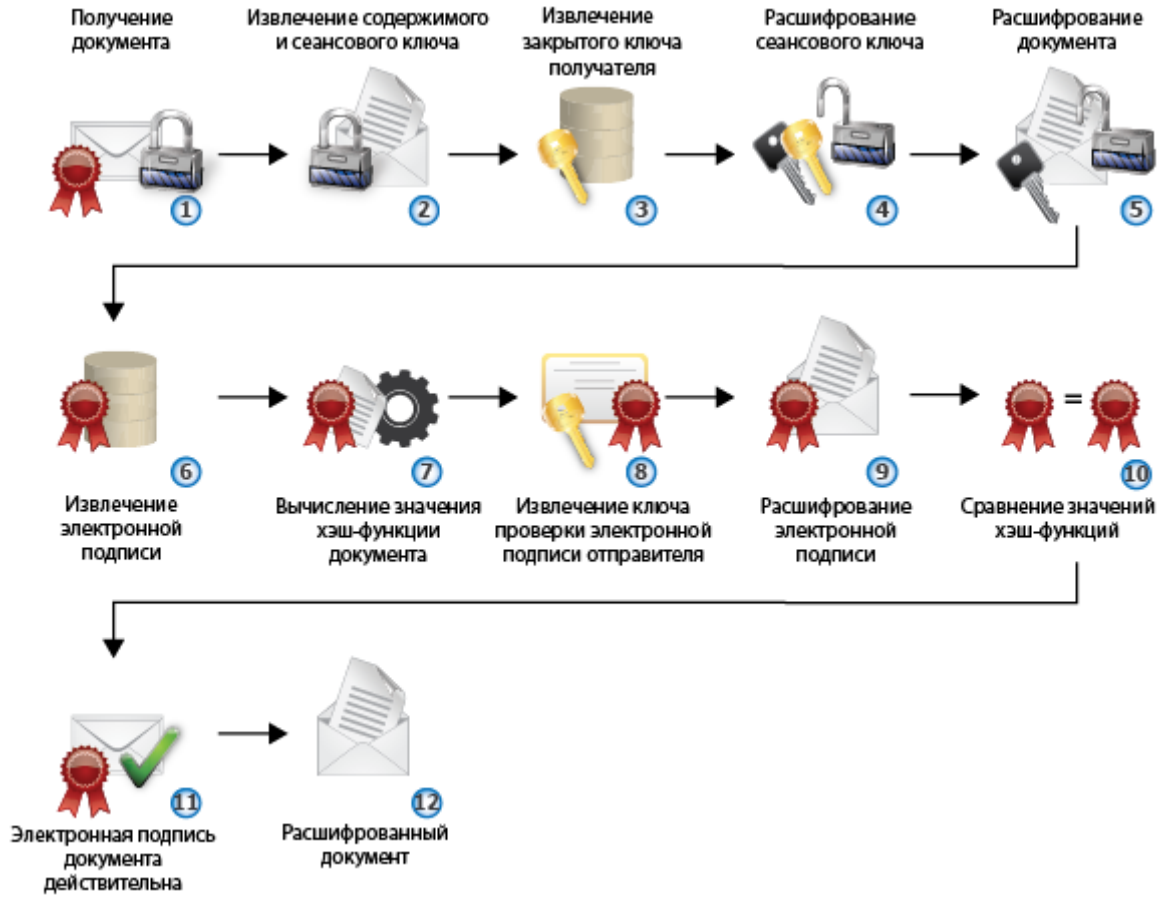


Рисунок 163. Процесс расшифрования и проверки электронной подписи документа

Ключевая система ViPNet

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

Таблица 7. Применение криптографических алгоритмов в ПО ViPNet

Криптографические алгоритмы	
С симметричными ключами	**С асимметричными ключами**
• шифрование IP-трафика • шифрование сообщений программы ViPNet Деловая почта • шифрование прикладных и служебных конвертов	• создание и проверка электронной подписи • шифрование в сторонних приложениях с помощью криптопровайдера ViPNet CSP

Симметричные ключи в ПО ViPNet

Симметричные алгоритмы используются для шифрования информации и контроля её целостности. Для каждой пары сетевых узлов ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager создаётся 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 ключами защиты, которые в свою очередь зашифрованы персональным ключом пользователя, поэтому доступ к этой матрице имеет только пользователь на сетевом узле. Симметричные ключи обмена следует передавать по защищённым каналам (дистрибутивы для первой установки справочников и ключей передаются лично). Если злоумышленники завладеют симметричными ключами, вся система защиты сетевого узла будет скомпрометирована.

Симметричные ключи обмена используются для шифрования IP-трафика, почтовых сообщений, прикладных и транспортных конвертов.

Рисунок 164. Применение ключей обмена

Для защиты ключей обмена применяется три уровня шифрования:

- ключи обмена зашифрованы на ключах защиты;
- ключи защиты зашифрованы на персональных ключах;
- в свою очередь, персональные ключи зашифрованы на парольных ключах.

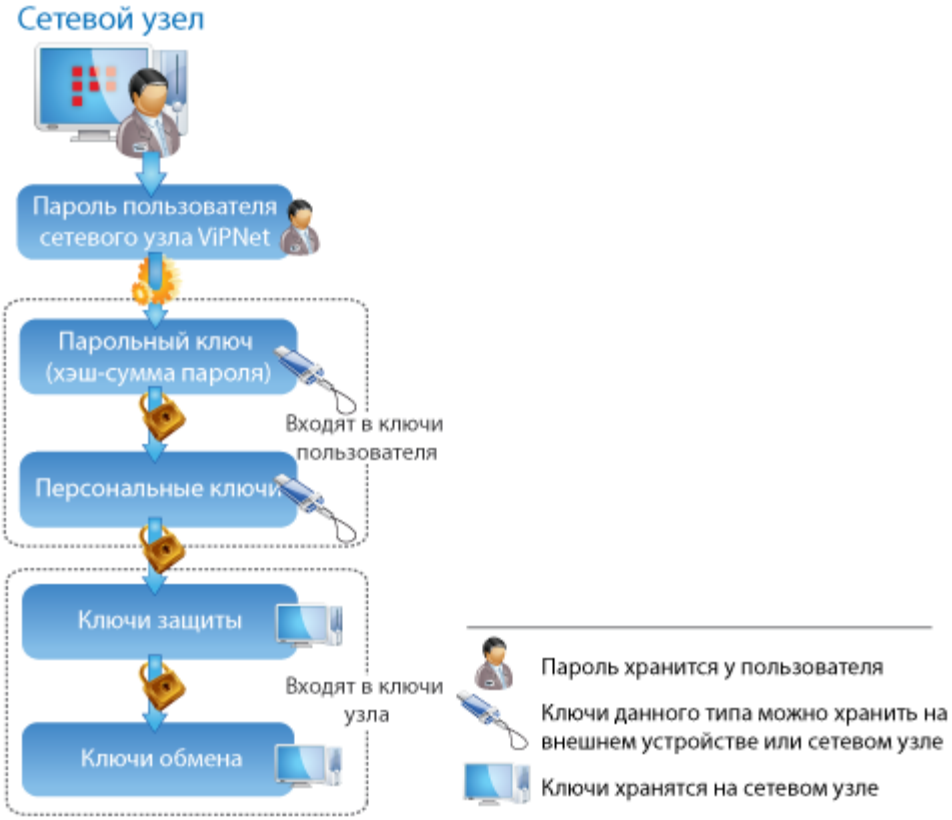


Рисунок 165. Иерархия защиты ключей обмена на сетевом узле

При создании структуры сети ViPNet администратор создаёт в программе ViPNet Administrator файл дистрибутива ключей (`*.dst`) для каждого пользователя сетевого узла ViPNet. Файлы дистрибутивов необходимы для установки справочников и ключей на сетевых узлах. Они содержат ключи пользователя (персональный ключ и ключи электронной подписи), набор ключей обмена с другими сетевыми узлами, справочники, необходимые для связи с другими сетевыми узлами, и регистрационный файл `infotecs.re`. Обновление ключей для сетевых узлов производится по инициативе администратора сети ViPNet.

Примечание. По собственной инициативе пользователь может сделать запрос на обновление сертификата электронной подписи. Для этого в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** нажмите **Обновить сертификат**.

В ПО ViPNet для шифрования по умолчанию используется симметричный алгоритм ГОСТ 28147-89 (длина ключа 256 бит).

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). Если на компьютере установлено ПО ViPNet, в состав которого входит криптопровайдер ViPNet CSP, асимметричные ключи можно использовать для шифрования (см. Асимметричное шифрование). 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 (ключ электронной подписи), а для проверки подписи — сертификат ключа проверки электронной подписи. Сертификат содержит открытый ключ (ключ проверки электронной подписи), удостоверенный (в том числе подписанный) уполномоченным лицом (администратором УКЦ), информацию о владельце сертификата, сроке его действия и прочее.

Пару асимметричных ключей можно независимо создать на сетевом узле ViPNet. Для этого в окне **Настройка параметров безопасности** на вкладке **Электронная подпись** нужно сделать запрос на обновление сертификата, выбрав в качестве назначения ключа **Электронная 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.

Ключ электронной подписи хранится в зашифрованном виде в файле, который называется контейнером ключей. Его следует хранить в тайне от других пользователей: рекомендуется использовать съёмные носители или внешние устройства. Схема защиты ключа электронной подписи в зависимости от места его хранения изображена на следующем рисунке.

Рисунок 166. Схема защиты ключа электронной подписи

Если ключ электронной подписи хранится на внешнем устройстве, ключом защиты для него является парольный ключ. Если ключ электронной подписи хранится на жёстком диске или в дистрибутиве ключей, ключом защиты для него является персональный ключ.

Ключи проверки электронной подписи в сетях ViPNet передаются в составе подписанного сообщения программы ViPNet Деловая почта. Также ключи проверки электронной подписи 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.

Следует понимать, что технология асимметричного шифрования основана на стандартном использовании интерфейса Microsoft CryptoAPI. Следовательно, при использовании данной технологии пользователи ViPNet могут быть не связаны между собой в смысле топологии сети ViPNet (их сети могут не являться доверенными). Для расшифрования сообщения получателю достаточно закрытого ключа, сертификата и установленного на компьютере программного обеспечения, в состав которого входит криптопровайдер ViPNet CSP.

C

События, отслеживаемые ПО ViPNet

Все события разделены на группы и подгруппы. Иерархическая схема этих групп изображена на следующем рисунке:

Рисунок 167. Классификация событий в журнале IP-пакетов

Блокированные IP-пакеты

*Таблица 8. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные фильтрами защищённой 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 защищённой 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 приёма на величину большую, чем указано в настройке допустимого времени отправки принятых пакетов
7	**Неизвестный метод шифрования**	Не поддерживается метод шифрования, код которого указан во входящем пакете
8	**Искаженный IPLIR заголовок**	Недопустимые параметры в расшифрованном пакете
9	**Неизвестный идентификатор сетевого узла**	Идентификатор отправителя в пакете неизвестен
13	**Превышено время жизни IP-пакета**	Пакет уничтожен из-за превышения лимита его нахождения в сети
14	**Получен IP-пакет для другого сетевого узла**	Принят пакет для другого адресата
15	**Слишком много фрагментов для IP-пакета**	Превышено допустимое количество одновременно обрабатываемых фрагментированных пакетов
16	**Исчерпана лицензия на количество туннелируемых адресов**	Это событие регистрируется только на координаторе, осуществляющем туннелирование. На координатор одновременно поступили пакеты от большего количества узлов, чем разрешено лицензией
17	**Неверный IP-адрес**	Поступил пакет с некорректным или неизвестным IP-адресом. Чаще всего событие возникает на координаторе в следующем случае: на координатор поступил зашифрованный пакет, предназначенный для туннелируемого узла данного координатора, но IP-адрес этого узла отсутствует в списке туннелируемых адресов координатора

18	**Неизвестный IP-адрес получателя**	В пакете отсутствует или указан неизвестный IP-адрес получателя
19	**Попытка отправителя послать сообщение от имени чужого узла**	Поступил пакет от узла, который не является его отправителем
70	**Пакет заблокирован транзитным фильтром для защищённого узла**	Это событие регистрируется только на координаторе с операционной системой Linux. Пакет заблокирован фильтрами для транзитного зашифрованного трафика

*Таблица 9. Группа **Все IP-пакеты\Блокированные IP-пакеты\IP-пакеты, блокированные фильтрами открытой сети***

№ события	Название события	Описание события
22	**Незашифрованный IP-пакет от сетевого узла**	От защищённого адресата пришёл открытый пакет
23	**Незашифрованный широковещательный IP-пакет от сетевого узла**	От защищённого адресата пришёл открытый широковещательный пакет
24	**Открытый IP-пакет для служб ViPNet**	Служебный трафик ViPNet поступил в открытом виде
30	**Локальный IP-пакет блокирован фильтром открытой сети**	Пакет блокируется локальным фильтром открытой сети или для пакета не удалось найти подходящий фильтр
31	**Транзитный IP-пакет блокирован фильтром открытой сети**	Это событие регистрируется только на координаторе. Пакет блокируется транзитным фильтром открытой сети или для пакета не удалось найти подходящий фильтр
32	**Широковещательный IP-пакет блокирован фильтром открытой сети**	Пакет блокируется фильтром открытого широковещательного трафика или для пакета не удалось найти подходящий фильтр
33	**IP-пакет блокирован фильтром антиспуфинга**	Это событие регистрируется только на координаторе. Найден соответствующий фильтр в таблице антиспуфинга
35	**Превышено максимальное число защищаемых адресов**	В течение заданного периода времени были получены IP-пакеты от большего количества адресов, чем задано в лицензии
37	**Пакет блокирован фильтром для туннелируемых узлов**	Это событие регистрируется только на координаторе. Пакет блокируется фильтром трафика туннелируемых узлов или для пакета не удалось найти подходящий фильтр
39	**IP-пакет блокирован фильтрами по умолчанию при загрузке компьютера**	Пакет заблокирован фильтрами по умолчанию при загрузке компьютера

*Таблица 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
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 появлялась несколько раз, обратитесь в службу поддержки ИнфоТеКС. Возможно, потребуется обновление версии драйвера, использующего больше машинных ресурсов, или более новая 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
94	**Недостаточно памяти**	Для выполнения какой-либо операции требуется выделение памяти, но выделить память не удалось
95	**Обнаружен сетевой узел с таким же идентификатором**	В сети появился узел с таким же идентификатором, но другим IP-адресом
97	**IP-пакет должен быть фрагментирован, но установлен флаг DF**	Заблокирован IP-пакет с установленным флагом DF, передача пакетов без фрагментации невозможна
98	**Недостаточно ресурсов для обработки IP-пакета**	Событие интерпретируется как событие 90
100	**IP-пакет заблокирован в ходе инспекции состояния соединения**	IP-пакет не принадлежит текущей сессии и заблокирован в ходе инспекции с отслеживанием состояния (Stateful Packet Inspection)
101	**Не найден маршрут для транзитного IP-пакета**	Это событие регистрируется только на координаторе. Не найдено правило для транзитного пакета в таблице маршрутов
103	**Превышено максимальное количество соединений**	Количество уже установленных соединений превышает максимально допустимое ПО ViPNet (не лицензией)
104	**Соединение уже существует**	Если параметры исходящих пакетов для создаваемого соединения совпадают с уже существующими, то такое соединение блокируется
105	**Не удалось выделить динамический порт для правила трансляции адресов**	Это событие регистрируется только на координаторе. Координатор не смог выделить порт для динамического правила трансляции адресов (например, все порты в пуле закончились)
111	**Не найден ключ обмена**	Не найден ключ для связи с сетевым узлом получателя
112	**Нарушена имитовставка открытой части зашифрованного пакета 4.2**	Неверное значение имито для транзитного зашифрованного трафика
113	**Неизвестный ID источника**	Неизвестный идентификатор сетевого узла–источника транзитного зашифрованного пакета
115	**Не удалось найти маршрут для IP-пакета**	По каким-либо причинам не найден маршрут в таблице маршрутизации
116	**Сетевой интерфейс не найден**	IP-пакет не может быть отправлен, так как не найден сетевой интерфейс
117	**Не удалось разрешить MAC-адрес по IP-адресу**	Не удалось определить MAC-адрес получателя пакета по его IP-адресу

118	**Не удалось произвести шифрование IP-пакета**	Ошибка при шифровании исходящего IP-пакета для защищённого 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 защищённого 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
131	**Ошибка в таблице маршрутизации**	Ошибка обработки прикладных протоколов: не удалось построить маршрут

Примечание. Если вы используете Windows Server 2008 R2 или более позднюю версию Windows, события 82 и 89 не фиксируются в журнале IP-пакетов, так как операционная система автоматически блокирует соответствующие IP-пакеты.

Пропущенные IP-пакеты и служебные события

*Таблица 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**	Найден разрешающий фильтр открытой сети для локальных IP-пакетов
61	**Пропущен незашифрованный широковещательный IP-пакет**	Найден разрешающий фильтр открытой сети для широковещательных IP-пакетов
62	**Пропущен незашифрованный транзитный IP-пакет**	Это событие регистрируется только на координаторе. Найден разрешающий фильтр открытой сети для транзитных IP-пакетов
63	**Пакет пропущен фильтром для туннелируемых узлов**	Это событие регистрируется только на координаторе. Найден разрешающий фильтр для IP-пакетов от туннелируемых узлов
64	**IP-пакет пропущен фильтрами по умолчанию при загрузке компьютера**	Пакет пропущен фильтрами, которые действуют при загрузке компьютера

*Таблица 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 межсетевой экран с динамической или статической трансляцией адресов.
46	**Изменились параметры доступа к сетевому узлу**	Драйвер обнаружил, что параметры доступа к сетевому узлу через внешнюю сеть изменились, и соответствующим образом скорректировал свои таблицы. Событие регистрируется для сетевых узлов, работающих через межсетевой экран с динамической или статической трансляцией адресов. В качестве IP-адресов и портов регистрируются данные из IP-пакета, поступившего из сети, до его преобразования драйвером.
47	**Истёк тайм-аут**	Истёк тайм-аут поддержки соединений через устройства с динамической трансляцией IP-адресов.
48	**Адрес сетевого узла зарегистрирован из широковещательного пакета**	Зарегистрировано событие, что от узла поступают широковещательные пакеты.
49	**Изменились параметры доступа к своему узлу из внешней сети**	Поступила информация об изменении параметров доступа через внешнюю сеть к своему сетевому узлу. В качестве IP-адресов и портов регистрируются данные по доступу к своему узлу (**Получатель**) и к узлу, от которого получена информация (**Отправитель**).
110	**На DNS-сервере зарегистрирован новый IP-адрес узла**	Поступило сообщение от DNS-сервера, что для узла с именем, указанным в поле **Отправитель**, зарегистрирован IP-адрес, указанный в поле **IP-адрес отправителя.**
114	**Имя на DNS- (WINS-) сервере не зарегистрировано**	Ответ DNS-сервера об отсутствующем имени заблокирован, запрос на преобразование этого имени передан другому DNS-серверу.
138	**Заблокирован пакет на публичный DNS-сервер**	Заблокирован запрос на публичный DNS-сервер, так как в текущем режиме работы этот запрос должен быть обработан защищённым DNS-сервером.

D

Региональные настройки

Для корректного отображения русской локализации интерфейса программ ViPNet в русифицированных ОС Microsoft Windows английской локализации необходимо установить поддержку кириллицы для программ, не поддерживающих Юникод. Эти настройки рекомендуется производить до установки самой программы.

Данные настройки также понадобится сделать, если установлен русскоязычный MUI (Multilanguage User Interface). Это значит, что ядро операционной системы английское, а русский язык для интерфейса и файлов справки был установлен позже. В этом случае региональные настройки по умолчанию английские и требуют изменения.

Внимание! Для изменения региональных настроек вы должны обладать правами администратора операционной системы.

Региональные настройки в Windows

Чтобы установить поддержку кириллицы:

1 Откройте панель управления (Control Panel) и в категории **Часы, язык и регион** (**Clock, Language, and Region**) выберите параметр **Изменение форматов даты, времени и чисел** (**Change date, time, or number formats**).

2 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

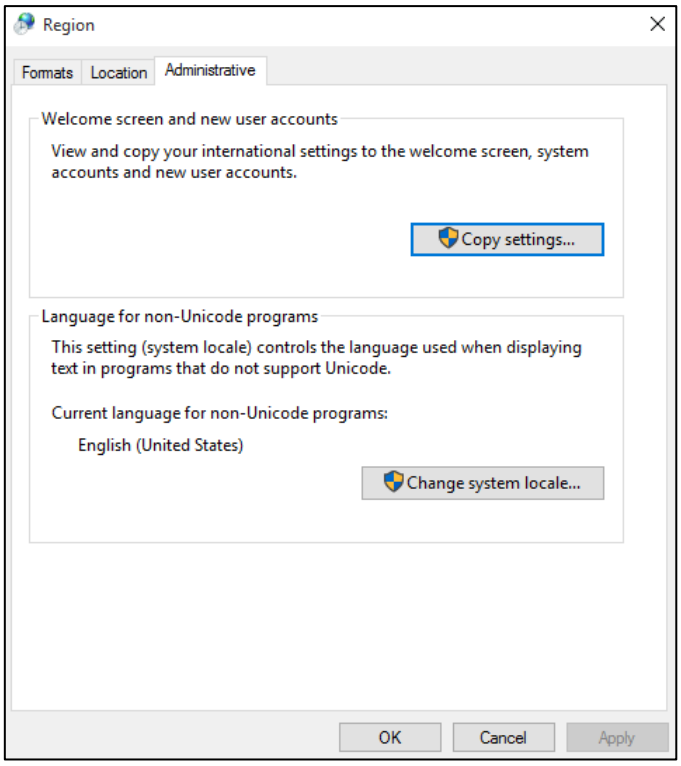


Рисунок 168. Дополнительные языковые параметры

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

4 В появившемся окне в списке выберите **Русский (Россия)** (**Russian (Russia)**).

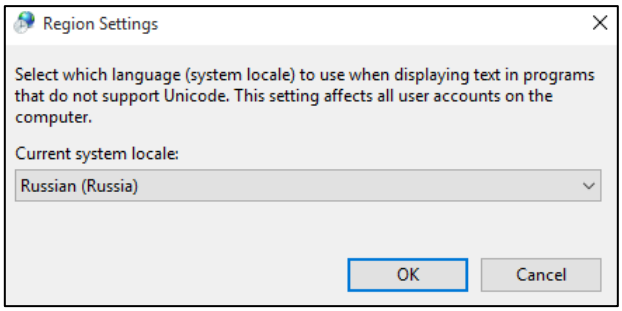


Рисунок 169. Выбор языка системы

5 Нажмите **OK**. Перезагрузите компьютер.

6 Дождитесь завершения перезагрузки компьютера, откройте панель управления (Control Panel) и в категории **Часы, язык и регион** (**Clock, Language, and Region**) выберите параметр **Изменение форматов даты, времени и чисел** (**Change date, time, or number formats**).

7 В окне **Регион** (**Region**) перейдите на вкладку **Дополнительно** (**Administrative**).

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

9 В открывшемся окне в списке **Копировать текущие параметры в** (**Copy your current settings to**) установите флажок **Экран приветствия и системные учетные записи** (**Welcome screen and system accounts**) и нажмите **OK**.

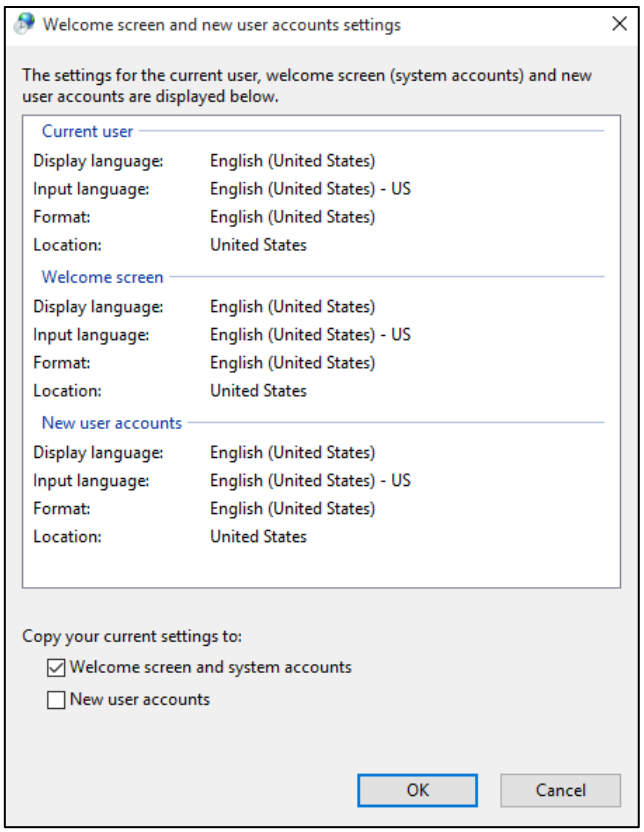


Рисунок 170. Копирование параметров

Также для исключения проблем с кодировкой в некоторых системах рекомендуется выполнить следующие действия:

1 В окне **Регион** (**Region**) на вкладке **Форматы** (**Formats**) в списке **Формат** (**Format**) выберите **Русский (Россия)** (**Russian (Russia)**).

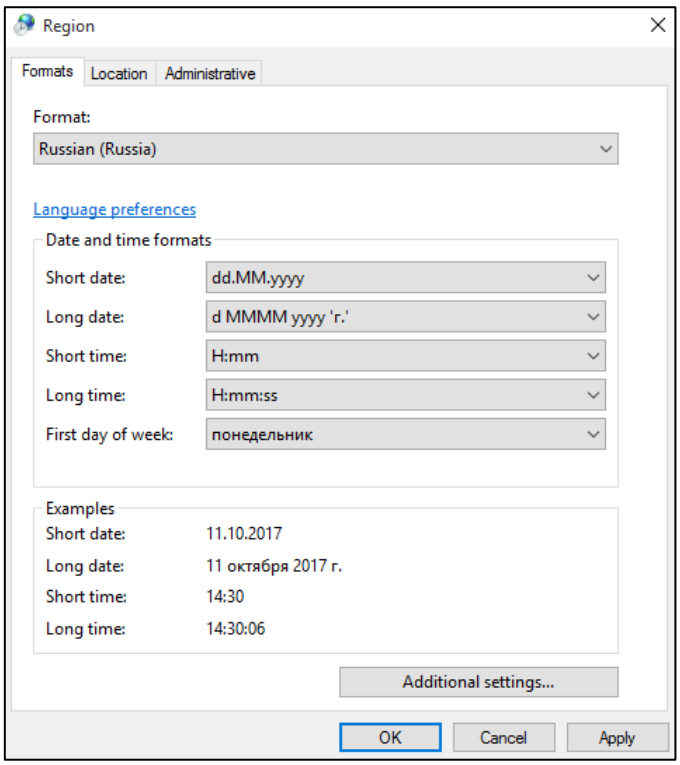


Рисунок 171. Настройка форматов

2 В окне **Регион** (**Region**) на вкладке **Местоположение** (**Location**) в списке **Основное расположение** (**Home location**) выберите **Россия** (**Russia**).

Примечание. В Windows 10 версии 1809 и выше нет вкладки **Location**, поэтому указанный параметр настраивать не нужно.

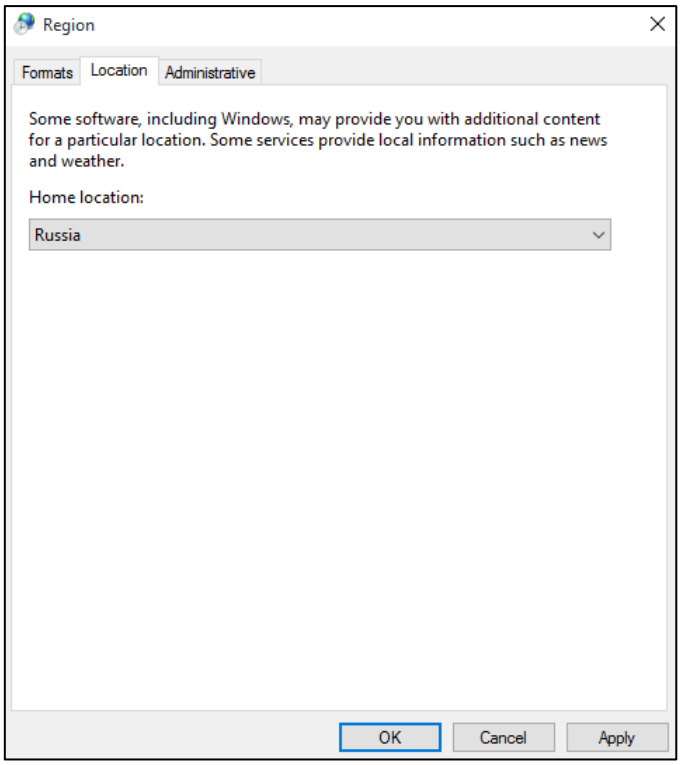


Рисунок 172. Выбор текущего расположения

Отключение Юникода (UTF-8) для поддержки языка во всём мире

Для установки и правильной работы программы ViPNet Client в Windows 10 отключите использование Юникода:

1 В меню **Пуск** выберите **Параметры** > **Время и язык** > **Язык** > **Административные языковые параметры**.

2 В окне **Регион** на вкладке **Дополнительно** нажмите **Изменить язык системы**.

3 В окне **Региональные стандарты** снимите флажок **Бета-версия: Использовать Юникод (UTF-8) для поддержки языка во всем мире**.

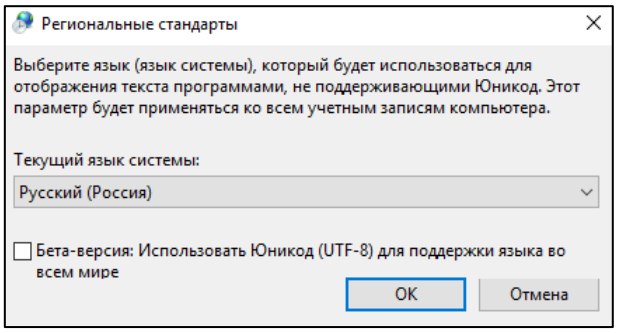


Рисунок 173. Отключение использования UTF-8

4 Перезагрузите компьютер, чтобы изменения вступили в силу.

E

Внешние устройства

Общие сведения

Внешние устройства предназначены для хранения контейнеров ключей, которые вы можете использовать для аутентификации, формирования электронной подписи или для других целей.

На внешнем устройстве могут храниться ключи, созданные по различным алгоритмам в программном обеспечении ViPNet или в сторонних программах. Максимальное количество контейнеров ключей, которое может храниться на одном внешнем устройстве, зависит от объёма памяти устройства.

Программное обеспечение ViPNet Client поддерживает два способа аутентификации с помощью внешнего устройства (см. Способы аутентификации пользователя):

- По персональному ключу пользователя ViPNet, который хранится на устройстве. Этот способ аутентификации имеет следующие ограничения:
  - Одно внешнее устройство невозможно использовать для аутентификации нескольких пользователей ViPNet.
  - Одно внешнее устройство невозможно использовать для аутентификации одного пользователя на нескольких узлах ViPNet.
  - Если используется этот способ аутентификации, тогда ключи электронной подписи пользователя, изданные в удостоверяющем центре на базе ПО ViPNet, должны храниться на одном устройстве с персональным ключом.
- По сертификату, который хранится на устройстве вместе с соответствующим закрытым ключом. Требования к сертификату см. в разделе Особенности аутентификации с помощью сертификата.

Все операции с контейнерами ключей и внешними устройствами вы можете выполнить в программе ViPNet CSP (см. Настройка параметров криптопровайдера ViPNet CSP). Чтобы

использовать какое-либо внешнее устройство, на компьютер необходимо установить драйверы этого устройства. Перед записью ключей на устройство убедитесь, что оно отформатировано.

Список поддерживаемых внешних устройств

В следующей таблице перечислены внешние устройства, которые могут быть использованы в ViPNet Client. Для каждого семейства устройств в таблице приведено описание, указаны условия и особенности работы с устройствами.

Таблица 14. Поддерживаемые внешние устройства

Название семейства устройств в ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
ESMART Token	Смарт-карты и токены типов: • **ESMART Token**, • **ESMART Token ГОСТ**	На компьютере должно быть установлено ПО ESMART PKI Client для Windows (рекомендуемая версия — 4.11). Устройства типа ESMART Token необходимо отформатировать с помощью ПО ESMART PKI Client для Windows с профилем ViPNet2. Перенос ключей подписи с устройства и на устройство ESMART Token ГОСТ невозможен, так как на устройстве используется аппаратная криптография с неизвлекаемым ключом.
Infotecs Software Token	**ViPNet SoftToken** — программная реализация стандарта PKCS#11.	Необходимо установить компонент ViPNet SoftToken (входит в состав ПО ViPNet OpenSSL). С помощью программы `token_manager.exe` на компьютере должен быть создан программный токен. Подробную информацию о работе с программным токеном см. в документе «ViPNet SoftToken. Руководство разработчика», раздел «Использование утилиты token_manager для работы с программными токенами».
aKey	Смарт-карты: • **aKey S1000**, • **aKey S1003**, • **aKey S1004** производства компании Ak Kamal Security.	На компьютере должна быть установлена библиотека `akpkcs11.dll`, предоставленная компанией Ak Kamal Security. Устройство имеет два ПИН-кода: администратора и пользователя. Значение этих ПИН-кодов по умолчанию — `12345678`. Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.

Название семейства устройств в ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
ViPNet HSM	Программно-аппаратный комплекс **ViPNet HSM** производства АО «ИнфоТеКС».	На компьютере должно быть установлено ПО ViPNet HSM SDK. В ViPNet CSP необходимо задать параметры подключения к серверу ViPNet HSM.
JaCarta	Персональные электронные ключи и смарт-карты: • **eToken ГОСТ**, • **eToken PRO (Java)**, • **JaCarta PKI**, • **JaCarta LT**, • **JaCarta SE,** • **JaCarta PKI/ГОСТ,** • **JaCarta PRO,** • **JaCarta-2 PKI/ГОСТ,** • **JaCarta-2 ГОСТ,** • **JaCarta-2 PRO/ГОСТ** производства компании «Аладдин Р.Д.».	На компьютере должно быть установлено ПО «Единый Клиент JaCarta» компании «Аладдин Р.Д.» (рекомендуемая минимальная версия — 2.13). Перенос ключей подписи с апплетов «Криптотокен» и «Криптотокен 2 ЭП» (модели JaCarta со словом «ГОСТ» в названии) и на эти апплеты невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. Работа с апплетом PRO через ПО «Единый Клиент JaCarta» версии 2.12 не поддерживается. Необходимо установить последнее обновление ПО «Единый Клиент JaCarta» с сайта производителя либо обратиться в службу поддержки компании «Аладдин Р.Д.».
Rutoken	Электронные идентификаторы: • **Рутокен ЭЦП 2.0 2000,** • **Рутокен ЭЦП 3.0 3220,** • **Рутокен ЭЦП 3.0 NFC 3100, серт. ФСБ,** • **Рутокен Lite** производства компании «Актив».	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.13.0.0). Перенос ключей подписи с устройств, а также на устройства Рутокен ЭЦП 2.0 невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом. При использовании Rutoken Lite возможна аутентификация только по персональному ключу на устройстве.
Rutoken S	Электронные идентификаторы **Рутокен S** производства компании «Актив».	На компьютере должны быть установлены драйверы Rutoken (рекомендуемая версия — 4.13.0.0).

Название семейства устройств в ViPNet CSP	Полные названия и типы устройств	Необходимые и рекомендуемые условия работы с семейством устройств
R301 Foros	Смарт-карты и токены **R301 Форос PKCS** производства компании «СмартПарк».	На компьютере должна быть установлена библиотека `foros_pkcs11.dll` (для 32-разрядной либо 64-разрядной архитектуры процессора), предоставленная компанией «СмартПарк». Перенос ключей подписи с устройств и на устройства данного семейства невозможен, так как на устройствах используется аппаратная криптография с неизвлекаемым ключом.
SafeNet eToken (eToken Aladdin)	Персональные электронные ключи и смарт-карты: • **Gemalto SafeNet eToken 5100/5105**, **5200/5205**, **5110**, **7300**, • **Gemalto SafeNet eToken 4100**, • **eToken PRO** производства компаний «Аладдин Р.Д.» и Gemalto (SafeNet).	Если компьютер работает под управлением ОС Windows 10, на нем должно быть установлено ПО SafeNet Authentication Client (рекомендуемая версия — 10.6.146). Если компьютер работает под управлением другой ОС, на нем должно быть установлено либо ПО PKI Client версии 5.1 SP1, либо ПО SafeNet Authentication Client (рекомендуемая версия — 10.6.146). Смарт-карта **eToken PRO** может использоваться с любым стандартным PC/SC-совместимым устройством считывания карт. **Примечание**. Если вам необходимо работать с устройством из семейства **SafeNet eToken (eToken Aladdin),** то во избежание появления ошибок при выполнении криптографических операций не устанавливайте на компьютер одновременно ПО «Единый Клиент JaCarta» и ПО SafeNet Authentication Client. Работа с устройствами JaCarta PRO с помощью драйверов SafeNet возможна, но не рекомендуется производителем.

Примечание. Список поддерживаемых операционных систем для каждого из приведённых устройств вы найдёте на официальном веб-сайте производителя этого устройства.

Алгоритмы и функции, поддерживаемые внешними устройствами

В следующей таблице перечислены криптографические алгоритмы, поддерживаемые внешними устройствами, приведена информация о возможности использования устройств в качестве датчиков случайных чисел, а также 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 ключа проверки электронной подписи), разработанных компанией RSA Laboratories. Стандарт определяет независимый от платформы интерфейс API для работы с криптографическими устройствами идентификации и хранения данных.

Таблица 15. Алгоритмы и функции, поддерживаемые внешними устройствами

Название семейства устройств в ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использо-вание ДСЧ в ViPNet CSP	Поддержка PKCS#11
ESMART Token	**ESMART Token** — отсутствует; **ESMART Token ГОСТ** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	**ESMART Token** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 **ESMART Token ГОСТ** — отсутствует	Да	Да
Infotecs Software Token	Изолированная программная реализация: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012		Нет	Да
aKey	**aKey S1000**, **aKey S1003**, **aKey S1004** — ГОСТ Р 34.10-2012; **aKey S1000**, **aKey S1003** — ГОСТ Р 34.10-2001	отсутствует	Нет	Да
ViPNet HSM	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	отсутствует	Нет	Да

Название семейства устройств в ViPNet CSP	Аппаратная поддержка российских криптографических алгоритмов (на устройстве)	Программная поддержка российских криптографических алгоритмов (в ViPNet CSP)	Использо-вание ДСЧ в ViPNet CSP	Поддержка PKCS#11
JaCarta (устройства JaCarta PKI, JaCarta SE, JaCarta LT, JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом Laser)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
JaCarta (устройства JaCarta PKI/ГОСТ и JaCarta-2 PKI/ГОСТ с апплетом ГОСТ, JaCarta-2 ГОСТ)	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (короткий ключ 256 бит)	отсутствует	Да	Да
Rutoken	**Рутокен ЭЦП 2.0** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012; **Рутокен Lite** — отсутствует	**Рутокен ЭЦП 2.0** — отсутствует; **Рутокен Lite** — ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	**ЭЦП 2.0** — да; **Lite** — нет	Да
Rutoken S	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да
SafeNet eToken (eToken Aladdin)	отсутствует	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012	Нет	Да

Примечание. Выработка ключей шифрования (функция `C_DeriveKey` интерфейса PKCS#11) поддерживается не всеми перечисленными устройствами. Для получения более подробной информации см. документацию по необходимому устройству.

F

Предустановленные сетевые фильтры

В таблицах перечислены сетевые фильтры, которые, в зависимости от конфигурации программы ViPNet Client, могут быть установлены по умолчанию.

Фильтры перечислены в соответствии с очерёдностью их применения в программе ViPNet Client. В этом же порядке они отображаются на панели просмотра главного окна в разделах **Фильтры защищённой сети** и **Фильтры открытой сети**.

Подробнее о сетевых фильтрах см. раздел Общие сведения о сетевых фильтрах.

Таблица 16. Фильтры защищённой сети

Действие фильтра	Имя фильтра	Источник	Назначение	Протоколы фильтрации пакетов и их свойства
Фильтры специальной конфигурации «Открытый Интернет»				
Разрешить	Служебный трафик ViPNet	InternetGateway	Все узлы	ViPNet: базовые службы (UDP: 2046, с 2048 на 2048, с 2050 на 2050) ViPNet StateWatcher (TCP, dst: 2047, 5100, 10092) ViPNet MFTP (TCP: dst:5000-5003)
Разрешить	Служебный трафик ViPNet	Все узлы	InternetGateway	ViPNet: базовые службы (UDP: 2046, с 2048 на 2048, с 2050 на 2050) ViPNet StateWatcher (TCP, dst: 2047, 5100, 10092) ViPNet MFTP (TCP: dst:5000-5003)

Действие фильтра	Имя фильтра	Источник	Назначение	Протоколы фильтрации пакетов и их свойства
Блокировать	Входящий трафик от координатора Открытого Интернета	InternetGateway	Все узлы	Все
Блокировать	Исходящий трафик на координатор Открытого Интернета	Все узлы	InternetGateway	Все
Предустановленные настраиваемые фильтры				
Разрешить	DHCP-трафик	Все узлы	Все узлы	DHCP (UDP: с 67 на 68, с 68 на 67)
Разрешить	NetBIOS- и WINS-трафик	Все узлы	Все узлы	NetBIOS-DGM (UDP: с 138 на 138) NetBIOS-NC (UDP: с 137 на 137)
Разрешить	Служебный трафик ViPNet	Все узлы	Все узлы	ViPNet: базовые службы (UDP: 2046, с 2048 на 2048, с 2050 на 2050) ViPNet StateWatcher (TCP, dst: 2047, 5100, 10092) ViPNet MFTP (TCP: dst:5000-5003)
Разрешить	Ping	Все узлы	Все узлы	Ping (ICMP8)
Разрешить	RDP-трафик	Все узлы	Все узлы	RDP (TCP, dst:3389)
Разрешить	IGMP-трафик	Все узлы	Все узлы	IGMP (IP: 2)
Разрешить	Мультимедиа-трафик	Все узлы	Все узлы	SIP (TCP/UDP, dst:5060) H323 (TCP, dst:1720) SCCP (TCP, dst:2000)
Разрешить	Весь трафик	Все узлы	Все узлы	Все
Фильтр по умолчанию				
Блокировать	Прочий трафик	Все узлы	Все узлы	Все

Таблица 17. Фильтры открытой сети

Действие фильтра	Имя фильтра	Источник	Назначение	Протоколы фильтрации пакетов и их свойства
Предустановленные настраиваемые фильтры				
Разрешить	DHCP-трафик	Все узлы	Все узлы	DHCP (UDP: с 67 на 68, с 68 на 67)
Разрешить	NetBIOS- и WINS-трафик	Все узлы	Все узлы	NetBIOS-DGM (UDP: с 138 на 138) NetBIOS-NC (UDP: с 137 на 137)
Разрешить	IGMP-трафик	Все узлы	Все узлы	IGMP (IP: 2)
Разрешить	Ping	Все узлы	Все узлы	Ping (ICMP8)
Разрешить	Исходящий трафик	Мой узел	Все узлы	Все
Фильтр по умолчанию				
Блокировать	Прочий трафик	Все узлы	Все узлы	Все

G

Совместная работа ViPNet Client с другими приложениями

Технология Hyper-V

Hyper-V — это система виртуализации, реализованная в 64-разрядной версии операционной системы Microsoft Windows Server 2008 R2.

Особенностью Hyper-V является то, что для обеспечения доступа машин к внешней сети требуется выделить один из физических сетевых интерфейсов компьютера. Этот интерфейс будет подключён 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 Client на компьютер с 64-разрядной операционной системой на всех сетевых интерфейсах компьютера включается служба Iplir lightweight Filter (x64 edition), то есть сетевой ViPNet-драйвер (см. Низкоуровневый ViPNet-драйвер сетевой защиты). Этот драйвер осуществляет шифрование, расшифрование и фильтрацию IP-пакетов, проходящих через сетевой интерфейс, и может нарушить работоспособность виртуальной сети Hyper-V.

Чтобы обеспечить работу виртуальной сети и программного обеспечения ViPNet в хостовой операционной системе, в настройках физического сетевого интерфейса, подключённого к виртуальной сети Hyper-V, требуется отключить службу Iplir lightweight Filter (x64 edition).

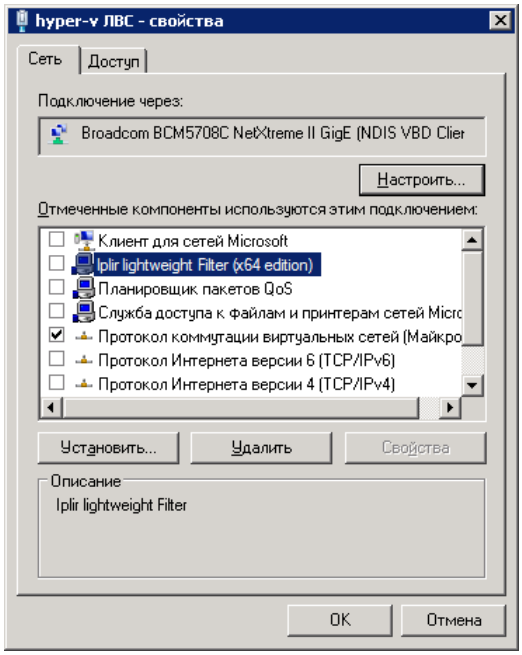


Рисунок 174. Настройки физического интерфейса, подключённого к виртуальной сети Hyper-V

Dallas Lock

Внимание! Рекомендации, приведённые в данном разделе, относятся к программному обеспечению Dallas Lock версии 8.0. Прежде чем приступать к настройке Dallas Lock 8.0 ознакомьтесь с руководством по эксплуатации программы.

Чтобы обеспечить на компьютере совместную работу программы ViPNet Client и системы защиты от несанкционированного доступа Dallas Lock, в программе ViPNet Client создайте фильтр (см. Создание сетевых фильтров), разрешающий входящие и исходящие соединения с сервером безопасности Dallas Lock по следующим портам TCP: 17490, 17491, 17492.

ESET NOD32 Smart Security

При совместной установке на компьютер ПО ViPNet Client и ESET NOD32 Smart Security возможны проблемы с установлением соединения между защищёнными узлами и доступом к ресурсам интернета. Чтобы обеспечить на компьютере совместное функционирование программ ViPNet Client и ESET NOD32 Smart Security, в программе ESET NOD32 Smart Security создайте правила, разрешающие обмен данными по протоколу 241 (см. Протоколы соединений в защищённой сети) и использование компонента `Itcsnatproxy.exe`.

Примечание. Приведённые ниже действия относятся только к ESET NOD32 Smart Security. Программы ESET NOD32 Internet Security и ESET NOD32 Антивирус дополнительно настраивать не требуется.

Выполните следующие действия:

1. Откройте главное окно программы ESET NOD32 Smart Security и выберите вкладку **Настройка**.
2. В правой части окна щёлкните ссылку **Сеть** и в открывшемся окне щёлкните ссылку **Настроить правила и зоны**.
3. В окне **Настройка зон и правил** нажмите **Создать**.
4. В окне **Новое правило** выберите вкладку **Общие** и в группе **Общая информация об этом правиле** укажите название разрешающего правила для протокола 241.

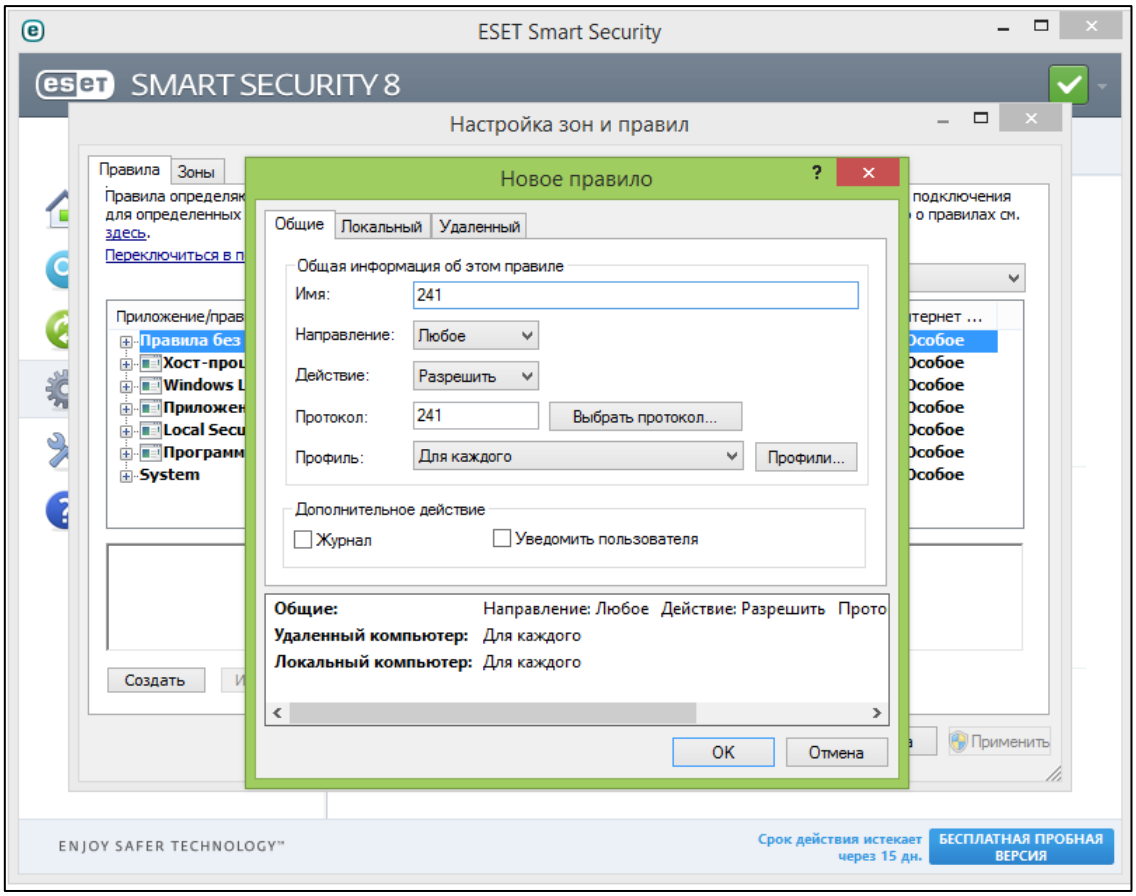


Рисунок 175. Создание правила в ESET NOD32 Smart Security для протокола 241

5 Нажмите **Выбрать протокол** и выберите протокол 241.

6 Нажмите **OK**, чтобы сохранить правило.

7 В окне **Настройка зон и правил** нажмите **Создать**, чтобы создать правило для компоненты `Itcsnatproxy.exe`.

8 В окне **Новое правило** на вкладке **Общие** в группе **Общая информация об этом правиле** укажите название разрешающего правила.

9 Перейдите на вкладку **Локальный** и в группе **Приложение** укажите путь к файлу `Itcsnatproxy.exe`. Например,

```
C:\Program Files (x86)\InfoTeCS\ViPNet Client\Itcsnatproxy.exe
```

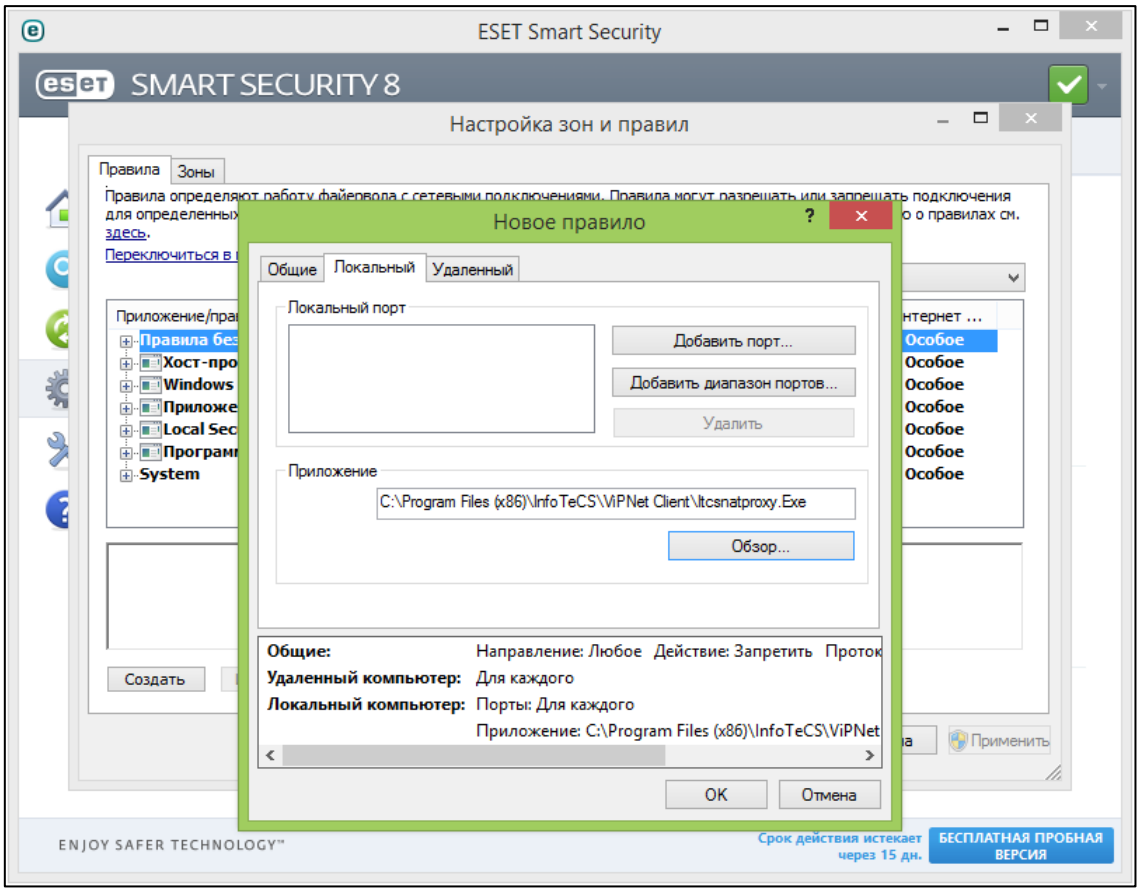


Рисунок 176. Создание правила в ESET NOD32 Smart Security для компоненты ltcsnatproxy.exe

10 Нажмите **OK**, чтобы сохранить правило.

11 В окне **Настройка зон и правил** нажмите **Применить**. Соединение между защищёнными узлами и доступ к ресурсам интернета будут восстановлены.

Avast

Если на сетевом узле ViPNet включён межсетевой экран Avast, могут возникнуть проблемы с соединением между сетевыми узлами ViPNet. Чтобы обеспечить совместное функционирование программ ViPNet Client и Avast, добавьте три правила для межсетевого экрана, разрешающие обмен данными по протоколу 241, а также прохождение входящего и исходящего UDP-трафика через порт 55777 (см. Протоколы соединений в защищённой сети). Для этого выполните следующие действия:

1 В главном окне программы выберите раздел **Защита** > **Брандмауэр** (**Настройки** > **Активная защита**) и рядом с пунктом **Брандмауэр** щёлкните ссылку **Настройки**.

2 В открывшемся окне выберите **Политики** и в группе **Предпочтения** установите флажок **Режим общего доступа к подключению интернета (ICS)**.

3 Нажмите **Правила работы с пакетами**, откроется окно **Правила для пакетов**.

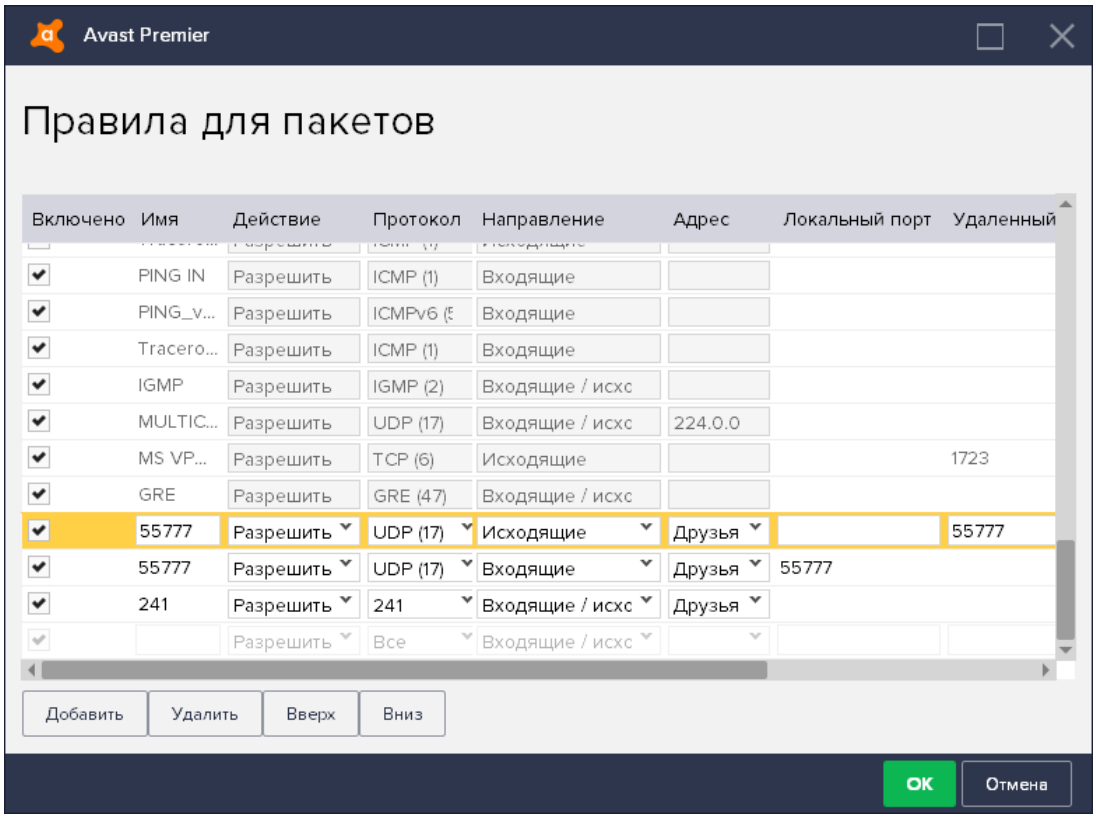


Рисунок 177. Создание правила в программе Avast

4 Нажмите **Добавить**, чтобы создать первое из трёх новых правил (например, правило для исходящего UDP-трафика), и настройте его в соответствии со значениями параметров, которые представлены в следующей таблице:

Таблица 18. Параметры правил для межсетевого экрана Avast

Правило	Действие	Протокол	Направление	Адрес	Локальный порт	Удалённый порт
Исходящий UDP-трафик	Разрешить	UDP	Исходящие	Друзья		55777
Входящий UDP-трафик	Разрешить	UDP	Входящие	Друзья	55777	
Протокол 241	Разрешить	241	Входящие/ исходящие	Друзья		

5 Создайте ещё два правила в соответствии со значениями из таблицы и нажмите **OK**.

6 Вернитесь в главное окно **Avast** и выберите раздел **Защита** > **Брандмауэр** (**Инструменты** > **Брандмауэр**).

7 В нижней части открывшегося окна щёлкните ссылку **Правила для приложений** и в открывшемся окне **Правила для приложений** прокрутите список приложений вниз, чтобы найти группу **«ИнфоТеКС»**.

8 Чтобы разрешить все соединения для программы ViPNet, выберите программу и в списке **Для всех остальных соединений** выберите **Определять автоматически**.

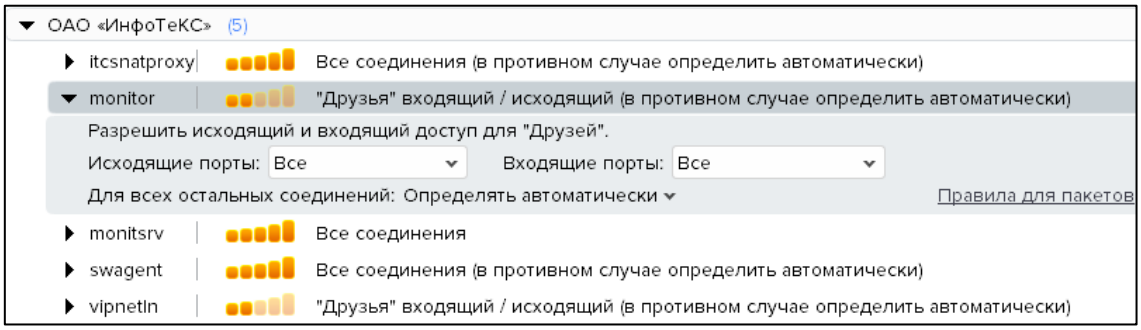


Рисунок 178. Настройка разрешения соединения с сетями в программе Avast

9 Повторите шаг 9 для каждой программы в группе **«ИнфоТеКС»** и затем нажмите **Закрыть**, чтобы завершить настройку межсетевого экрана Avast для совместной работы с ПО ViPNet.

Если на компьютере установлен антивирус Avast и возникают проблемы в работе электронной почты, воспользуйтесь рекомендациями из раздела Невозможно получить и отправить сообщения электронной почты.

AVG Internet Security

Если на сетевом узле ViPNet включён межсетевой экран AVG Internet Security, могут возникнуть проблемы с соединением между сетевыми узлами ViPNet. Чтобы обеспечить совместную работу программ ViPNet Client и AVG Internet Security, вы можете:

- отключить межсетевой экран AVG Internet Security;
- добавить три правила для межсетевого экрана AVG Internet Security, разрешающие обмен данными по протоколу 241, а также прохождение входящего и исходящего UDP-трафика через порт 55777 (см. Протоколы соединений в защищённой сети).

Чтобы добавить правила, выполните следующие действия:

1 В главном окне AVG Internet Security выберите **Меню** > **Настройки**.

2 В открывшемся окне выберите раздел **Компоненты** и рядом с пунктом **Усиленный брандмауэр** щёлкните ссылку **Настройка**.

3 В разделе **Политики** нажмите **Правила работы с пакетами**.

Примечание. Для создания правил в более ранней версии AVG Internet Security выполните следующие действия: В главном окне программы выберите **Firewall** >  , затем нажмите **Режим для опытных пользователей**. В разделе **Системные службы** нажмите **Управление системными правилами**.

4 Нажмите **Добавить**, чтобы создать первое из трёх новых правил (например, правило для входящего UDP-трафика), и настройте его в соответствии со значениями параметров, которые представлены в следующей таблице:

Таблица 19. Параметры правил для межсетевого экрана AVG Internet Security

Правило	Протокол	Направление	Локальный порт	Удаленный порт	Удаленный адрес	Действие
Входящий UDP-трафик	UDP	Входящее	55777	Все порты	Все сети	Разрешить
Исходящий UDP-трафик	UDP	Исходящее	Все порты	55777	Все сети	Разрешить
Протокол 241	241	В обоих направлениях			Все сети	Разрешить

5 Создайте ещё два правила в соответствии со значениями из таблицы и нажмите **OK**, чтобы завершить настройку межсетевого экрана AVG Internet Security.

Если на компьютере установлен антивирус AVG Internet Security и возникают проблемы в работе электронной почты, воспользуйтесь рекомендациями из раздела Невозможно получить и отправить сообщения электронной почты.

Secret Net

При совместной установке на компьютер ПО ViPNet Client и Secret Net возможны проблемы при обновлении справочников и ключей сетевого узла ViPNet. Это связано с тем, что в ПО Secret Net ограничен доступ пользователей к конфиденциальным данным, в том числе к папкам, в которых ПО ViPNet Client хранит справочники и ключи.

Чтобы справочники и ключи обновлялись при любом уровне доступа пользователей ПО Secret Net, у папок `C:\ProgramData\InfoTeCS, C:\ProgramData\InfoTeCS.Admin` и папки установки ViPNet Client (по умолчанию `C:\Program Files (x86)\InfoTeCS\ViPNet Client`) должна быть установлена категория управления доступом **Неконфиденциально**. Проверьте, какая категория управления доступом установлена:

1 Войдите под учётной записью, обладающей правами на управление категориями конфиденциальности, или назначьте эти права:

1.1 Выберите **Пуск** > **Код безопасности** > **Управление пользователями**.

1.2 Для пользователя выберите **Параметры безопасности** > **Доступ**.

1.3 Установите уровень допуска, отличный от **Неконфиденциально**.

1.4 Установите галочку **Управление категориями конфиденциальности.**

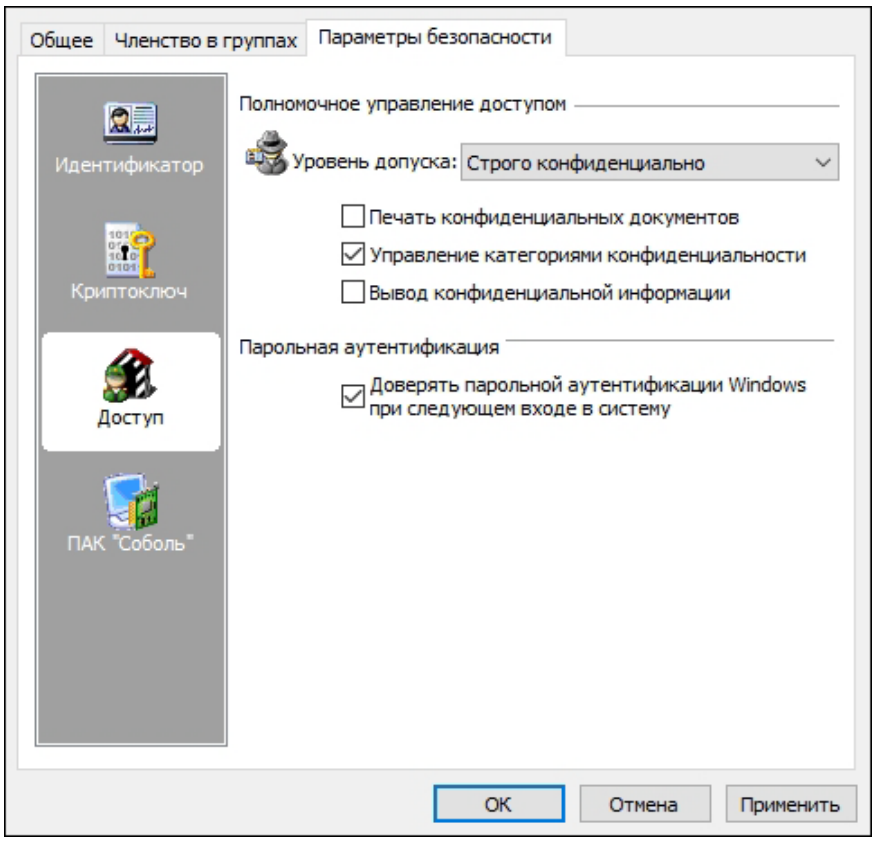


Рисунок 179. Параметры безопасности

2 Проверьте конфиденциальность папок `C:\ProgramData\InfoTeCS`, `C:\ProgramData\InfoTeCS.Admin` и папки установки ViPNet Client (по умолчанию `C:\Program Files (x86)\InfoTeCS\ViPNet Client`):

2.1 Щёлкните папку правой кнопкой мыши и в контекстном меню выберите **Свойства**.

2.2 Перейдите на вкладку **Secret Net Studio**.

2.3 Проверьте, чтобы в списке **Категория** было выбрано **Неконфиденциально**.

2.4 Нажмите **OK**.

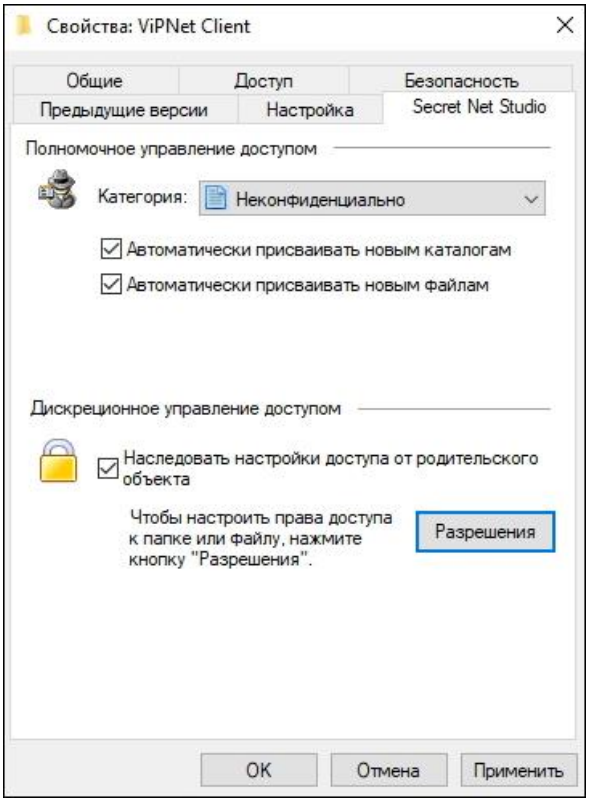


Рисунок 180. Настройка конфиденциальности папки

Совет. Для Secret Net версии 8 выполните рекомендации из документа «Secret Net Studio. Совместимость с другими программными средствами», раздел «ViPNet Client».

Cisco Agent Desktop

Если регламент работы контакт-центра требует прослушивания и записи разговоров операторов супервизором и для данных операций используются приложения Cisco Agent Desktop (на узлах операторов) и Cisco Supervisor Desktop (на узле супервизора), то на компьютерах операторов не следует устанавливать ПО ViPNet Client. Защиту трафика, передаваемого между узлами операторов и супервизора, в этом случае можно организовать с помощью туннелированных соединений.

При совместном использовании Cisco Agent Desktop и ViPNet Client передача голосового трафика на узел супервизора производится некорректно по следующим причинам. Голосовой трафик операторов зеркалируется драйвером Cisco Agent Desktop на узел супервизора, где прослушивается и записывается супервизором с помощью Cisco Supervisor Desktop. Если на узле оператора установлен ViPNet Client, то весь исходящий трафик передаётся в обработанном виде (IP-пакеты имеют преобразованный заголовок). Но зеркалируемый голосовой трафик не проходит обработку в ViPNet Client из-за того, что передаётся приложением Cisco Agent Desktop сразу на узел супервизора. При этом в необработанном виде голосовой трафик не может быть принят на его узле.

Данная проблема возникает из-за того, что Intermediate Ndis-драйвер приложения Cisco Agent Desktop, отвечающий за зеркалирование трафика на узел супервизора, и сетевой ViPNet-драйвер, осуществляющий обработку трафика, находятся на разных уровнях стека протокола TCP/IP. ViPNet-драйвер в стеке TCP/IP располагается на сетевом уровне. Драйвер Cisco встраивается в стек ниже — на канальном уровне — и зеркалирует голосовой трафик на узел супервизора напрямую, не передавая его ViPNet-драйверу. Поэтому IP-пакеты отправляются супервизору в необработанном виде.

Если на узлах операторов не будет установлено ПО ViPNet, то весь IP-трафик (в том числе голосовой) будет передаваться в открытом виде и сможет быть принят на узле супервизора при наличии соответствующих фильтров открытого трафика. Чтобы IP-трафик через внешние сети передавался в зашифрованном виде, между узлами операторов и супервизора следует организовать туннелируемые соединения.

Если функции прослушивания и записи разговоров операторов не осуществляются в контакт-центре, то тогда на узлах операторов вместе с приложением Cisco Agent Desktop можно установить ПО ViPNet Client.

H

История версий

В приложении описаны основные изменения в предыдущих версиях ViPNet Client.

Что нового в версии 4.5.5 hotfix 8

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

Что нового в версии 4.5.5 hotfix 7

- **Поддержка Windows 11 версии 23H2 (сборка 22631)**
- **Окончание поддержки операционных систем**
  - Windows 10, версия 20H2, сборка 19042;
  - Windows Server 2012;
  - Windows Server 2012 R2;

  Список совместимых ОС см. в разделе Системные требования.

Что нового в версии 4.5.5 hotfix 6

- **Исправление ошибок**

Что нового в версии 4.5.5 hotfix 5

- **Поддержка новых версий Windows**

  Реализована поддержка операционных систем:

  - Windows 10 (32/64-разрядная), версия 22H2, сборка 19045;
  - Windows 11, версия 22H2, сборка 22621.

- **Окончание поддержки Windows 8.1**

  Прекращена поддержка Windows 8.1 в связи с окончанием поддержки производителем. Список совместимых ОС см. в разделе Системные требования.

- **Поддержка новых внешних устройств**

  Реализована поддержка внешних устройств производства компании «Актив»:

  - Рутокен ЭЦП 3.0 3220;
  - Рутокен ЭЦП 3.0 NFC 3100, серт. ФСБ.

  Подробнее см. Список поддерживаемых внешних устройств.

Что нового в версии 4.5.5

- **Удалённое подключение к защищённой сети без переключения конфигураций**

  Теперь администратор может разрешить пользователям, которые работают в конфигурации с запретом открытых соединений, подключаться к защищённой сети через внешнего провайдера с авторизацией на Captive portal.

  Для этого в настройках программы ViPNet задаётся параметр **Разрешать открытые соединения при отсутствии связи с сервером соединений**. При этом внешняя сеть доступна только тогда, когда нет соединения с защищённой сетью. При подключении к защищённой сети доступ к открытой сети автоматически блокируется. А значит, работа в сети ViPNet безопасна и подключиться к сети ViPNet через интернет можно из конфигурации с запретом открытых соединений.

  Подробнее см. Параметры защиты трафика (на стр. 216).

  Также эту настройку можно выполнить централизованно из программы ViPNet Policy Manager (см. Разрешать открытые соединения при отсутствии связи с сервером соединений на стр. 204).

- **Управление размером MSS протокола TCP через ViPNet Policy Manager**

  Ранее уменьшить максимальный размер TCP-сегмента (MSS) можно было только в настройках программы ViPNet Client непосредственно на каждом сетевом узле. Теперь это значение можно указать сразу для многих пользователей ViPNet Client. Для этого администратор сети в программе ViPNet Policy Manager указывает нужное значение и отправляет политику безопасности на сетевые узлы ViPNet.

Подробнее см. Централизованное уменьшение MSS (на стр. 201).

- **Вход в Windows без входа в программу ViPNet Client**

  Теперь администратор может разрешить пользователям ViPNet с минимальными полномочиями не запускать программу ViPNet Client (см. Запуск программы на стр. 68), а войти сразу в Windows. Это полезно в особых ситуациях, например, если требуется разблокировать USB-устройство для аутентификации, когда несколько раз введён неправильный пароль. При этом использовать эту возможность для повседневной работы не рекомендуется, поскольку до входа в программу ViPNet компьютер не защищён.

  Подробнее см. Параметры запуска программы при загрузке Windows (на стр. 215).

  Также эту настройку можно выполнить централизованно из программы ViPNet Policy Manager (см. Централизованная настройка входа в программу на стр. 202).

- **Применение на сетевом узле политики с настройками конфигураций**

  Ранее создать конфигурацию (сборник фильтров и настроек ViPNet Client) можно было только непосредственно на сетевом узле. Теперь ViPNet Client может принять из управляющего приложения ViPNet ЦУС политику (в формате `lzh`), в которой записаны настройки разных конфигураций. Это позволит администратору быстро применить нужные наборы сетевых фильтров на большом числе сетевых узлов, не настраивая каждый узел отдельно.

  Для формирования политики с различными конфигурациями обратитесь к представителям «ИнфоТеКС» (см. Обратная связь на стр. 27). Формирование такой политики в ViPNet Policy Manager не поддерживается.

- **Поддержка новых версий Windows**

  Реализована поддержка операционных систем:

  - Windows Server 2019, сборка 17763,
  - Windows Server 2022, сборка 20348,
  - Windows 10 (32/64-разрядная), версия 21H2, сборка 19044,
  - Windows 11, версия 21H2, сборка 22000.

Что нового в версии 4.5.3

В этом разделе представлен краткий обзор изменений в ViPNet Client версии 4.5.3 по сравнению с 4.5.2.

- **Переключение конфигураций программы с помощью ярлыка на рабочем столе**

  Теперь вы можете создать ярлык для любой конфигурации и переключать конфигурацию с рабочего стола. Подробнее см. раздел Управление конфигурациями программы (на стр. 196).

- **Переключение между публичными и корпоративными DNS-серверами из ЦУСа**

  Теперь администратор сети может удалённо переключать DNS-зоны (публичные или корпоративные), которые будет использовать ваш сетевой узел. Подробнее см. раздел Создание списка DNS (WINS) серверов вручную (на стр. 118).

- **Окончание поддержки Windows 7/8/Server 2008 R2**

  Прекращена поддержка Windows 7, Windows 8, Windows Server 2008 R2 в связи с окончанием их поддержки производителем. Список совместимых ОС см. в разделе Системные требования (на стр. 22).

- **Графический интерфейс транспортного модуля MFTP**

  Теперь работать с журналом, очередью и статистикой конвертов можно через программу «ViPNet Транспортный модуль».

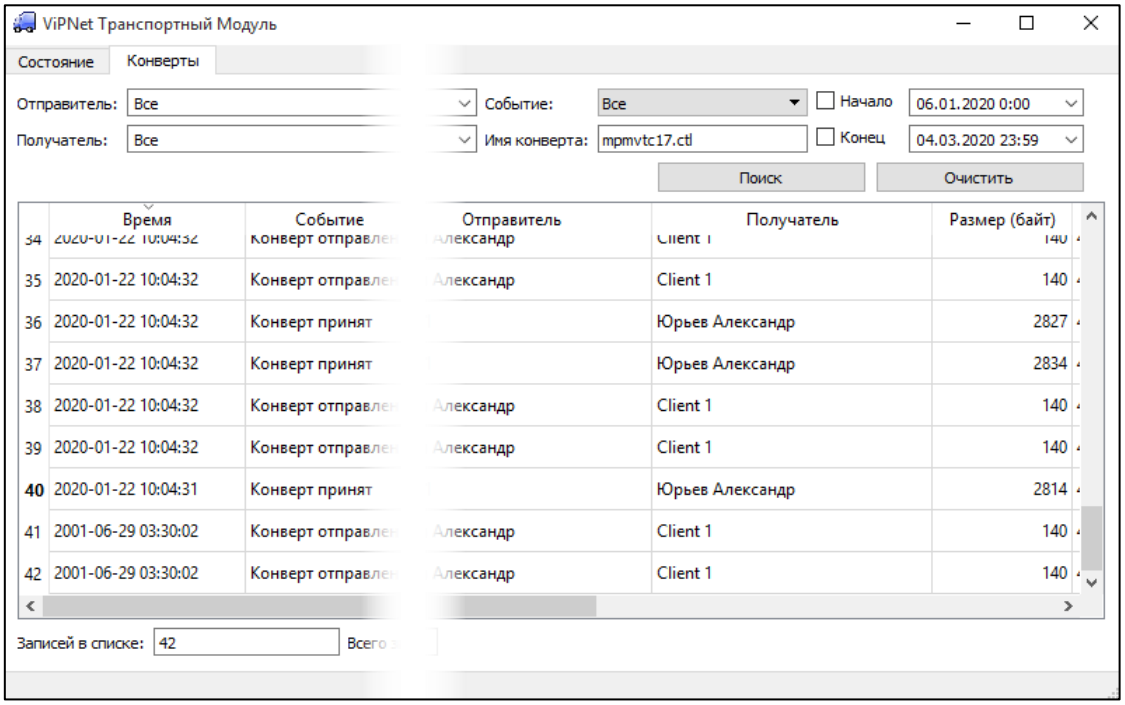


Рисунок 181. Просмотр журнала конвертов

Подробнее см. документ «ViPNet MFTP 4. Руководство администратора», разделы «Просмотр журнала конвертов» и «Просмотр очереди конвертов».

Что нового в версии 4.5.2

В этом разделе представлен краткий обзор изменений в версии 4.5.2 по сравнению с 4.5.1.

- **Автоматическая синхронизация времени на вашем компьютере с временем в сети ViPNet**

  Если время на вашем компьютере отличается от времени в сети ViPNet, то работа в защищённой сети невозможна. Чтобы не отслеживать время самостоятельно, вы можете в настройках программы ViPNet установить автоматическую синхронизацию времени на вашем компьютере с временем в сети ViPNet. Подробнее см. раздел Настройка подключения к защищённой сети (на стр. 94).

- **Работа программы ViPNet Деловая почта без программы ViPNet Client**

Теперь вы можете установить программу ViPNet Деловая почта отдельно от программы ViPNet Client. Эта возможность была временно недоступна в версии 4.5.1.

- **Частичная работа программы при истечении срока действия лицензии**

  При истечении срока действия лицензии на программу ViPNet вы можете получить обновлённую лицензию из центра управления сетью по защищённой сети ViPNet. Подробнее см. раздел Лицензирование программы ViPNet Client (на стр. 48).

- **Поддержка Windows 10 версии 1903**

- **Изменение состава семейств внешних устройств**

  В новой версии программы ViPNet Client изменился состав следующих семейств устройств:

  - К семейству JaCarta отнесены устройства типов eToken GOST, JaCarta GOST и JCDS.
  - К семейству Rutoken отнесены устройства типов Rutoken ECP и Rutoken Lite.
  - К семейству Rutoken S отнесены устройства типов Rutoken и Rutoken S.

  Подробнее см. раздел Список поддерживаемых внешних устройств (на стр. 344).

- **Поддержка внешних устройств JaCarta-2 ГОСТ**

  Для аутентификации в программе ViPNet Client вы можете использовать внешние устройства JaCarta-2 с апплетом ГОСТ версии 2.5.5 и выше. Подробнее см. раздел Особенности аутентификации с помощью сертификата (на стр. 72).

Что нового в версии 4.5.1

В этом разделе представлен краткий обзор изменений в версии 4.5.1 по сравнению с 4.5.0.

- **Проверка сертификата средствами ОС Windows**

  Проверка действительности сертификата для аутентификации (см. Особенности аутентификации с помощью сертификата на стр. 72) теперь выполняется средствами ОС Windows, что соответствует принятой международной практике. При этом процесс аутентификации с помощью сертификата не изменился.

- **Защита дистрибутива ключей с помощью сертификата**

  Для безопасной передачи дистрибутива ключей и справочников по открытым каналам связи администратор сети ViPNet может зашифровать его на вашем сертификате. Установка зашифрованного дистрибутива (файл *.enc) выполняется так же, как и незашифрованного (файл *.dst). Подробнее см. в документе «Работа с защищёнными DST. Быстрый старт».

- **Изменения в настройках обработки трафика**

  При необходимости в режиме администратора теперь можно отключить инспекцию пакетов с хранением состояния.

- **Поддержка Windows 10 версии 1809 (сборка 17763.55)**

- **Отказ от поддержки канала SMTP/POP3 в транспортном модуле MFTP**

Канал SMTP/POP3 предполагает передачу конвертов через почтовые серверы и имеет низкую эффективность по сравнению с каналом MFTP. Канал SMTP/POP3 разрабатывался для сетей, где было невозможно использование других протоколов на базе TCP. Подробнее об использовании этого канала в прежних версиях программы см. «ViPNet MFTP. Руководство администратора» версии 4.5.0 и ниже, раздел «Передача конвертов через почтовые серверы».

Если канал SMTP/POP3 был указан в настройках модуля MFTP или в файле конфигурации mftpconf.xml, то при обновлении программы он автоматически заменится на MFTP (см. «ViPNet MFTP. Руководство администратора», раздел «Управление каналами передачи конвертов»).

Если после обновления ПО ViPNet Client наблюдаются перебои в работе защищённой сети на некоторых узлах, проверьте настройки модуля MFTP на этих узлах и вместо канала SMTP/POP3 укажите канал MFTP. Подробнее см. После обновления программы наблюдаются перебои в работе защищённой сети (на стр. 273).

- **Выявлена несовместимость одновременной работы ViPNet Client с HP Velocity**

  При совместной установке или использовании ViPNet Client и HP Velocity возникают проблемы, приводящие к неработоспособности ПО. Для обеспечения корректной работы ViPNet Client перед его установкой на ПК следует удалить HP Velocity.

  HP Velocity — это устаревшая служебная программа для повышения скорости соединения в ненадёжных сетях. HP Velocity не содержит полезных функций для работы в современных сетях и не поддерживается производителем Hewlett-Packard.

- **ViPNet Деловая почта работает только совместно с программой ViPNet Client**

  Новая версия программы поддерживает работу ПО ViPNet Деловая почта только на защищённом сетевом узле. Функцию защиты сетевого трафика выполняет программа ViPNet Client. Поэтому если у вас установлена ViPNet Деловая почта без ViPNet Client, вы не сможете установить новую версию ViPNet Client. Рекомендуем пользоваться текущей версией программы до выхода новой совместимой версии ViPNet Client. Если обновление требуется немедленно, обратитесь в службу поддержки ИнфоТеКС.

Что нового в версии 4.5.0

В этом разделе представлен краткий обзор изменений в версии 4.5.0 по сравнению с 4.3.4.

- **Реализована новая архитектура ПО ViPNet Client**

  В составе программы ViPNet Client появился новый компонент — ViPNet Сервис управления драйвером защиты (см. Сервис управления драйвером защиты ViPNet на стр. 16), функционирующий как служба Windows.

  Сервис управления выполняет часть функций, которые в предыдущих версиях выполняла программа ViPNet Client, а именно:

  - загрузку в ViPNet-драйвер справочной информации о структуре сети, правил фильтрации и ключей шифрования;

- приём и передачу на другие сетевые узлы информации о состоянии узла и параметрах доступа;
- ведение журнала IP-пакетов (см. Работа с журналом IP-пакетов на стр. 184) и журнала событий (см. Просмотр журнала событий на стр. 221).

Теперь для полноценной работы ПО ViPNet вам не требуется постоянно запущенной программы ViPNet Client. Достаточно выполнить вход в программу ViPNet Client, после чего её можно закрыть. ViPNet Client потребуется запустить вновь для приёма обновлений ViPNet или изменения настроек.

Реализация новой архитектуры позволила повысить безопасность и надёжность программного обеспечения ViPNet.

- **Переработан транспортный модуль ViPNet MFTP**

  Программа ViPNet MFTP была заменена кроссплатформенной службой Транспортный модуль ViPNet MFTP (на стр. 16). Служба имеет оптимальные параметры по умолчанию и, как правило, не нуждается в настройке. Указать нестандартные параметры транспортного модуля вы можете с помощью конфигурационного файла.

- **Разработан новый установщик программ ViPNet**

  Новый установщик позволяет объединить в один файл любое количество программ ViPNet и установить их за один раз. Кроме того, установкой и составом программы ViPNet CSP теперь можно управлять из единого установщика. В предыдущих версиях программы установка ПО ViPNet CSP выполнялась автоматически, без возможности пользовательской настройки.

- **Автоматическое восстановление программы**

  В случае аварийного завершения работы программы перезапуск программы или служб ОС выполняется автоматически. Из интерфейса удалены настройки программы **Перезапускать Client при аварийном завершении** и **Использовать функцию watchdog**.

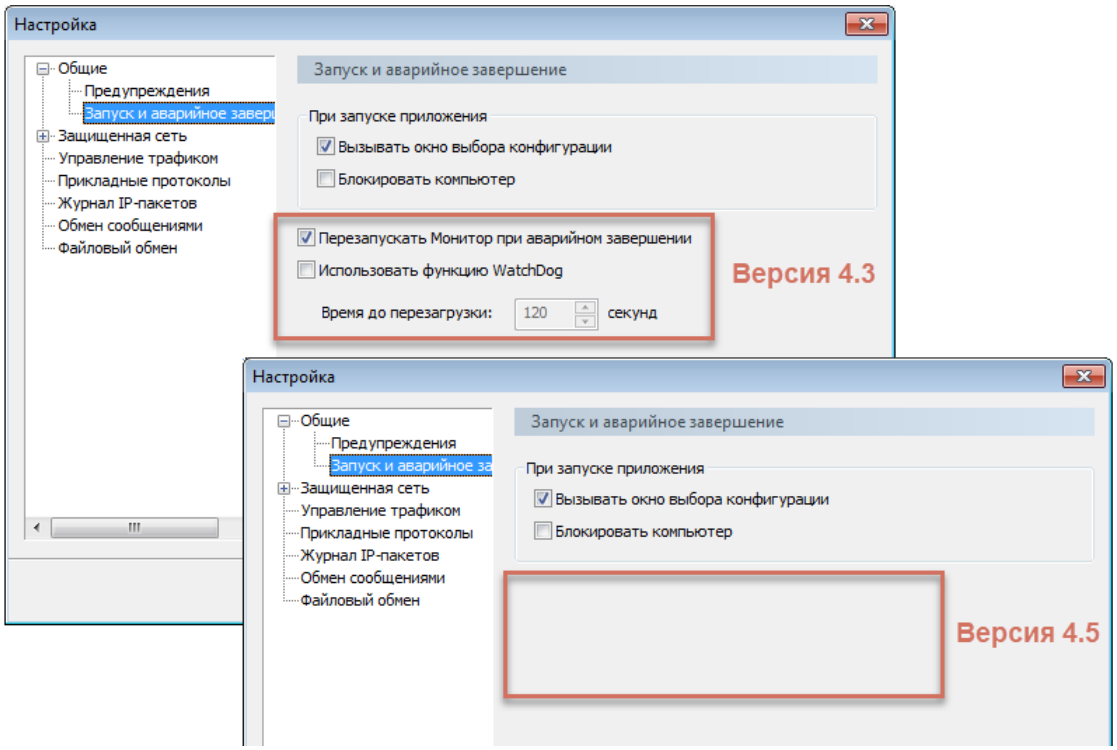


Рисунок 182. Удаление настроек аварийного завершения программы

- **Изменился внешний вид значка программы**

Теперь на рабочем столе и в области уведомлений значок вызова программы ViPNet Client имеет вид:  .

- **Добавлен модуль расширенной фильтрации**

  В состав новой версии программы добавлен модуль расширенной фильтрации (на стр. 17), который позволяет:

  - Создавать фильтры прикладного уровня (на стр. 148).
  - Реализовать взаимодействие с антивирусом (на стр. 218).

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

  Начиная с версии 4.5.0, программа ViPNet Client не поддерживает совместную работу с ViPNet SafeDisk-V (см. Обновление при использовании программы SafeDisk-V на стр. 45).

Что нового в версии 4.3.4

В этом разделе представлен краткий обзор изменений в версии 4.3.4 по сравнению с 4.3.3.

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

Что нового в версии 4.3.3

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.3 по сравнению с версией 4.3.2.

- **Поддержка Windows Server 2016**

  Начиная с версии 4.3.3, программа ViPNet Client поддерживает операционную систему Windows Server 2016.

- **Совместимость с Secure Boot в ОС Windows 10**

  В версии 4.3.3 устранены конфликты совместной работы с функцией Secure Boot в системе Windows 10. Теперь её отключение не требуется.

- **Возможность установки адресов видимости туннелируемых узлов по умолчанию**

  В версии 4.3.3 появилась возможность автоматической установки адресов видимости туннелей для новых координаторов. А также групповое изменение адресов видимости туннелей для уже существующих координаторов.

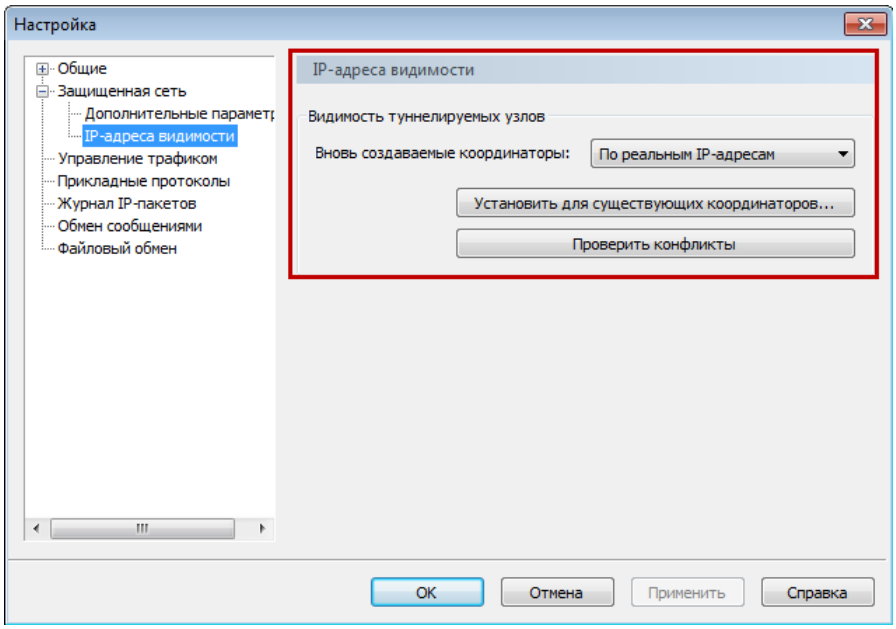


Рисунок 183. Установка адресов видимости туннелируемых узлов

- **Новые возможности журнала событий**

  Администратор узла ViPNet при просмотре журнала событий может применить фильтр для отображения:

  - событий, зарегистрированных в заданный интервал времени;
  - событий, связанных с выбранным пользователем;
  - только одного вида событий.

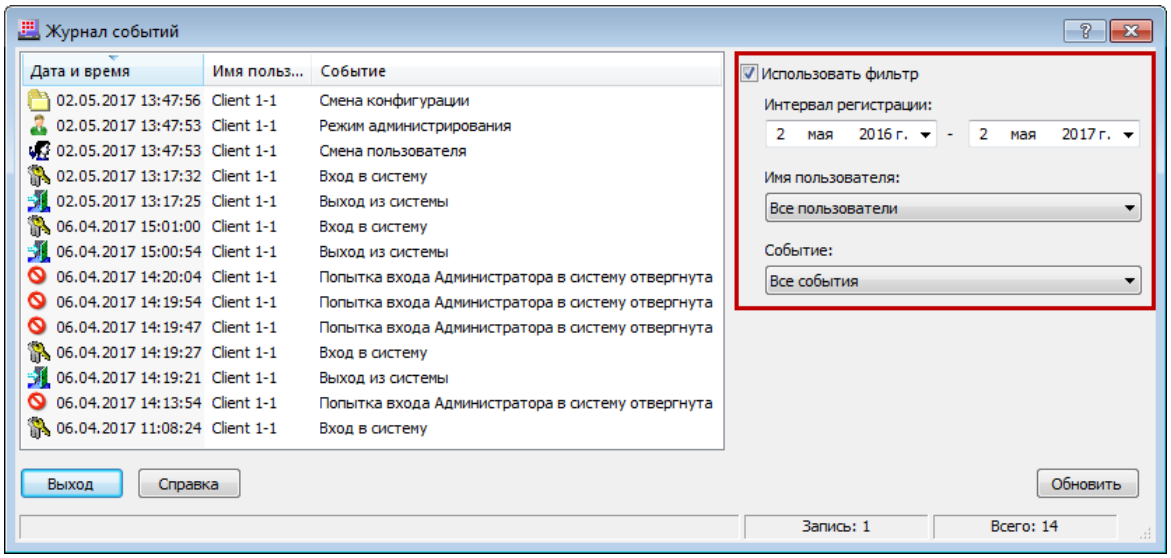


Рисунок 184. Возможность применения фильтров при просмотре журнала событий

- **Дополнена документация ViPNet Client**

  В руководство добавлен сценарий аварийного удаления программы из безопасного режима ОС Windows.

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

  Начиная с версии 4.3.3, при специальном уровне полномочий 3 (подробно о полномочиях см. документ «Классификация полномочий. Приложение к документации ViPNet») пользователю предоставляется доступ в интернет.

Что нового в версии 4.3.2

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.2 по сравнению с версией 4.3.1.

- **Изменён порядок обновления ПО ViPNet Client в защищённой сети**

  Перед тем, как обновить ПО ViPNet Client до версии 4.3.2 на сетевых узлах защищённой сети, обновите ПО ViPNet Client (см. Обновление ViPNet Client на стр. 42) на сетевом узле с программой ViPNet Центр управления сетью.

- **Изменён список поддерживаемых операционных систем**

  Начиная с версии 4.3.2, прекращена поддержка ОС Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008 в связи с прекращением их поддержки производителем и наличием уязвимостей в этих ОС.

- **Изменение требований к сертификатам, используемым при аутентификации**

  - Раньше для выполнения аутентификации с помощью сертификата необходимым условием являлось наличие назначения «Проверка подлинности клиента» в расширении сертификата Расширенное использование ключа. Теперь для аутентификации вы можете использовать сертификат с назначением «Шифрование ключей» в расширении

Использование ключа (см. Особенности аутентификации с помощью сертификата на стр. 72).

- **Режим «Публичный DNS»**

  Теперь при работе с защищёнными DNS-серверами вы можете использовать режим «Публичный DNS» (см. Использование публичного DNS-сервера на стр. 123), который позволяет переключаться на внешний DNS-сервер интернет-провайдера в случае нестабильной связи с защищённым DNS-сервером корпоративной сети.

- **Принудительное соединение с координатором по TCP-туннелю**

  В версии 4.3.2 вы можете настроить постоянное подключение к серверу IP-адресов по TCP-туннелю, установив соответствующий флажок в настройках (см. Настройка подключения к защищённой сети на стр. 94). В предыдущих версиях соединение по TCP-туннелю устанавливалось автоматически и только при нестабильной связи по протоколу UDP.

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

Что нового в версии 4.3.1

В этом разделе представлен краткий обзор изменений и новых возможностей версии 4.3.1 по сравнению с версией 4.3.0.

- **Поддержка Windows 10**

  Начиная с версии 4.3.1, ПО ViPNet Coordinator поддерживает операционную систему Windows 10.

- **Отключение поддержки TLS/SSL в программе ViPNet CSP по умолчанию**

  Теперь при установке программы ViPNet CSP в составе ПО ViPNet Client поддержка протокола TLS/SSL отключена. Вы можете включить поддержку, запустив установочный файл программы ViPNet CSP и добавив соответствующий компонент.

- **Исправление ошибок**

  Исправлены ошибки, обнаруженные при эксплуатации предыдущих версий программы.

Что нового в версии 4.3.0

- **Восстановление предустановленных фильтров и групп объектов**

  В версии 4.3 появилась возможность восстановить предустановленные сетевые фильтры. Это позволяет отказаться от произведённых изменений в настраиваемых фильтрах и вернуться к исходному состоянию. Вместе с фильтрами также будут восстановлены предустановленные группы объектов.

- **Поддержка централизованного управления алгоритмом шифрования и сохранением пароля в реестре**

  На сетевых узлах версии 4.3 автоматически изменяются алгоритм шифрования и разрешение на сохранение пароля в реестре в соответствии со значениями, которые передаёт администратор сети ViPNet в составе обновления справочников и ключей. Централизованное управление этими параметрами возможно в ПО ViPNet Administrator версии 4.4.1 и выше. Пользователь или администратор сетевого узла по-прежнему может изменить указанные параметры, однако изменение будет действительно до следующего обновления справочников и ключей.

- **Поддержка централизованного управления состоянием сетевого экрана Windows**

  На клиентах версии 4.3 автоматически устанавливается состояние сетевого экрана Windows, заданное администратором сети ViPNet в программе ViPNet Центр управления сетью версии 4.4.1 и выше. Если для управления сетью используется более ранняя версия ViPNet Administrator, то при первом запуске программы ViPNet Client сетевой экран Windows автоматически отключается.

- **Дополнительные параметры установки с помощью групповых политик**

  Появилась возможность задать дополнительные параметры при установке ПО ViPNet Client с помощью групповых политик. Теперь, используя готовые файлы настроек в формате MST, вы можете выбрать, нужно ли устанавливать программу ViPNet Деловая почта и дополнительные компоненты ViPNet CSP.

Термины и сокращения

PKI (Public Key Infrastructure)

Инфраструктура открытых ключей — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам (в том числе ключам проверки электронной подписи) в распределённых системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг интернета.

TCP-туннель настраивается на координаторе, который является для клиента сервером соединений.

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

Аутентификация

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

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-адреса узла. Виртуальные IP-адреса узлу ViPNet (Б) назначаются непосредственно на узле А. На других узлах узлу ViPNet (Б) могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если сетевые узлы ViPNet работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удалённых узлов в приложениях ViPNet.

Внешние IP-адреса

Адреса внешней сети.

Внешняя сеть

Сеть, отделённая от внутренней сети межсетевым экраном.

Дистрибутив ключей

Файл с расширением *.dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Запрос на сертификат

Защищённое электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи 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).

Защищённое соединение

Соединение между узлами, зашифрованное с помощью программного обеспечения ViPNet.

Защищённые прикладные серверы

Прикладные серверы (веб-сервер, почтовый сервер, FTP-сервер и так далее), размещённые на защищённых узлах.

Защищённый DNS или WINS сервер

Сервер DNS или WINS, размещённый на защищённом узле.

Защищённый интернет-шлюз (открытый интернет)

Технология, реализованная в программном обеспечении ViPNet. При подключении к интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

Защищённый узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключ проверки электронной подписи (ключ проверки ЭП)

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является несекретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи (ключ ЭП)

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключи пользователя ViPNet

Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

Координатор (ViPNet-координатор)

Сетевой узел ViPNet, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В сети ViPNet-координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

Корневой сертификат

Сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

Лицензия на сеть

Разрешение на пользование определённым набором функций продуктовой линейки ViPNet. В частности, лицензия на сеть ViPNet определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешённую версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

Обновление справочников и ключей

Файлы, формируемые администратором сети ViPNet в управляющем приложении (ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр) при изменении справочников и ключей для сетевых узлов ViPNet, то есть, в случае добавления, удаления сетевого узла ViPNet, добавления пользователя, издания нового сертификата и так далее. Администратор сети ViPNet централизованно высылает на сетевой узел сформированные новые ключи и справочники из ЦУСа.

Открытый сервер DNS или WINS

Сервер DNS или WINS на открытом узле.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

Папка ключей сетевого узла

Папка, в которой находятся ключи сетевого узла ViPNet и справочники.

Пароль администратора сетевого узла ViPNet

Пароль для входа на сетевом узле ViPNet в режим администратора, в рамках которого становятся доступны дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр.

Пароль пользователя на основе парольной фразы

Пароль пользователя необходим для входа в любую программу ViPNet. Случайный пароль создаётся на основе парольной фразы, которую можно использовать для запоминания пароля. Парольные фразы могут быть созданы на нескольких языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объёму словаря. 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 раскладке латиницей первые X букв из каждого слова парольной фразы, содержащей Y слов. Пользователь сам задаёт параметры X и Y, а также язык парольной фразы.

Например, при использовании трёх первых букв из каждого слова парольной фразы «Затейливый ювелир утащил сдобу» получим пароль «pfn.dtenfclj».

Политики безопасности

Набор параметров — сетевых фильтров и правил трансляции сетевых адресов, регулирующих безопасность сетевого узла.

Полномочия пользователя

Разрешения на определённые действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задаёт полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ создаёт для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удалённого обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищённых узлов.

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищённых узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Структура сети ViPNet

Упорядоченная совокупность связей между компонентами сети ViPNet, такими как:

- рабочее место администратора сети ViPNet;
- координаторы;
- клиенты.

Каждый клиент должен быть зарегистрирован на координаторе. Связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через интернет или другие публичные сети, путём инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей.

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

Файл контейнера

Специальный файл, в котором хранится защищённая информация. Этот файл подключается в качестве нового логического диска в вашей операционной системе. Вы можете работать с этим диском, как с обычным диском Windows: перетаскивать, копировать, вставлять, удалять файлы и так далее.

Файл контейнера имеет расширение `*.sdc` и по умолчанию является скрытым. Чтобы увидеть этот файл, на **Панели управления** откройте **Свойства папки**, на вкладке **Вид** включите опцию **Показывать скрытые файлы и папки**.

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в неё сертификаты также действительны.

Частный адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в интернете. Чтобы выйти в интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

Электронная подпись (ЭП)

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.