

A low-angle, upward-looking photograph of a modern skyscraper with a glass facade. The building's structure is composed of a grid of dark metal frames and large glass panels. The sky is visible through the glass, appearing as a bright, overcast blue. The perspective creates a sense of height and architectural scale.

ViPNet Client 4U for Linux

Руководство пользователя

© АО «ИнфоТеКС», 2022

ФРКЕ.00239-01 34 01

Версия продукта 4.13

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения АО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

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.....	5
О документе.....	5
Соглашения документа.....	5
О программе	7
Системные требования.....	7
Требования к корпоративной сети	9
Список поддерживаемых внешних устройств	9
Что нового в версии 4.13	9
Комплект поставки	10
Обратная связь.....	11
 Общие сведения	12
Для чего нужно устанавливать ключи.....	12
Способы аутентификации в ViPNet Client 4U.....	12
 Работа в командной строке.....	14
Установка ключей	14
Обновление ключей.....	16
Удаление ключей	17
Запуск и завершение работы.....	17
Проверка связи с координатором	18
Смена способа аутентификации.....	19
Просмотр списка защищенных узлов.....	20
Просмотр информации о своем узле и версии ViPNet Client 4U	22
Обращение в службу технической поддержки	23
 Работа в графическом интерфейсе	24
Установка ключей	24
Обновление ключей.....	27
Удаление ключей	27
Запуск и завершение работы.....	28
Проверка связи с координатором	29
Смена способа аутентификации.....	29
Просмотр списка защищенных узлов.....	30
Просмотр информации о своем узле и версии ViPNet Client 4U	31

Контроль целостности и работоспособности.....	32
Обращение в службу технической поддержки	33
История версий.....	34
Что нового в версии 4.12.....	34
Что нового в версии 4.11.....	34
Что нового в версии 4.10.....	34
Что нового в версии 4.9	34
Что нового в версии 4.8	35
Глоссарий.....	38

Введение

О документе

В данном документе содержится информация о назначении и установке программы ViPNet Client 4U for Linux (далее — ViPNet Client 4U), а также приведены рекомендации по работе с ней.

Документ предназначен для пользователей сети ViPNet, которые работают с ViPNet Client 4U на компьютерах с операционной системой GNU/Linux (далее — ОС Linux).

Соглашения документа

Обозначение	Описание
	Внимание! Содержит критически важную информацию
	Примечание. Содержит рекомендательную информацию
	Совет. Содержит полезные приемы и хорошие практики
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская ее, 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.

Обозначения при описании команд в документе:

- Команды, которые могут быть выполнены пользователем Linux, содержат приглашение:
`user@host:~$ команда`
- Команды, которые могут быть выполнены администратором Linux, содержат приглашение:
`root@host:~# команда`
- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки:
`команда <параметр>`

- Необязательные параметры или ключевые слова заключены в квадратные скобки:
команда <обязательный параметр> [необязательный параметр]
- Допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:
команда {вариант-1 | вариант-2}

О программе

Программа ViPNet Client 4U защищает IP-трафик на компьютерах с ОС Linux путем шифрования IP-пакетов.

С помощью ViPNet Client 4U пользователи могут подключаться к сетевым узлам ViPNet или [туннелируемым узлам](#) (см. глоссарий, стр. 39) по защищенному каналу через координатор ViPNet и получать доступ к размещенным на этих узлах ресурсам: корпоративным веб-порталам, электронной почте, системе IP-телефонии и другим корпоративным сервисам. Доступ к открытым ресурсам интернета осуществляется напрямую. В отличие от соединения с защищенными узлами сети ViPNet, соединение с открытыми узлами не зашифровано и не контролируется координатором.

Также пользователи ViPNet Client 4U могут установить программы ViPNet Connect (голосовые и видеозвонки, обмен сообщениями) и ViPNet Деловая почта (обмен письмами), чтобы общаться с пользователями сети ViPNet по защищенному каналу.

ViPNet Client 4U поставляется в одном из двух вариантов:

- Консольная версия — доступна работа с ViPNet Client 4U только в командной строке.
- Графическая версия — доступна работа с ViPNet Client 4U и в командной строке, и в графическом интерфейсе.

Установка, обновление и удаление ViPNet Client 4U на компьютер выполняются администратором сети ViPNet, так как для этого требуются права суперпользователя ОС (root). Подробнее см. в документе «ViPNet Client 4U for Linux. Руководство администратора», глава «Установка, обновление и удаление ViPNet Client 4U».

Системные требования

Требования к компьютеру для установки ViPNet Client 4U:

- Процессор — Intel Core Duo или другой схожий по производительности 64-разрядный процессор.
- Объем оперативной памяти — не менее 1 Гбайт.
- Свободное место на жестком диске — не менее 500 Мбайт (рекомендуется 1 Гбайт).
- Операционная система одного из следующих дистрибутивов:

Таблица 1. Поддерживаемые операционные системы

Архитектура процессора	Дистрибутив Linux
x86-64	• Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6). • Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).

Архитектура процессора	Дистрибутив Linux
	• Astra Linux Common Edition (очередное обновление 2.12). • ГосЛинукс IC5. • ГосЛинукс IC6. • РЕД ОС 7.3. • Альт Рабочая станция 8 СП. • Альт Рабочая станция 9. • Альт Рабочая станция 10. • ЛОТОС. • РОСА «КОБАЛЬТ» 7.3 (пользовательская редакция). • AlterOS 7.5. • EMIAS OS 1.0. • Ubuntu 18.04. • Ubuntu 20.04. • Debian 9. • Debian 10. • Debian 11. • CentOS 8.
«Эльбрус»	• Astra Linux Special Edition РУСБ.10265-01 (очередное обновление 8.1).
ARMv5	• OpenWrt Chaos Calmer Build for RTU968V2 v.2.6.4E.
ARMv7	• Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7). • Сборка для микроконтроллера SM160 на основе ОС Debian. • Сборка для микроконтроллера Topaz MX240 на основе ОС OpenEmbedded. • Сборка для микроконтроллера Topaz MX681 на основе ОС OpenEmbedded. • Raspberry PI OS.
ARMv8	• Байкал-М (Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7). • Nvidia Jetson tx2. • Ubuntu 18.04 LTS. • Ubuntu 20.04 LTS. • Debian 11.



Примечание. Также возможна работа ViPNet Client 4U на менее производительных устройствах. При необходимости гарантированной поддержки менее производительного устройства [обратитесь в ИнфоТеКС](#) (на стр. 11).

На устройствах со слабыми процессорами работа с ViPNet Client 4U может быть замедлена.

Требования к корпоративной сети

Для использования ViPNet Client 4U требуется лицензия на ПО и сеть ViPNet под управлением:

- [ViPNet Administrator](#) (см. глоссарий, стр. 38) версии 4.6.4 и выше.
- ViPNet Prime версии 1.4.1 и выше.

Список поддерживаемых внешних устройств

Производитель	Устройство
«Аладдин Р.Д.»	Jacarta PKI/GOST (JC205-1 v3.0)
	JaCarta-2 ГОСТ(JC206-2.F27 v4.0)
	JaCarta ГОСТ(JC201 v3.0)
	JaCarta-2 PKI/ГОСТ (JC007-12.F27 v4.0)
	JaCarta PKI/Flash (JC212-1.Q09)
	JaCarta SF/ГОСТ (JC226-J.F27J06J08)
	JaCarta ГОСТ(JC001-2 v3.0)
	JaCarta-2 PKI/ГОСТ (JC207-12.F27 v4.0)
	JaCarta PKI (JC200 v3.0)
«Актив»	JaCarta ГОСТ(JC101-2 v2.0)
	Рутокен ЭЦП 2.0 (2000, 2100, 3000)
	Рутокен PKI (1800)
	Рутокен Lite (1000)
	Рутокен ЭЦП

Что нового в версии 4.13

- **Сетевой экран ViPNet Client 4U**

В новой версии ViPNet Client 4U вы можете фильтровать IP-трафик:

- Фильтровать защищенный IP-трафик с помощью сетевых фильтров из программы ViPNet Policy Manager и модуля ViPNet Prime Policy Management или сетевых фильтров, настроенных вручную в файле *.xml.
- Запретить открытый IP-трафик на компьютере при включенном VPN-соединении. При этом вы сможете работать только с защищенными узлами ViPNet и туннелируемыми

ресурсами, а также с открытым трафиком, необходимым для работы ОС и ViPNet Client 4U (трафик интерфейсов loopback, TUN, серверов DHCP, NTP).

Параметры работы сетевого экрана настраиваются администратором ViPNet Client 4U. При настройке требуется вводить пароль администратора сетевого узла.

- **Адрес доверенного DNS-сервера**

Раньше адрес доверенного DNS-сервера для открытой сети был 8.8.8.8, теперь используются адреса 77.88.8.88, 77.88.8.2.

- **Поддержка программы ViPNet Деловая почта**

Теперь вы можете установить на компьютер с ViPNet Client 4U программу ViPNet Деловая почта, чтобы обмениваться письмами с пользователями сети ViPNet по защищенному каналу.

- **Поддержка смены адресации узлов в сети ViPNet**

Раньше в сети ViPNet использовались адреса узлов из диапазона 7.ID.ID.7, теперь используются адреса из диапазона 7.X.ID.ID. Со стороны ViPNet Client 4U поддерживается новая адресация узлов ViPNet. В качестве адреса вашего узла также используется адрес из диапазона 7.X.ID.ID.

После обновления ViPNet Client 4U до версии 4.13 перезапустите на компьютере все сервисы, которые использовали сеть ViPNet и виртуальный сетевой интерфейс TUN. Также измените адрес сетевого интерфейса TUN во всех конфигурационных файлах сервисов, где он указан.

- **Сертификат электронной подписи ИнфоТеКС в составе DEB-пакета**

Теперь сертификат электронной подписи ИнфоТеКС входит в подписанный DEB-пакет ViPNet Client 4U и устанавливается в ОС Astra Linux Special Edition автоматически вместе с ViPNet Client 4U.

Комплект поставки

- Пакеты установки в форматах DEB, RPM и IPK.
- Документы в формате PDF:
 - «ViPNet Client 4U for Linux. Руководство администратора».
 - «ViPNet Client 4U for Linux. Руководство пользователя».
 - «ViPNet Client 4U for Linux. Соответствие пакетов установки поддерживаемым платформам».
 - «ViPNet Client 4U for Linux. Установка на промышленные контроллеры».
 - «ViPNet Client 4U for Linux. Установка на контроллер Wago».
 - «ViPNet Client 4U for Linux. Лицензионные соглашения на компоненты сторонних производителей».

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](#).

Общие сведения

Для чего нужно устанавливать ключи

Перед использованием ViPNet Client 4U установите на компьютер ключи ViPNet. С помощью этих ключей шифруется IP-трафик при соединениях с другими узлами защищенной сети. Без этого работа ViPNet Client 4U в защищенной сети будет невозможна.

Установка ключей (на стр. 24, на стр. 14) на компьютер выполняется с помощью дистрибутива ключей (файла *.dst) и пароля пользователя ViPNet. Вы можете получить их лично или другим доверенным способом у администратора сети ViPNet. Если для вас выбран способ аутентификации в ViPNet Client 4U с помощью персонального ключа на внешнем устройстве (см. [Способы аутентификации в ViPNet Client 4U](#) на стр. 12), то администратор сети ViPNet также передаст вам внешнее устройство и ПИН к нему.

После установки ключей пароль пользователя ViPNet или ПИН от устройства также может потребоваться вводить при подключении к сети ViPNet в зависимости от уровня полномочий, назначенного вам администратором сети ViPNet:

- Минимальный уровень полномочий — ввод пароля или ПИН требуется всегда.
- Максимальный, средний и специальный уровни полномочий — ввод пароля или ПИН не требуется ни при каких условиях.

Примечание. Перед созданием ключей администратор сети ViPNet в ViPNet Administrator должен назначить вашему узлу [роль](#) (см. глоссарий, стр. 39) «Client for Linux» (0091). Иначе работа ViPNet Client 4U будет невозможна.



Если предполагается установка дистрибутива ключей на маломощное устройство, для файла дистрибутива ключей должны выполняться следующие ограничения:

- Максимальный размер файла *.dst — 5 Мбайт.
 - Максимальное количество туннелей — 3000.
 - Максимальное количество связей с узлами — 500.
-

Способы аутентификации в ViPNet Client 4U

ViPNet Client 4U поддерживает два способа аутентификации пользователей:

- Пароль — однофакторная аутентификация, пользователь вводит только пароль.

- Персональный ключ на внешнем устройстве (токене) — двухфакторная аутентификация, пользователь подключает к компьютеру внешнее устройство с персональным ключом и вводит ПИН.

Способ аутентификации выбирает администратор сети ViPNet при создании дистрибутива ключей. Подробнее см. документ «ViPNet Client 4U for Linux. Руководство администратора», раздел «Порядок установки программы ViPNet Client 4U».

Если выбран второй способ аутентификации, то администратор сети ViPNet записывает персональный ключ пользователя на внешнее устройство и задает ПИН для него во время создания дистрибутива ключей. Затем администратор сети ViPNet передает пользователю файл дистрибутива ключей (*.dst), пароль пользователя ViPNet, внешнее устройство с персональным ключом и ПИН к нему.

Подключать к компьютеру внешнее устройство с персональным ключом и вводить ПИН к нему в ViPNet Client 4U потребуется при установке ключей, а также при каждом подключении к сети ViPNet (при этом вводить ПИН потребуется, только если вы обладаете минимальным уровнем полномочий). Без аутентификации по персональному ключу на внешнем устройстве работа в сети ViPNet будет невозможна.

Также в процессе работы с ViPNet Client 4U вы можете самостоятельно сменить способ аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве (см. [Смена способа аутентификации](#) на стр. 19).

Работа в командной строке

Установка ключей

Установка ключей при аутентификации по паролю

1 В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient installkeys <путь_к_дистрибутиву_ключей> [--psw  
<пароль_от_дистрибутива_ключей>] [--no-failprotect] [--no-autostart] [--no-start]
```

где:

- `--psw` — параметр для указания пароля пользователя ViPNet. Чтобы снизить риск компрометации пароля, применять параметр `--psw` не рекомендуется, так как при этом пароль отображается в консоли в явном виде. Вводите пароль по запросу во время выполнения команды.



Примечание. Если пароль указывается с помощью параметра `--psw` и содержит спецсимволы, используйте экранирование спецсимволов. Подробнее см. в справочных материалах используемого командного интерпретатора (например, `man bash`).

- `--no-failprotect` — отключение ежеминутной проверки работоспособности ViPNet Client 4U и ее автоматического запуска в случае нештатного завершения работы. Для более надежной работы ViPNet Client 4U применять этот параметр не рекомендуется. По умолчанию счетчик попыток восстановления работоспособности ViPNet Client 4U выставлен на 10 попыток, на промышленных контроллерах — на бесконечное число попыток.
 - `--no-autostart` — отключение автоматического запуска ViPNet Client 4U и подключения к сети ViPNet после авторизации пользователя в ОС. Для более надежной работы ViPNet Client 4U применять этот параметр не рекомендуется.
 - `--no-start` — отказ автоматического подключения к сети ViPNet после установки ключей.
- 2** Если пароль не был указан в команде, введите пароль пользователя ViPNet и нажмите клавишу **Enter**.
- 3** Подождите, пока ключи будут установлены. Выполнение команды может занять некоторое время.

Если в файле будут выявлены ошибки, появится уведомление об этом. Обратитесь к администратору сети ViPNet.

В результате ключи будут установлены в рабочий каталог ViPNet. После установки ключей VPN-соединение будет включено автоматически. Если при установке ключей был указан параметр `--no-start`, включите VPN-соединение вручную (см. [Запуск и завершение работы](#) на стр. 17).

Установка ключей при аутентификации с помощью внешнего устройства

1 Подключите внешнее устройство к компьютеру.

2 В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient installkeys <путь_к_дистрибутиву_ключей> [--pin <ПИН-код>]
[--psw <пароль_от_дистрибутива_ключей>] [--token-select <часть_названия>]
[--no-failprotect] [--no-autostart] [--no-start]
```

где:

- `--pin` — параметр для указания ПИН от внешнего устройства с персональным ключом пользователя. Чтобы снизить риск компрометации ПИН, применять параметр `--pin` не рекомендуется, так как при этом ПИН отображается в консоли в явном виде. Вводите ПИН по запросу во время выполнения команды.
- `--psw` — параметр для указания пароля пользователя ViPNet. Чтобы снизить риск компрометации пароля, применять параметр `--psw` не рекомендуется, так как при этом пароль отображается в консоли в явном виде. Вводите пароль по запросу во время выполнения команды.



Примечание. Если пароль указывается с помощью параметра `--psw` и содержит спецсимволы, используйте экранирование спецсимволов. Подробнее см. в справочных материалах используемого командного интерпретатора (например, `man bash`).

- `--token-select` — параметр для поиска (по любой части названия) и выбора внешнего устройства, если к компьютеру подключено несколько внешних устройств. Если конкретное внешнее устройство не будет указано с помощью этого параметра, в консоли отобразится список подключенных внешних устройств и предложение выбрать одно из них.
 - `--no-failprotect` — отключение ежеминутной проверки работоспособности ViPNet Client 4U и ее автоматического запуска в случае нештатного завершения работы. Для более надежной работы ViPNet Client 4U применять этот параметр не рекомендуется. По умолчанию счетчик попыток восстановления работоспособности ViPNet Client 4U выставлен на 10 попыток, на промышленных контроллерах — на бесконечное число попыток.
 - `--no-autostart` — отключение автоматического запуска ViPNet Client 4U и подключения к сети ViPNet после авторизации пользователя в ОС. Для более надежной работы ViPNet Client 4U применять этот параметр не рекомендуется.
 - `--no-start` — отказ от автоматического подключения к сети ViPNet после установки ключей.
- 3 Если не был указан параметр `--token-select` или найдено несколько внешних устройств, введите номер нужного внешнего устройства и нажмите **Enter**.

- 4 Если ПИН не был указан в команде, введите ПИН от внешнего устройства и нажмите **Enter**.
- 5 Если пароль не был указан в команде и вам назначен максимальный, средний или специальный уровень полномочий, введите пароль пользователя ViPNet и нажмите **Enter**. При минимальном уровне полномочий вводить этот пароль не потребуется.
- 6 Подождите, пока ключи будут установлены. Выполнение команды может занять некоторое время.

Если в файле будут выявлены ошибки, появится уведомление об этом. Обратитесь к администратору сети ViPNet.

```
user@host:~$ vipnetclient installkeys Perminov_Pavel/abn_1738.dst
Your key set requires Logon Device
Please make sure that your Logon Device is attached and press Enter
Searching for connected Logon Devices ...

Device 1:
Module:          ruToken(slot:00000000)
Model:           Rutoken ECP
Label:           Rutoken ECP <no label>
Manufacturer:    Aktiv Co.
Serial:          31905a82
Pin:             OK

Device 2:
Module:          JaCarta(slot:0001FFFF)
Model:           JaCarta Laser
Label:
Manufacturer:    Aladdin R.D.
Serial:          6195300000B78547
Pin:             OK

... Success
Please type a device number and press Enter: 2
Type ViPNet user PIN:
Type ViPNet user password:
Installing keys of the "user" user ... Success
Turning on ViPNet autostart at "user" logon ... Success
Logging on to ViPNet software as "user" ... Success
user@host:~$
```

Рисунок 1. Установка ключей при аутентификации с помощью внешнего устройства

В результате ключи будут установлены в рабочий каталог ViPNet. После установки ключей VPN-соединение будет включено автоматически. Если при установке ключей был указан параметр `--no-start`, включите VPN-соединение вручную (см. [Запуск и завершение работы](#) на стр. 17).

Обновление ключей

Обновление ключей на узле необходимо, если была изменена структура сети ViPNet или свойства сетевых узлов, а также в случае смены [мастер-ключей](#) (см. глоссарий, стр. 38). Администратор сети ViPNet создает новые ключи и централизованно отправляет их на узлы, где они будут приняты и установлены автоматически, без участия пользователя.

Если новые ключи не могут быть переданы по сети, обновите их вручную:

- 1 [Удалите установленные ключи](#) (на стр. 17).
- 2 [Установите новые ключи](#) (на стр. 14).

Удаление ключей

Чтобы удалить ключи (например, [при обновлении ключей](#) (на стр. 16) или же в случае смены компьютера):

- 1 В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient deletekeys [--skip-accept]
```

где:

`--skip-accept` — автоматическое подтверждение удаления ключей.

- 2 Если не был указан параметр `--skip-accept`, подтвердите удаление ключей, для этого введите `Y` и нажмите **Enter**.

Запуск и завершение работы

Запуск всех компонентов ViPNet Client 4U и подключение к сети ViPNet выполняются автоматически после установки ключей и при каждой авторизации в ОС пользователя, установившего ключи.

Автоматический запуск программы и подключение к сети ViPNet после авторизации пользователя в ОС не выполняются в следующих случаях:

- Если пользователь ViPNet обладает минимальными полномочиями.
- Если используется аутентификация пользователя ViPNet по персональному ключу на внешнем устройстве (см. [Способы аутентификации в ViPNet Client 4U](#) на стр. 12) и внешнее устройство не подключено к компьютеру.
- Если при установке ключей был указан параметр `--no-autostart`.

Чтобы запустить ViPNet Client 4U и включить VPN-соединение вручную:

- 1 Если в ViPNet Client 4U используется аутентификация пользователя по персональному ключу на внешнем устройстве, подключите внешнее устройство к компьютеру.
- 2 В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient start {[--pin <ПИН-код>] | [--psw  
<пароль_от_дистрибутива_ключей>]} [--token-select <часть_названия>]  
[--no-failprotect]
```

где:

- `--pin` — параметр для указания ПИН от внешнего устройства с персональным ключом пользователя (если используется соответствующий способ аутентификации). ПИН требуется вводить только при минимальном уровне полномочий пользователя. Чтобы снизить риск компрометации ПИН, применять параметр `--pin` не рекомендуется, так как при этом ПИН отображается в консоли в явном виде. Вводите ПИН по запросу во время выполнения команды.

- `--psw` — параметр для указания пароля пользователя ViPNet (если используется аутентификация пользователя по паролю). Пароль требуется вводить только при минимальном уровне полномочий пользователя. Чтобы снизить риск компрометации пароля, применять параметр `--psw` не рекомендуется, так как при этом пароль отображается в консоли в явном виде. Вводите пароль по запросу во время выполнения команды.



Примечание. Если пароль указывается с помощью параметра `--psw` и содержит спецсимволы, используйте экранирование спецсимволов. Подробнее см. в справочных материалах используемого командного интерпретатора (например, `man bash`).

- `--token-select` — параметр для поиска (по любой части названия) и выбора внешнего устройства, если к компьютеру подключено несколько внешних устройств. Если конкретное внешнее устройство не будет указано с помощью этого параметра, в консоли отобразится список подключенных внешних устройств и предложение выбрать одно из них.
 - `--no-failprotect` — отключение ежеминутной проверки работоспособности ViPNet Client 4U и ее автоматического запуска в случае нештатного завершения работы. Для более надежной работы ViPNet Client 4U применять этот параметр не рекомендуется. По умолчанию счетчик попыток восстановления работоспособности ViPNet Client 4U выставлен на 10 попыток, на промышленных контроллерах — на бесконечное число попыток.
- 3 Если для аутентификации используется внешнее устройство и не был указан параметр `--token-select` либо найдено несколько внешних устройств, введите номер нужного внешнего устройства и нажмите **Enter**.
 - 4 Если вы обладаете минимальными полномочиями в ViPNet Client 4U, введите пароль пользователя ViPNet или ПИН и нажмите клавишу **Enter**.
 - 5 Подождите, пока VPN-соединение будет включено. Выполнение команды может занять некоторое время.

Чтобы остановить ViPNet Client 4U и выключить VPN-соединение, выполните:

```
user@host:~$ vipnetclient stop
```

Если используется аутентификация пользователя по персональному ключу на внешнем устройстве, то при отключении внешнего устройства от компьютера VPN-соединение будет автоматически выключено.

Проверка связи с координатором

При [подключении к сети ViPNet](#) (на стр. 17) программа ViPNet Client 4U автоматически проверяет связь с координатором, являющимся [сервером соединений](#) (см. глоссарий, стр. 39) для вашего компьютера. Если координатор недоступен, взаимодействие с другими узлами сети ViPNet невозможно.

Также вы можете проверить связь с координатором вручную. Например, если прервалась связь с какими-либо ресурсами защищенной сети, и вы хотите проверить подключение к сети ViPNet. Для этого:

- 1 В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient debug --ping
```

- 2 Дождитесь результата выполнения команды.

Если связь с координатором отсутствует, повторите попытку через некоторое время или обратитесь к администратору сети ViPNet.



Примечание. Также вы можете проверить связь с другими узлами:

```
user@host:~$ vipnetclient debug --ping <идентификатор_узла_ViPNet>
```

Смена способа аутентификации

В ViPNet Client 4U вы можете сменить способ аутентификации (см. [Способы аутентификации в ViPNet Client 4U](#) на стр. 12) — с аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве. Для этого:

- 1 Подключите внешнее устройство к компьютеру.

- 2 В консоли ОС Linux выполните:

```
$ vipnetclient debug --change-logon-type [--pin <ПИН-код>] [--token-select <часть_названия>]
```

где:

`--pin` — параметр для задания ПИН для внешнего устройства, на которое будет записан персональный ключ пользователя. Чтобы снизить риск компрометации ПИН, применять параметр `--pin` не рекомендуется, так как при этом ПИН отображается в консоли в явном виде. Вводите ПИН по запросу во время выполнения команды.

`--token-select` — параметр для поиска (по любой части названия) и выбора внешнего устройства, если к компьютеру подключено несколько внешних устройств. Если конкретное внешнее устройство не будет указано с помощью этого параметра, в консоли отобразится список подключенных внешних устройств и предложение выбрать одно из них.

- 3 Если не был указан параметр `--token-select` или найдено несколько внешних устройств, введите номер нужного внешнего устройства и нажмите **Enter**.
- 4 Если ПИН не был указан в команде, введите ПИН для внешнего устройства и нажмите **Enter**.
- 5 Подождите, пока персональный ключ будет записан на внешнее устройство. При извлечении внешнего устройства до завершения операции способ аутентификации не будет изменен.

Если при переносе персонального ключа на внешнее устройство возникнет ошибка (например, на устройстве записан чужой персональный ключ или устройство повреждено), обратитесь к администратору сети ViPNet.

```

user@host:~$ vipnetclient debug --change-logon-type
Please make sure that your Logon Device is attached and press Enter
Searching for connected Logon Devices ...

Device 1:
Module:      ruToken(slot:00000000)
Model:       Rutoken ECP
Label:       Rutoken ECP <no label>
Manufacturer: Aktiv Co.
Serial:      31905a82
Pin:         OK

Device 2:
Module:      JaCarta(slot:0001FFFF)
Model:       JaCarta Laser
Label:
Manufacturer: Aladdin R.D.
Serial:      6195300000B78547
Pin:         OK

... Success
Please type a device number and press Enter: 2
Type ViPNet user PIN:
Changing logon mode to Logon Device ... Success
user@host:~$

```

Рисунок 2. Смена способа аутентификации

Просмотр списка защищенных узлов

- 1 Чтобы просмотреть список защищенных узлов, в консоли ОС Linux выполните:

```
user@host:~$ vipnetclient list --nodes
```

В консоли отобразится список защищенных узлов, с которыми ваш компьютер может взаимодействовать в сети ViPNet. В этом списке типы узлов отмечены как `client` (клиент) и `server` (координатор). Координатор, являющийся сервером соединений, отмечен в списке символом `*`.

```

user@host:~$ vipnetclient list --nodes
ID      Type   Access IP      Name
3500000A server* 7.0.0.10      Координатор Москва
35000013 client 7.0.0.19      Иванов Денис
35000014 client 7.0.0.20      Николаев Александр
35000015 client 7.0.0.21      Петров Алексей
35000016 client 7.0.0.22      Соколова Ирина
35000017 client 7.0.0.23      Сидоров Андрей
35000018 client 7.0.0.24      Маслова Мария
35000019 client 7.0.0.25      Перминов Павел
3500001A client 7.0.0.26      Юрьев Александр
3500001B client 7.0.0.27      Максимов Олег
3500001C client 7.0.0.28      Фёдоров Алексей
35000026 server 7.0.0.38      Координатор Уфа
35000027 server 7.0.0.39      Координатор Пенза
user@host:~$

```

Рисунок 3. Просмотр списка узлов

- 2 Чтобы просмотреть подробную информацию об узле из списка, при включенном VPN-соединении выполните:

```
user@host:~$ vipnetclient iplirdiag -s ipsettings --node-info <идентификатор_узла>
```

В консоли отобразится подробная информация об узле (идентификатор и имя узла, его IP-адрес видимости и другая информация). Для координаторов отображаются также туннелируемые ими IP-адреса открытых узлов.

```
user@host:~$ vipnetclient iplirdiag -s ipsettings --node-info 35D0000A
Calling the "iplirdiag" with the following parameters: -s ipsettings --node-info 35D0000A ... Success

Node row
node: 35D0000A
proxyType: StaticWithoutFixIpAddress
visibility: Virtual
methodIpAccess: FirewallIp
numRealIps: 2
numTunnelingIps: 3
firstVirtualIp: 7.0.0.10
firewallIp: 10.0.166.10
accessUdpPort: 55777
multicastPort: 0
proxyId: FFFFFFFE
forwardId: 00000000
forwardIdExist: 0
incType: IncapsForceVirtualIp (0x401000)
properties: SupportGostOfb Unknown (0x80004)
encryption: gost
timeout: 0
timestamp: 1644996539
lastAdapterNumber: 0
m_ForwardIp (obs): 10.0.166.10
Internet Gateway mode: No

Access point for node: 35D0000A
node: 35D0000A
ipAddress: 10.0.166.10
udpPort: 55777

The ip address table for node 35D0000A(rows 2):
Real      Visibility
10.0.166.10  7.0.0.10
192.168.1.150  7.1.0.10

The tunneling ip address table for node 35D0000A(rows 3):
Begin real      End real      Begin visibility  End visibility
10.0.0.40       10.0.0.40     10.0.0.40         10.0.0.40
192.168.1.1     192.168.1.10  192.168.1.1       192.168.1.10
192.168.10.12   192.168.10.12 192.168.10.12     192.168.10.12
user@host:~$
```

Рисунок 4. Просмотр подробной информации об узле

Совет. Вы можете обращаться к узлам защищенной сети не только по IP-адресам и DNS-именам, но и по служебным адресам ViPNet:

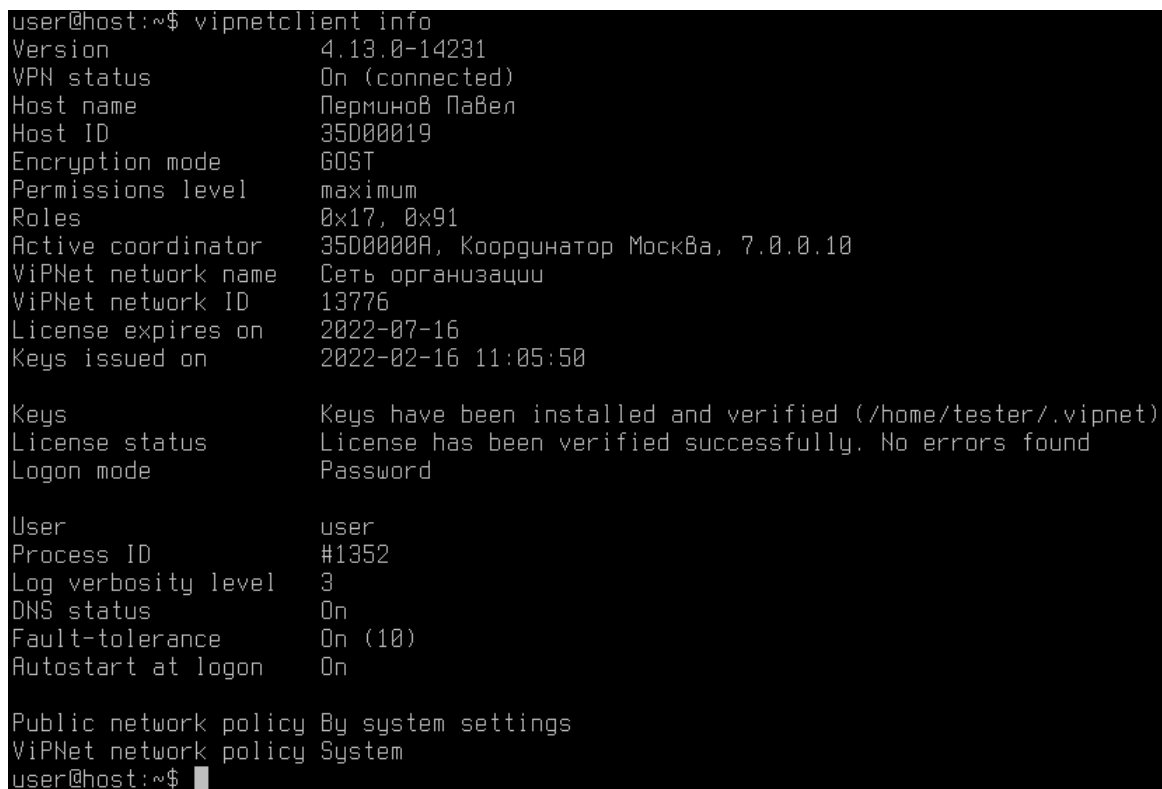


- <идентификатор_узла_ViPNet>.vipnet — для обращения к сетевым узлам ViPNet. Например, 2DBF001D.vipnet.
 - <IP-адрес_туннеля>.<идентификатор_туннелирующего_координатора>.vipnet — для обращения к ресурсам, туннелируемым координатором ViPNet. Например, 10.0.2.26.2DBF000A.vipnet.
-

Просмотр информации о своем узле и версии ViPNet Client 4U

- 1 Чтобы просмотреть информацию о своем узле и версии ViPNet Client 4U, в консоли ОС Linux выполните:

```
user@host:~$ vipnetclient info
```



```
user@host:~$ vipnetclient info
Version                4.13.0-14231
VPN status              On (connected)
Host name               Перминов Павел
Host ID                 35000019
Encryption mode         GOST
Permissions level       maximum
Roles                   0x17, 0x91
Active coordinator      3500000A, Координатор Москва, 7.0.0.10
ViPNet network name     Сеть организации
ViPNet network ID       13776
License expires on      2022-07-16
Keys issued on          2022-02-16 11:05:50

Keys                   Keys have been installed and verified (/home/tester/.vipnet)
License status          License has been verified successfully. No errors found
Logon mode              Password

User                    user
Process ID              #1352
Log verbosity level     3
DNS status              On
Fault-tolerance         On (10)
Autostart at logon      On

Public network policy   By system settings
ViPNet network policy   System
user@host:~$
```

Рисунок 5. Просмотр информации о своем узле

- 2 Чтобы просмотреть информацию только о версии ViPNet Client 4U, выполните:

```
user@host:~$ vipnetclient --version
```

Если в строке `DNS status` отображается статус, отличный от `on`, следуйте указаниям раздела «Нарушена работа программы ViPNet Client 4U с DNS» в документе «ViPNet Client 4U for Linux. Руководство администратора».

Если разница во времени на вашем компьютере и координаторе, который является сервером соединений, больше разрешенной на координаторе, взаимодействие между ними невозможно. В этом случае при выполнении команды `vipnetclient info` отобразится сообщение о разнице во времени и рекомендация перевести часы на компьютере.

Если в строке `License status` отображается информация об истечении срока действия лицензии, обратитесь к администратору сети ViPNet для обновления лицензии.

Обращение в службу технической поддержки

В случае возникновения ошибок в работе ViPNet Client 4U, создайте и передайте отчет о работе программы в ИнфоТеКС:

- 1 Создайте отчет о работе ViPNet Client 4U. Для этого в консоли ОС Linux выполните:

```
user@host:~$ vipnetclient report [--output  
<каталог_для_сохранения_отчета>/<имя_файла_отчета>]
```

где:

--output — параметр для указания имени отчета и каталога, в который будет сохранен файл отчета. Если в команде вы не укажете каталог и имя отчета, то отчет будет сохранен в каталоге, в котором была выполнена команда `vipnetclient report`, с использованием шаблона имени по умолчанию — `report_<версия_клиента>_<дата>_<время>.zip`.

- 2 Подождите, пока будет создан отчет о работе ViPNet Client 4U. Выполнение команды может занять некоторое время.

В результате будет создан архив с отчетом о работе ViPNet Client 4U в формате ZIP.
- 3 Создайте электронное письмо с описанием проблемы и прикрепите к письму архив с отчетом о работе ViPNet Client 4U.
- 4 Отправьте письмо в [ИнфоТеКС](#) (на стр. 11).

Работа в графическом интерфейсе

Установка ключей

Установка ключей при аутентификации по паролю

1 Откройте ViPNet Client 4U одним из способов:

- В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient-gui
```
- В списке установленных на компьютере программ щелкните значок ViPNet Client 4U .
- Дважды щелкните файл *.dst в файловом менеджере. При этом откроется окно **Установка ключей**, см. пункт 4.

Если на компьютере уже установлены ключи, появится уведомление о невозможности установить новый дистрибутив ключей. В этом случае см. [Обновление ключей](#) (на стр. 27) или [Удаление ключей](#) (на стр. 27).

2 В ViPNet Client 4U нажмите **Добавить ключи**.

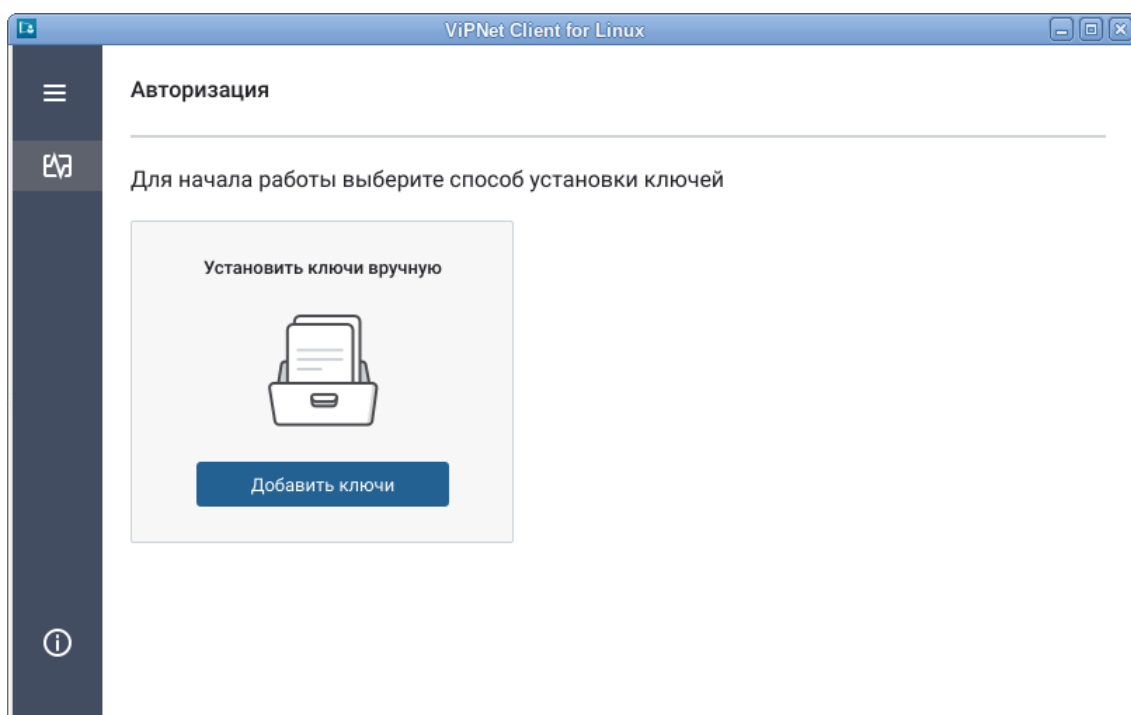


Рисунок 6. Установка дистрибутива ключей

3 Выберите файл дистрибутива ключей (*.dst).

Если в файле будут выявлены ошибки, появится уведомление об этом. Обратитесь к администратору сети ViPNet.

4 В окне **Установка ключей** введите пароль пользователя ViPNet и нажмите **Далее**.

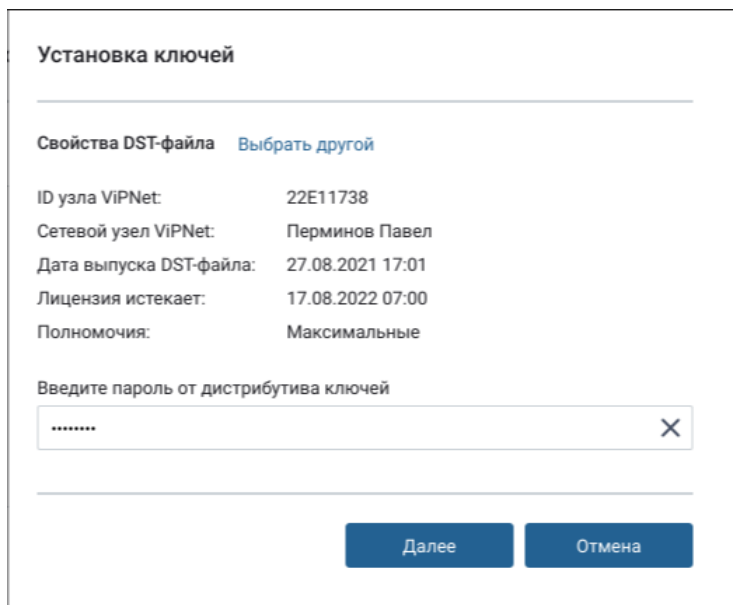


Рисунок 7. Установка ключей при аутентификации по паролю

5 Подождите, пока ключи будут установлены. Это может занять некоторое время.

После установки ключей VPN-соединение будет включено автоматически.

Установка ключей при аутентификации с помощью внешнего устройства

1 Подключите внешнее устройство к компьютеру.

2 Откройте ViPNet Client 4U одним из способов:

- В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient-gui
```
- В списке установленных на компьютере программ щелкните значок ViPNet Client 4U .
- Дважды щелкните файл *.dst в файловом менеджере. При этом откроется окно **Установка ключей**, см. пункт 5.

Если на компьютере уже установлены ключи, появится уведомление о невозможности установить новый дистрибутив ключей. В этом случае см. [Обновление ключей](#) (на стр. 27) или [Удаление ключей](#) (на стр. 27).

3 В ViPNet Client 4U нажмите **Добавить ключи**.

4 Выберите файл дистрибутива ключей (*.dst).

Если в файле будут выявлены ошибки, появится уведомление об этом. Обратитесь к администратору сети ViPNet.

- 5 В окне **Установка ключей** нажмите **Далее**.

Установка ключей

Свойства DST-файла [Выбрать другой](#)

ID узла ViPNet: 22E11738
Сетевой узел ViPNet: Перминов Павел
Дата выпуска DST-файла: 27.08.2021 17:01
Лицензия истекает: 17.08.2022 07:00
Полномочия: Максимальные
Тип аутентификации: С использованием персонального ключа на внешнем устройстве

Далее **Отмена**

Рисунок 8. Установка ключей при аутентификации с помощью внешнего устройства

- 6 Если к компьютеру подключено несколько устройств, выберите нужное устройство в списке и нажмите **Далее**.

Установка ключей

Подключите устройство и выберите его в списке

Обновить список устройств

Rutoken ECP <no label> (Rutoken ECP)	31905A82
(JaCarta Laser)	6195300000B78547

Назад **Далее** **Отмена**

Рисунок 9. Выбор внешнего устройства

- 7 Введите ПИН от внешнего устройства и нажмите **Далее**.

Рисунок 10. Ввод ПИН-кода к внешнему устройству

- 8 Если вам назначен максимальный, средний или специальный уровень полномочий, введите пароль пользователя ViPNet и нажмите **Далее**. При минимальном уровне полномочий вводить этот пароль не потребуется.
- 9 Подождите, пока ключи будут установлены. Это может занять некоторое время.

После установки ключей VPN-соединение будет включено автоматически.

Обновление ключей

Обновление ключей на узле необходимо, если была изменена структура сети ViPNet или свойства сетевых узлов, а также в случае смены [мастер-ключей](#) (см. глоссарий, стр. 38). Администратор сети ViPNet создает новые ключи и централизованно отправляет их на узлы, где они будут приняты и установлены автоматически, без участия пользователя.

Если новые ключи не могут быть переданы по сети, обновите их вручную:

- 1 [Удалите установленные ключи](#) (на стр. 27).
- 2 [Установите новые ключи](#) (на стр. 24).

Удаление ключей

Чтобы удалить ключи (например, [при обновлении ключей](#) (на стр. 27) или же в случае смены компьютера):

- 1 В ViPNet Client 4U выберите **Профиль**  и нажмите **Удалить набор ключей**.

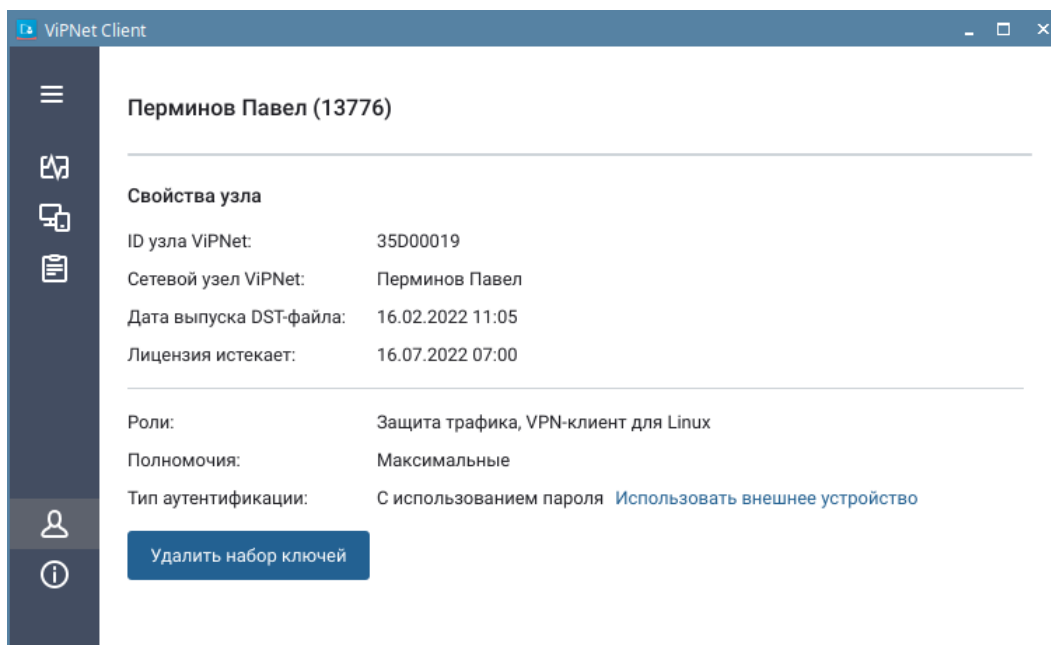


Рисунок 11. Удаление ключей

- 2 Подтвердите удаление ключей.

Запуск и завершение работы

Для запуска ViPNet Client 4U и подключения к сети ViPNet:

- 1 Если в ViPNet Client 4U используется аутентификация пользователя по персональному ключу на внешнем устройстве (см. [Способы аутентификации в ViPNet Client 4U](#) на стр. 12), подключите внешнее устройство к компьютеру.
- 2 Выполните одно из действий:
 - В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient-gui
```
 - В списке установленных на компьютере программ щелкните значок ViPNet Client 4U .
- 3 В ViPNet Client 4U нажмите **Включить**.
- 4 [При необходимости](#) (на стр. 12) введите пароль пользователя ViPNet или ПИН от внешнего устройства с персональным ключом и нажмите **ОК**.
- 5 Подождите, пока VPN-соединение будет включено. Это может занять некоторое время.

При подключении к защищенной сети ViPNet будет [проверено соединение с вашим координатором](#) (на стр. 29). Если соединение установлено, вы сможете работать с корпоративными ресурсами.

Чтобы отключиться от сети ViPNet, в ViPNet Client 4U нажмите **Выключить**.

Если используется аутентификация пользователя по персональному ключу на внешнем устройстве, то при отключении внешнего устройства от компьютера VPN-соединение будет автоматически выключено.

Проверка связи с координатором

При [подключении к сети ViPNet](#) (на стр. 28) программа ViPNet Client 4U автоматически проверяет связь с координатором, являющимся [сервером соединений](#) (см. глоссарий, стр. 39) для вашего компьютера. Если координатор недоступен, взаимодействие с другими узлами сети ViPNet невозможно.

Также вы можете проверить связь с координатором вручную. Например, если прервалась связь с какими-либо ресурсами защищенной сети, и вы хотите проверить подключение к сети ViPNet. Для этого в ViPNet Client 4U нажмите . Если связь с координатором отсутствует, повторите попытку через некоторое время или обратитесь к администратору сети ViPNet.



Примечание. Если разница во времени на вашем компьютере и координаторе, который является сервером соединений, больше разрешенной на координаторе, взаимодействие между ними невозможно. В этом случае в ViPNet Client 4U появится уведомление о разнице во времени и рекомендация перевести часы на компьютере.

Смена способа аутентификации

В ViPNet Client 4U вы можете сменить способ аутентификации (см. [Способы аутентификации в ViPNet Client 4U](#) на стр. 12) — с аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве. Для этого:

- 1 Подключите внешнее устройство к компьютеру.
- 2 В ViPNet Client 4U выберите **Профиль** .
- 3 Щелкните **Использовать внешнее устройство**.
- 4 Если к компьютеру подключено несколько устройств, в окне **Перенос персонального ключа на внешнее устройство** выберите нужное устройство в списке и нажмите **Далее**.

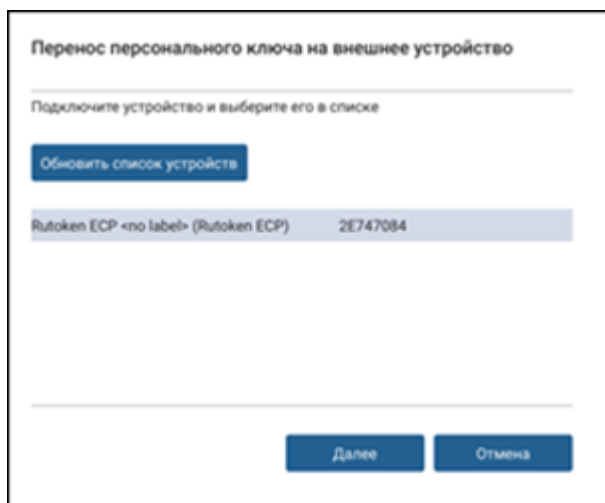


Рисунок 12. Смена способа аутентификации

- 5 Введите ПИН от внешнего устройства и нажмите **Далее**.
- 6 Подождите, пока персональный ключ будет записан на внешнее устройство. При извлечении внешнего устройства до завершения операции способ аутентификации не будет изменен.

Если при переносе персонального ключа на внешнее устройство возникнет ошибка (например, на устройстве записан чужой персональный ключ или устройство повреждено), обратитесь к администратору сети ViPNet.

Просмотр списка защищенных узлов

- 1 В ViPNet Client 4U выберите раздел **Сетевые узлы** .
- Отобразится список защищенных узлов, с которыми ваш компьютер может взаимодействовать в сети ViPNet.
- 2 Чтобы найти узел в списке, в поле поиска начните вводить имя или идентификатор узла.
- 3 Чтобы просмотреть только список координаторов, в списке **Все узлы** выберите **Координаторы**.
- 4 Чтобы просмотреть подробную информацию об узле, выберите его в списке узлов. Справа отобразится панель с информацией об узле: идентификатор узла и его IP-адрес видимости. Для координаторов также отображаются туннелируемые ими IP-адреса открытых узлов.

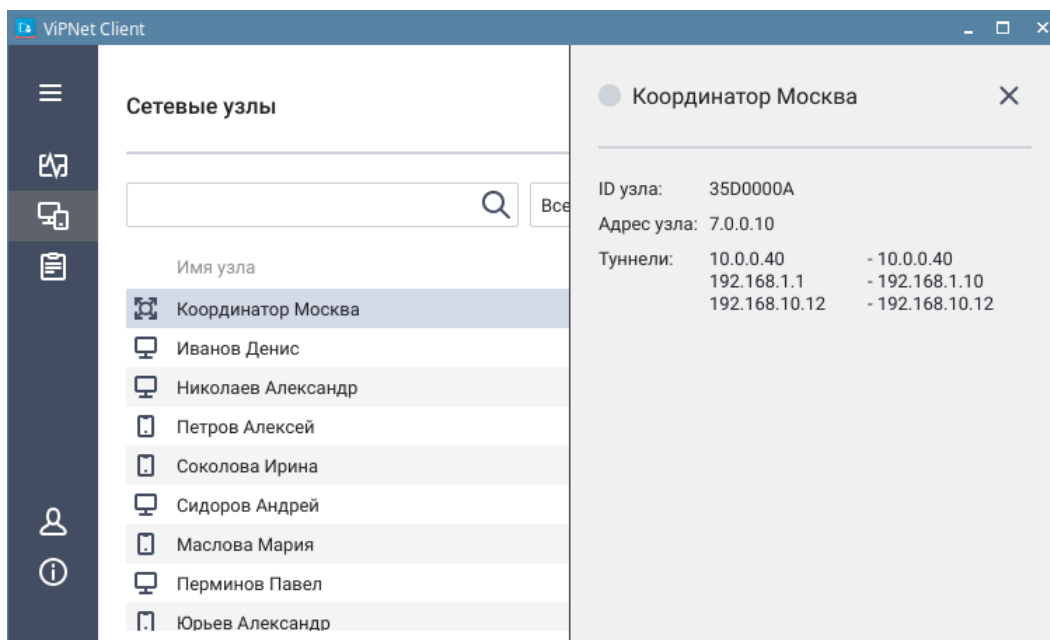


Рисунок 13. Просмотр информации об узлах

Совет. Вы можете обращаться к узлам защищенной сети не только по IP-адресам и DNS-именам, но и по служебным адресам ViPNet:



- `<идентификатор_узла_ViPNet>.vipnet` — для обращения к сетевым узлам ViPNet. Например, `2DBF001D.vipnet`.
- `<IP-адрес_туннеля>.<идентификатор_туннелирующего_координатора>.vipnet` — для обращения к ресурсам, туннелируемым координатором ViPNet. Например, `10.0.2.26.2DBF000A.vipnet`.

Просмотр информации о своем узле и версии ViPNet Client 4U

- 1 Чтобы просмотреть версию ViPNet Client 4U, выберите **О программе** .
- 2 Чтобы просмотреть информацию о своем узле, выберите **Профиль** .

Контроль целостности и работоспособности

Если правилами вашей организации предусмотрена периодическая регламентная проверка целостности и работоспособности используемого ПО, системный администратор, администратор безопасности или сам пользователь может выполнить в ViPNet Client 4U следующие проверки:

- Проверка целостности программного обеспечения ViPNet Client 4U и среды функционирования.
- Проверка работоспособности криптографических алгоритмов.
- Проверка работоспособности датчиков случайных чисел.

Для проверки целостности и работоспособности ViPNet Client 4U:

- 1 В ViPNet Client 4U выберите **Безопасность**  и нажмите **Начать проверку**.
- 2 Дождитесь завершения проверки, это может занять несколько минут.

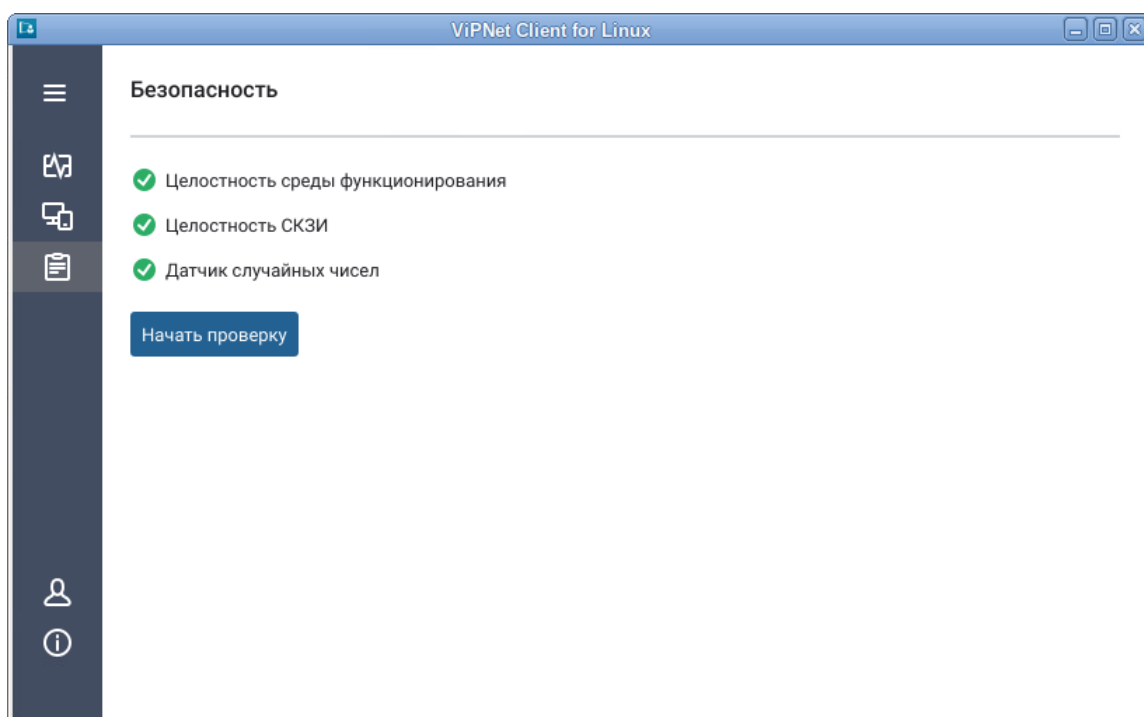


Рисунок 14. Просмотр результатов контроля функционирования

В случае нарушения целостности или при неработоспособности компонентов ViPNet Client 4U, например, в результате вмешательства посторонних лиц, работа с программой будет невозможна. В этом случае обратитесь к администратору вашей сети ViPNet для восстановления работоспособности программы.

Обращение в службу технической поддержки

В случае возникновения ошибок в работе ViPNet Client 4U, создайте и передайте отчет о работе программы в ИнфоТеКС:

- 1 В ViPNet Client 4U выберите **О программе** .
- 2 Нажмите **Создать отчет об ошибке**.
- 3 Нажмите **Обзор** и укажите папку для сохранения отчета о работе ViPNet Client 4U. Затем нажмите **Сохранить**.
- 4 Подождите, пока будет создан отчет, это может занять некоторое время.
В результате будет создан архив с отчетом о работе ViPNet Client 4U в формате ZIP.
- 5 Создайте электронное письмо с описанием проблемы и прикрепите к нему архив с отчетом о работе ViPNet Client 4U.
- 6 Отправьте письмо в [ИнфоТеКС](#) (на стр. 11).

История версий

В данном приложении описаны основные изменения в различных версиях ViPNet Client 4U.

Что нового в версии 4.12

Исправление ошибок

В ViPNet Client 4U были исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Что нового в версии 4.11

Аутентификация с помощью внешних устройств

Раньше в программе ViPNet Client 4U использовалась только однофакторная аутентификация пользователя по паролю. В новой версии программы ViPNet Client 4U реализована двухфакторная аутентификация пользователя с помощью персонального ключа на внешнем устройстве и ПИН-кода к нему (см. [Способы аутентификации в ViPNet Client 4U](#) на стр. 12). Способ аутентификации выбирает администратор сети ViPNet при создании дистрибутива ключей.

Что нового в версии 4.10

- **Увеличение производительности**

В новой версии программы ViPNet Client 4U за счет включения аппаратного ускорения повышена скорость шифрования и передачи трафика через VPN-соединение.

- **Исправление ошибок**

В ViPNet Client 4U были исправлены ошибки, обнаруженные при эксплуатации предыдущей версии программы.

Что нового в версии 4.9

Поддержка ViPNet Connect for Linux

В новой версии ViPNet Client 4U обеспечена работа с программой ViPNet Connect for Linux на ОС Альт Линукс 8.2.

Что нового в версии 4.8

- **Обращение к сетевым узлам по служебным именам**

Теперь вы можете обращаться к узлам сети ViPNet по их служебным именам (например, для организации удаленного доступа, проверки связи с узлами, доступа к корпоративным ресурсам). Для обращения к сетевому узлу по служебному имени вводите следующее:

- `<идентификатор_узла_ViPNet>.vipnet` — для обращения к сетевым узлам ViPNet. Например, `2DBF001D.vipnet`.
- `<IP-адрес_туннеля>.<идентификатор_туннелирующего_координатора>.vipnet` — для обращения к ресурсам, туннелируемым координатором ViPNet. Например, `10.0.2.26.2DBF000A.vipnet`.

- **Уведомление о разнице во времени с координатором**

Если разница во времени на координаторе и клиенте с программой ViPNet Client 4U, который стоит за этим координатором, больше разрешенной на координаторе, взаимодействие между ними невозможно. В этом случае в интерфейсе ViPNet Client 4U будет отображаться оповещение о разнице во времени и рекомендация перевести часы на компьютере.

Данная функция поддерживается только координаторами с ПО ViPNet Coordinator for Linux.

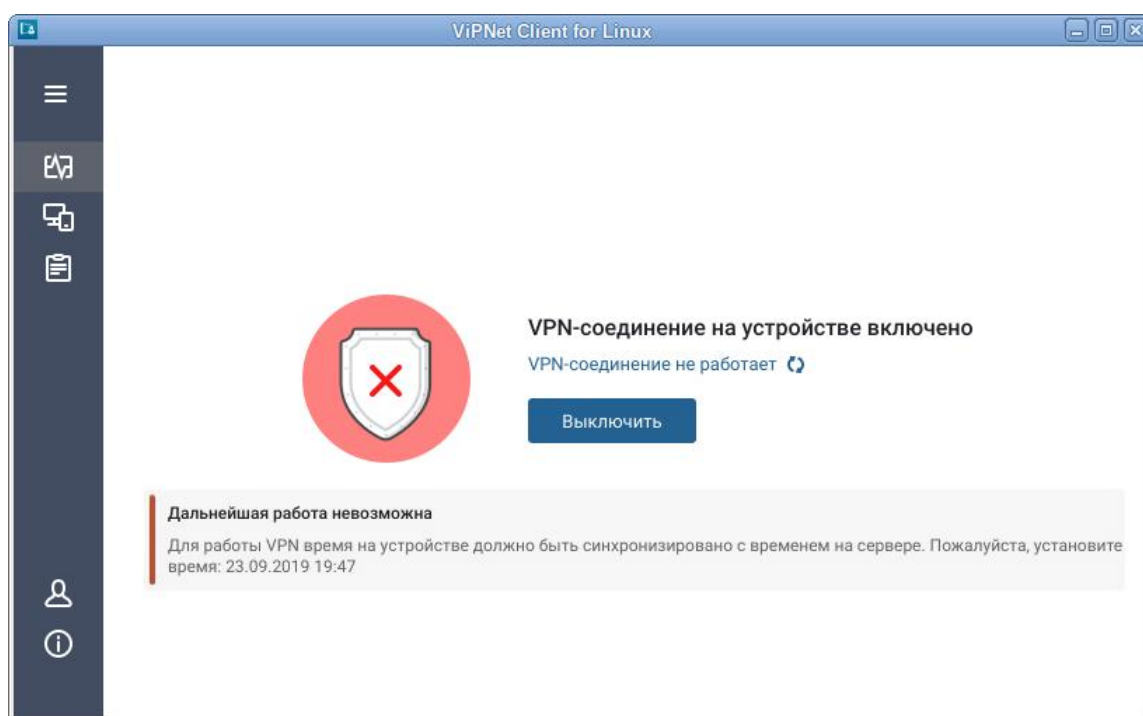


Рисунок 15. Уведомление о разнице во времени с координатором

- **Отображение уведомлений в интерфейсе и в командной строке**

В новой версии программы ViPNet Client 4U в интерфейсе и в командной строке (при выполнении команды `vipnetclient info`) отображаются оповещения о разнице во времени с координатором, о необходимости установки нового дистрибутива ключей после смены

мастер-ключей, об обновлении программы ViPNet Client 4U, о неудавшемся обновлении программы ViPNet Client 4U.

```
tester@astra:~$ vipnetclient info
Warning: clock is out of sync with the active coordinator.
Contact the administrator to correct your clock
Version          4.8.0-5172
VPN status       clock is out of sync

Host name        #Pracheva_lin_7
Host ID          15FD0CFA
Permissions level maximum
Roles            0x17, 0x65, 0x91
Active coordinator 15FD000A, CorWin_01, 11.0.0.1
ViPNet network name Infotecs, Release Control
ViPNet network ID 5629
License expires on 2022-10-10
Keys issued on   2019-04-29 16:41:56

Keys             Keys have been installed and verified (/home/tester/.vipnet)
License status   Your license has expired

User            tester
Process ID      #56117
Logging level    3
DNS status       enabled
Fault-tolerance  enabled(10)
Autostart        enabled
tester@astra:~$
```

Рисунок 16. Уведомления о разнице во времени с координатором и просроченной лицензии

- Предупреждение об установке неподписанной сборки программы ViPNet Client 4U в ОС Astra Linux Special Edition «Смоленск»

Теперь для компьютеров с ОС Astra Linux Special Edition «Смоленск» с замкнутой программной средой поставляется специальный подписанный пакет установки программы ViPNet Client 4U. Если вы установите неподписанный пакет программы ViPNet Client 4U, то при включении мандатного контроля программа работать не будет. Во время установки неподписанного пакета программы ViPNet Client 4U отображается уведомление об этом.

```
tester@astra:~$ sudo dpkg -i vipnetclient-gui_gost_ru_amd64_4.8.0-5172.deb
Выбор ранее не выбранного пакета vipnetclient-gui.
(Чтение базы данных ... на данный момент установлено 125876 файлов и каталогов.)
Подготовка к распаковке vipnetclient-gui_gost_ru_amd64_4.8.0-5172.deb ...
WARNING: You are installing unsigned package on Astra Linux
This program will stop working when executable file control will be enabled
Contact the administrator
Распаковывается vipnetclient-gui (4.8.0-5172) ...
Настраивается пакет vipnetclient-gui (4.8.0-5172) ...
vipnetclient-gui: begin configure
Package version: 4.8.0-5172
Reloading running processes . success
vipnetclient-gui: end configure
Обрабатываются триггеры для systemd (232-25+deb9u2astra.se14) ...
Обрабатываются триггеры для man-db (2.7.6.1-2) ...
Обрабатываются триггеры для mime-support (3.60) ...
Обрабатываются триггеры для hicolor-icon-theme (0.15-1) ...
Обрабатываются триггеры для shared-mime-info (1.8-1) ...
```

Рисунок 17. Уведомление об установке неподписанной сборки ViPNet Client 4U

- **Создание отчета о работе программы в графической версии программы**

Раньше создание отчета о работе программы ViPNet Client 4U для отправки в ИнфоТеКС выполнялось только в командной строке. Теперь вы можете создать отчет и с помощью интерфейса ViPNet Client 4U (см. [Обращение в службу технической поддержки](#) на стр. 33).

- **Открытие файлов *.dst с помощью программы ViPNet Client 4U**

Теперь вы можете быстро перейти к установке дистрибутива ключей, дважды щелкнув файл *.dst в файловом менеджере. В результате автоматически откроется окно **Установка ключей**.

- **Многопоточная обработка IP-трафика**

В новой версии программы ViPNet Client 4U вы можете управлять количеством потоков, используемых драйверной частью программы ViPNet Client 4U. Увеличение количества используемых потоков позволяет повысить скорость обработки IP-трафика. По умолчанию программа ViPNet Client 4U использует 4 потока.

Глоссарий

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.

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.

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.

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.

Мастер-ключ

Ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена;
- мастер-ключ ключей защиты ключей обмена;
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Роль

Функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

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.

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 защищенных узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Суперпользователь (root)

Учетная запись в UNIX-системах, пользователь которой наделен специальными полномочиями, позволяющими осуществлять полный контроль над системой, изменять системные файлы, запускать специальные приложения, выполнять резервное копирование системы. Полномочия пользователя, работающего в системе с правами root, ничем не ограничены.

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей.