ViPNet Client 4U for Linux

Руководство пользователя

infotecs

© АО «ИнфоТеКС», 2021

ФРКЕ.00239-01 34 01

Версия продукта 4.12

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)

Веб-сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru

Содержание

Введение **5**
О документе 5
Соглашения документа 5
О программе 6
Системные требования 6
Требования к корпоративной сети 8
Список поддерживаемых внешних устройств 8
Новые возможности версии 4.12 9
Комплект поставки 9
Обратная связь 9

Общие сведения **11**
Защищенная сеть ViPNet 11
Компьютер с программой ViPNet Client 4U for Linux в сети ViPNet 11
Для чего нужно устанавливать ключи 12
Способы аутентификации в программе ViPNet Client 4U for Linux 13

Работа с программой ViPNet Client 4U for Linux в командной строке **15**
Установка ключей 15
Обновление ключей 17
Удаление ключей 18
Запуск и завершение работы 18
Проверка связи с координатором 19
Смена способа аутентификации 20
Просмотр списка защищенных узлов 21
Просмотр информации о своем узле и версии программы ViPNet Client 4U for Linux 22
Обращение в службу технической поддержки 24

Работа с программой ViPNet Client 4U for Linux в графическом интерфейсе **25**
Установка ключей 25
Обновление ключей 28
Удаление ключей 28
Запуск и завершение работы 29
Интерфейс программы ViPNet Client 4U for Linux 30
Проверка связи с координатором 31

Смена способа аутентификации 32
Просмотр информации о своем сетевом узле и версии программы ViPNet Client 4U for Linux 33
Просмотр списка защищенных узлов и поиск узла 33
Контроль целостности и работоспособности 34
Обращение в службу технической поддержки 35

История версий 37
Новые возможности версии 4.11 37
Новые возможности версии 4.10 37
Новые возможности версии 4.9 37
Новые возможности версии 4.8 38

Глоссарий 41

Введение

О документе

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

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

Соглашения документа

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

Таблица 1. Обозначения, используемые в примечаниях

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

Таблица 2. Обозначения, используемые для выделения информации в тексте

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

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены пользователем операционной системы, содержат приглашение `user@host` с символами «~$»:

```
user@host:~$ команда
```

- Команды, которые могут быть выполнены администратором операционной системы, содержат приглашение `root@host` с символом «~#»:

  ```
  root@host:~# команда
  ```

- Параметры, которые должны быть заданы пользователем, заключены в угловые скобки. Например:

  ```
  команда <параметр>
  ```

- Необязательные параметры или ключевые слова заключены в квадратные скобки. Например:

  ```
  команда <обязательный параметр> [необязательный параметр]
  ```

- Если при вводе команды можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой. Например:

  ```
  команда {вариант-1 | вариант-2}
  ```

О программе

Программа ViPNet Client 4U for Linux предназначена для защиты IP-трафика на компьютерах с ОС Linux путем шифрования IP-пакетов.

С помощью программы ViPNet Client 4U for Linux, установленной на компьютере, вы можете подключаться к сетевым узлам ViPNet или узлам, которые туннелируются координаторами ViPNet, по защищенным каналам и получать доступ к размещенным на этих узлах ресурсам: корпоративным веб-порталам, электронной почте, системе IP-телефонии, различным серверам и другим корпоративным сервисам.

Программа ViPNet Client 4U for Linux поставляется в одном из двух вариантов:

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

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

Системные требования

Требования к компьютеру для установки программы ViPNet Client 4U for Linux:

- 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 3. Поддерживаемые операционные системы

Архитектура процессора	Дистрибутив Linux
x86-64	• Astra Linux Special Edition «Смоленск». • Astra Linux Common Edition 2.12.29 «Орел». • ГосЛинукс IC5. • РЕД ОС 7.2. • РЕД ОС 7.3. • Альт Рабочая станция 8.2. • Альт Рабочая станция 8 СП. • Альт Рабочая станция 9.1. • ЛОТОС (редакция для серверов и рабочих станций). • РОСА «КОБАЛЬТ» (пользовательская редакция). • AlterOS 7.5. • EMIAS OS 1.0. • Ubuntu 18.04.5 LTS. • Ubuntu 20.04.2 LTS. • Debian 9.13. • Debian 10.9. • CentOS 7.1. • CentOS 7.9. • CentOS 8.2. • CentOS 8.3.
«Эльбрус»	• Astra Linux Special Edition «Ленинград».
ARMv5	• OpenWrt Chaos Calmer Build for RTU968V2 v.2.6.4E.
ARMv7	• Astra Linux Special Edition «Новороссийск». • 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 4. Raspbian.
ARMv8	• Nvidia Jetson tx2. • Raspberry PI 4. Ubuntu 18.04. • Ubuntu Desktop 18.04.5 LTS. • Ubuntu Desktop 20.04 LTS.

Примечание. Также возможна работа программы ViPNet Client 4U for Linux на менее производительных устройствах. При необходимости гарантированной поддержки менее производительного устройства обратитесь в ИнфоТеКС (на стр. 9).

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

Требования к корпоративной сети

Для использования программы ViPNet Client 4U for Linux требуется, чтобы в организации существовала сеть ViPNet, управление которой осуществляется с помощью программного обеспечения ViPNet Administrator (см. глоссарий, стр. 41) версии 4.6.4 и выше, и была соответствующая лицензия.

Список поддерживаемых внешних устройств

Программа ViPNet Client 4U for Linux поддерживает аутентификацию с помощью следующих внешних устройств:

Таблица 4. 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)
	JaCarta ГОСТ(JC101-2 v2.0)
«Актив»	Рутокен ЭЦП 2.0 (2100)
	Рутокен PKI (1800)
	Рутокен ЭЦП 2.0 (2000)
	Рутокен ЭЦП 2.0 (3000)
	Рутокен Lite (1000)
	Рутокен ЭЦП

Новые возможности версии 4.12

Ниже представлен краткий обзор изменений и новых возможностей программы ViPNet Client 4U for Linux версии 4.12 по сравнению с версией 4.11. Информация об изменениях в предыдущих версиях приведена в приложении История версий (на стр. 37).

Исправление ошибок

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

Комплект поставки

Комплект поставки программы ViPNet Client 4U for Linux включает следующее:

- 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 и решениях ViPNet, распространенные вопросы и другая полезная информация собраны 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.

  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

Защищенная сеть ViPNet

Программа ViPNet Client 4U for Linux предназначена для использования в сети ViPNet. Сеть ViPNet представляет собой виртуальную защищенную сеть, которая может быть развернута поверх локальных или глобальных сетей любой структуры. В отличие от многих популярных VPN-решений, технология ViPNet обеспечивает защищенное взаимодействие между сетевыми узлами (см. глоссарий, стр. 42) по схеме «клиент-клиент».

Защита информации в сети ViPNet осуществляется с помощью специального программного обеспечения, которое шифрует соединения между сетевыми узлами. Для шифрования трафика используются симметричные ключи (см. глоссарий, стр. 43), которые создаются централизованно.

Для управления защищенной сетью ViPNet предназначен программный комплекс ViPNet Administrator (см. глоссарий, стр. 41). С помощью этого программного комплекса администратор сети ViPNet создает сетевые узлы и связи между ними, настраивает параметры отдельных узлов и создает дистрибутивы ключей (см. глоссарий, стр. 41) для каждого узла.

Сетевые узлы ViPNet делятся на два типа:

- Клиент (ViPNet-клиент) (см. глоссарий, стр. 41) — предназначен для работы пользователей сети ViPNet. Сетевой узел ViPNet Client 4U for Linux является клиентом.
- Координатор (ViPNet-координатор) (см. глоссарий, стр. 42) — сервер сети ViPNet.

Также сеть ViPNet может включать открытые узлы (компьютеры без программного обеспечения ViPNet), соединения которых через интернет или другие публичные сети защищаются координаторами ViPNet с помощью туннелирования (см. глоссарий, стр. 43).

Компьютер с программой ViPNet Client 4U for Linux в сети ViPNet

Программа ViPNet Client 4U for Linux позволяет вам организовать доступ к узлам защищенной сети ViPNet или узлам, которые туннелируются координаторами ViPNet (см. глоссарий, стр. 43). Если вы работаете в компании, где развернута сеть ViPNet, вы можете получить доступ к узлам этой сети, только если ваш компьютер также защищен средствами ViPNet.

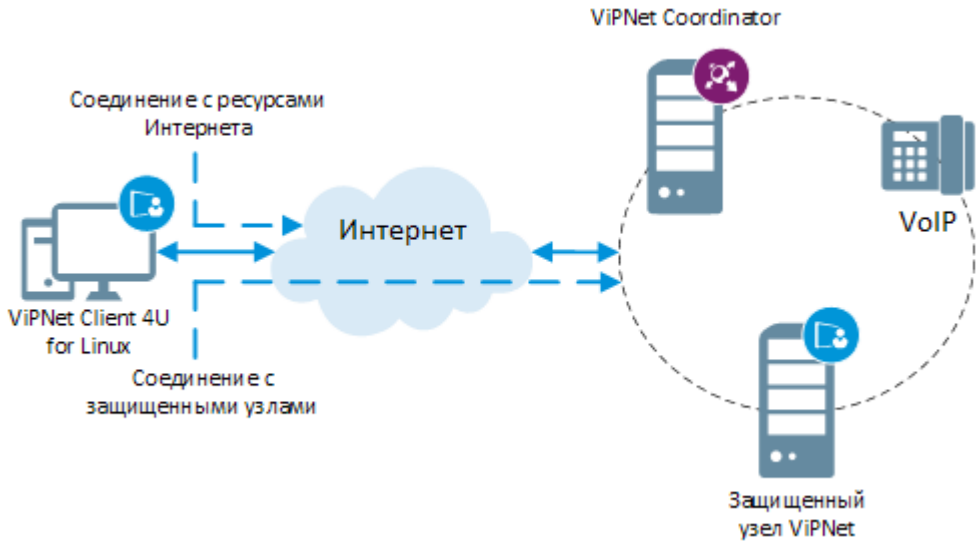

Рисунок 1. Работа ViPNet Client 4U for Linux с защищенными узлами ViPNet и ресурсами Интернета

После установки на ваш компьютер программы ViPNet Client 4U for Linux вы можете пользоваться информационными ресурсами и сервисами на узлах ViPNet: веб-порталом, почтовым сервером, IP-телефонией и так далее.

На компьютере с программой ViPNet Client 4U for Linux вы можете обращаться к узлам защищенной сети не только по IP-адресам, но и по служебным именам ViPNet (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`.

Для чего нужно устанавливать ключи

Перед использованием программы ViPNet Client 4U for Linux необходимо установить ключи сетевого узла ViPNet. С помощью ключей узла осуществляется шифрование IP-трафика при соединениях с другими узлами защищенной сети. Без этого работа ViPNet Client 4U for Linux в защищенной сети будет невозможна.

Установка ключей (на стр. 25, на стр. 15) на компьютер выполняется с помощью дистрибутива ключей и пароля к нему. В дистрибутиве ключей также содержится информация о роли, назначенной вашему узлу администратором сети ViPNet. Узлу должна быть назначена роль (см. глоссарий, стр. 42) «Client for Linux» (0091), иначе работа программы ViPNet Client 4U for Linux на узле будет невозможна.

Дистрибутив ключей вы можете получить лично или другим доверенным способом у администратора сети ViPNet в виде файла дистрибутива ключей (`*.dst`) и пароля к нему. Если для вас выбран способ аутентификации в программе ViPNet Client 4U for Linux с помощью персонального ключа на внешнем устройстве (см. Способы аутентификации в программе ViPNet Client 4U for Linux на стр. 13), то администратор сети ViPNet также передаст вам внешнее устройство и ПИН-код к нему.

Пароль к дистрибутиву ключей требуется вводить в процессе установки ключей на компьютер, а также при подключении к сети ViPNet после запуска программы ViPNet Client 4U for Linux в зависимости от уровня полномочий, назначенного вам администратором сети ViPNet (см. Запуск и завершение работы на стр. 29, Запуск и завершение работы на стр. 18).

Примечание. 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 программе ViPNet Client 4U for Linux

Программа ViPNet Client 4U for Linux 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-код.

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 for Linux».

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

Подключать к компьютеру внешнее устройство с персональным ключом и вводить ПИН-код к нему в программе ViPNet Client 4U for Linux потребуется при установке ключей, а также при каждом подключении к сети ViPNet (при этом вводить ПИН-код потребуется, 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 программой ViPNet Client 4U for Linux вы можете самостоятельно сменить способ аутентификации на аутентификацию по персональному ключу на внешнем устройстве (см. Смена способа аутентификации на стр. 20).

Работа с программой ViPNet Client 4U for Linux в командной строке

Установка ключей

Чтобы установить ключи ViPNet на компьютер с программой ViPNet Client 4U for Linux, выполните следующие действия:

1. Если в программе ViPNet Client 4U for Linux будет использоваться аутентификация пользователя по персональному ключу на внешнем устройстве (см. Способы аутентификации в программе ViPNet Client 4U for Linux на стр. 13), подключите внешнее устройство к компьютеру.
2. Войдите в консоль ОС Linux с правами пользователя.
3. Выполните команду:

   ```
   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-кода от внешнего устройства с персональным ключом пользователя (если используется соответствующий способ аутентификации). Чтобы снизить риск компрометации ПИН-кода, применять параметр `--pin` не рекомендуется, так как при этом ПИН-код отображается в консоли в явном виде. Вводите ПИН-код по запросу во время выполнения команды.
   - `--psw` — параметр для указания пароля от дистрибутива ключей. 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. При использовании аутентификации пользователя по персональному ключу на внешнем устройстве пароль от дистрибутива ключей потребуется ввести, если администратор сети ViPNet назначил вам максимальный или средний уровень полномочий. Если вы обладаете минимальным уровнем полномочий, вводить пароль при установке ключей не потребуется.

   - `--token-select` — параметр для поиска (по любой части названия) и выбора внешнего устройства, если используется соответствующий способ аутентификации и 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` — параметр для отключения ежеминутной проверки работоспособности программы ViPNet Client 4U for Linux и ее автоматического запуска в случае нештатного завершения работы. Для более надежной работы программы ViPNet Client 4U for Linux применять данный параметр не рекомендуется.
- `--no-autostart` — параметр для отключения автоматического запуска программы ViPNet Client 4U for Linux и подключения к сети ViPNet после авторизации пользователя в ОС. Для более надежной работы программы ViPNet Client 4U for Linux применять данный параметр не рекомендуется.

Примечание. Автоматический запуск программы и подключение к сети ViPNet после авторизации пользователя в ОС также не выполняются, если пользователь обладает минимальными полномочиями в программе ViPNet Client 4U for Linux и если используется аутентификация пользователя по персональному ключу на внешнем устройстве.

- `--no-start` — параметр для отключения автоматического подключения к сети ViPNet после установки ключей.

4. Если не был указан параметр `--token-select` или по результатам поиска найдено несколько внешних устройств, введите номер нужного внешнего устройства и нажмите клавишу **Enter**.
5. Если ПИН-код не был указан в команде, при появлении соответствующего запроса введите ПИН-код от внешнего устройства и нажмите клавишу **Enter**.
6. Если пароль не был указан в команде, при появлении соответствующего запроса введите пароль от дистрибутива ключей и нажмите клавишу **Enter**.
7. Подождите, пока ключи будут установлены. Выполнение команды может занять некоторое время.

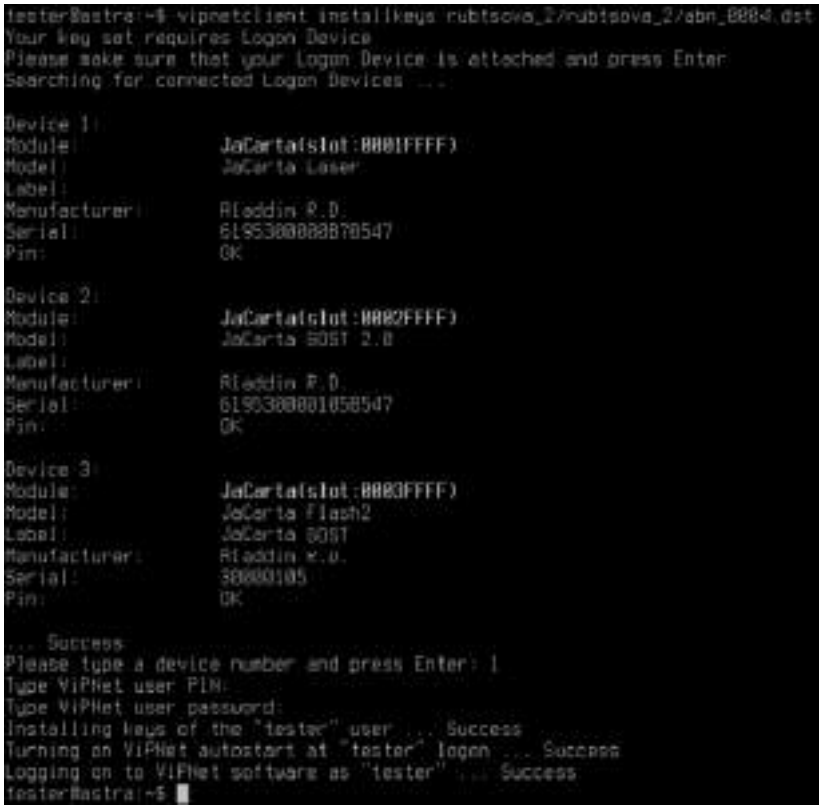

Рисунок 2. Установка дистрибутива ключей при аутентификации с помощью внешнего устройства

Примечание. Если в файле дистрибутива ключей будут выявлены ошибки или этот файл не будет удовлетворять требованиям к дистрибутиву ключей для программы ViPNet Client 4U for Linux, появится сообщение с информацией об этом. Обратитесь к администратору сети ViPNet для устранения причины ошибок, а затем установите новый дистрибутив ключей.

В результате ключи будут установлены в рабочий каталог ViPNet. После установки ключей подключение к сети ViPNet будет выполнено автоматически. Если при установке ключей был указан параметр `--no-start` или используется аутентификация пользователя по персональному ключу на внешнем устройстве, включите VPN-соединение вручную (см. Запуск и завершение работы на стр. 18).

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. 42). 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 по каким-либо причинам не могут быть переданы по сети, вы можете обновить их вручную. Также обновления ключей может потребоваться устанавливать вручную, если произошла смена мастер-ключей в сети. Для этого выполните следующие действия:

1 Удалите ключи, установленные на компьютере (см. Удаление ключей на стр. 18).

2 Установите новые ключи (см. Установка ключей на стр. 15).

Ключи будут обновлены, и вы сможете продолжить работу в сети ViPNet.

Удаление ключей

При необходимости вы можете удалить ключи, установленные на компьютере. Это может понадобиться, например, при обновлении ключей (см. Обновление ключей на стр. 28) или в случае передачи компьютера для работы другому пользователю ViPNet.

Чтобы удалить установленные на компьютере ключи, выполните следующие действия:

1 Войдите в консоль ОС Linux с правами пользователя.

2 Если включено VPN-соединение, выключите его с помощью команды:

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

3 Удалите ключи с помощью команды:

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

4 При появлении запроса подтвердить удаление ключей введите символ `Y` и нажмите клавишу **Enter**.

Запуск и завершение работы

Запуск всех компонентов программы ViPNet Client 4U for Linux и подключение к сети ViPNet выполняются автоматически после установки ключей и при каждой авторизации в операционной системе пользователя, выполнившего установку ключей.

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 программе ViPNet Client 4U for Linux на стр. 13) и внешнее устройство не подключено к компьютеру.
- Если при установке ключей был указан параметр `--no-autostart`.

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

1 Если в программе ViPNet Client 4U for Linux используется аутентификация пользователя по персональному ключу на внешнем устройстве, подключите внешнее устройство к компьютеру.

2 Войдите в консоль ОС Linux с правами пользователя.

3 Выполните команду:

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

где:

- `--pin` — параметр для указания ПИН-кода от внешнего устройства с персональным ключом пользователя (если используется соответствующий способ аутентификации). ПИН-код требуется вводить только при минимальном уровне полномочий пользователя. Чтобы снизить риск компрометации ПИН-кода, применять параметр `--pin` не рекомендуется, так как при этом ПИН-код отображается в консоли в явном виде. Вводите ПИН-код по запросу во время выполнения команды.
- `--psw` — параметр для указания пароля от дистрибутива ключей (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.
- `--no-failprotect` — параметр для отключения ежеминутной проверки работоспособности программы ViPNet Client 4U for Linux и ее автоматического запуска в случае нештатного завершения работы. Для более надежной работы программы ViPNet Client 4U for Linux применять данный параметр не рекомендуется.

4 Если вы обладаете минимальными полномочиями в программе ViPNet Client 4U for Linux, появится сообщение с запросом ввести ПИН-код от внешнего устройства или пароль от дистрибутива ключей (в зависимости от используемого способа аутентификации). Введите ПИН-код или пароль и нажмите клавишу **Enter**.

5 Подождите, пока VPN-соединение будет включено. Выполнение команды может занять некоторое время.

Чтобы остановить программу ViPNet Client 4U for Linux и выключить VPN-соединение, выполните команду:

```
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 включении защищенного соединения с сетью ViPNet (см. Запуск и завершение работы на стр. 18) программой ViPNet Client 4U for Linux автоматически будет проверена связь с координатором, являющимся сервером соединений (см. глоссарий, стр. 42) для данного клиента. Если координатор доступен, то защищенное соединение с сетью ViPNet считается установленным.

Если же координатор недоступен, взаимодействие с другими узлами сети ViPNet будет 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. Чтобы проверить связь с координатором:

1 Войдите в консоль ОС Linux с правами пользователя.

2 Выполните команду:

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

3 Дождитесь результата выполнения команды.

Если связь с координатором отсутствует, повторите попытку через некоторое время.

Примечание. Также вы можете проверить связь с другими узлами с помощью команды:
`user@host:~$ vipnetclient debug --ping <идентификатор_узла_ViPNet>`

Смена способа аутентификации

В программе ViPNet Client 4U for Linux вы можете сменить способ аутентификации (см. Способы аутентификации в программе ViPNet Client 4U for Linux на стр. 13) — с аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве. Для этого:

1 Подключите внешнее устройство к компьютеру.

2 Войдите в консоль ОС Linux с правами пользователя.

3 В консоли выполните команду:

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

где:

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

4 Если не был указан параметр `--token-select` или по результатам поиска найдено несколько внешних устройств, введите номер нужного внешнего устройства и нажмите клавишу **Enter**.

5 Если ПИН-код не был указан в команде, при появлении соответствующего запроса введите ПИН-код для внешнего устройства и нажмите клавишу **Enter**.

6 Подождите, пока персональный ключ будет записан на внешнее устройство. При извлечении внешнего устройства до завершения операции способ аутентификации не будет изменен.

Рисунок 3. Способ аутентификации успешно изменен

Просмотр списка защищенных узлов

Вы можете просмотреть, с какими другими защищенными узлами сети ViPNet (клиентами и координаторами) связан ваш узел. Для этого выполните следующие действия:

1 Войдите в консоль ОС Linux с правами пользователя.

2 Выполните команду:

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

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

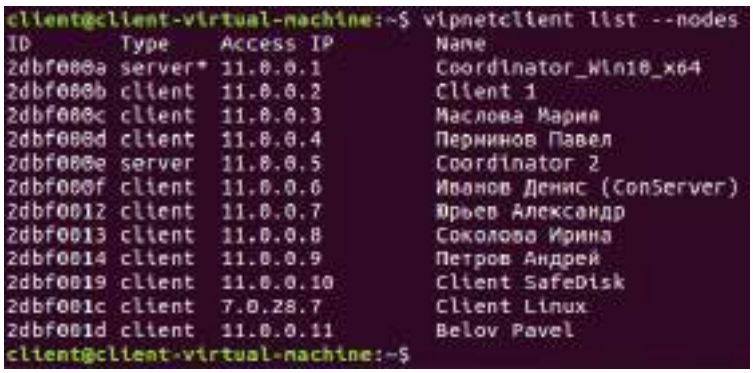

Рисунок 4. Просмотр списка защищенных узлов

3 Чтобы просмотреть подробную информацию об узле из списка, выполните команду:

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

> **Внимание!** Данная команда выполняется только при включенном VPN-соединении (см. Запуск и завершение работы на стр. 18).

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.

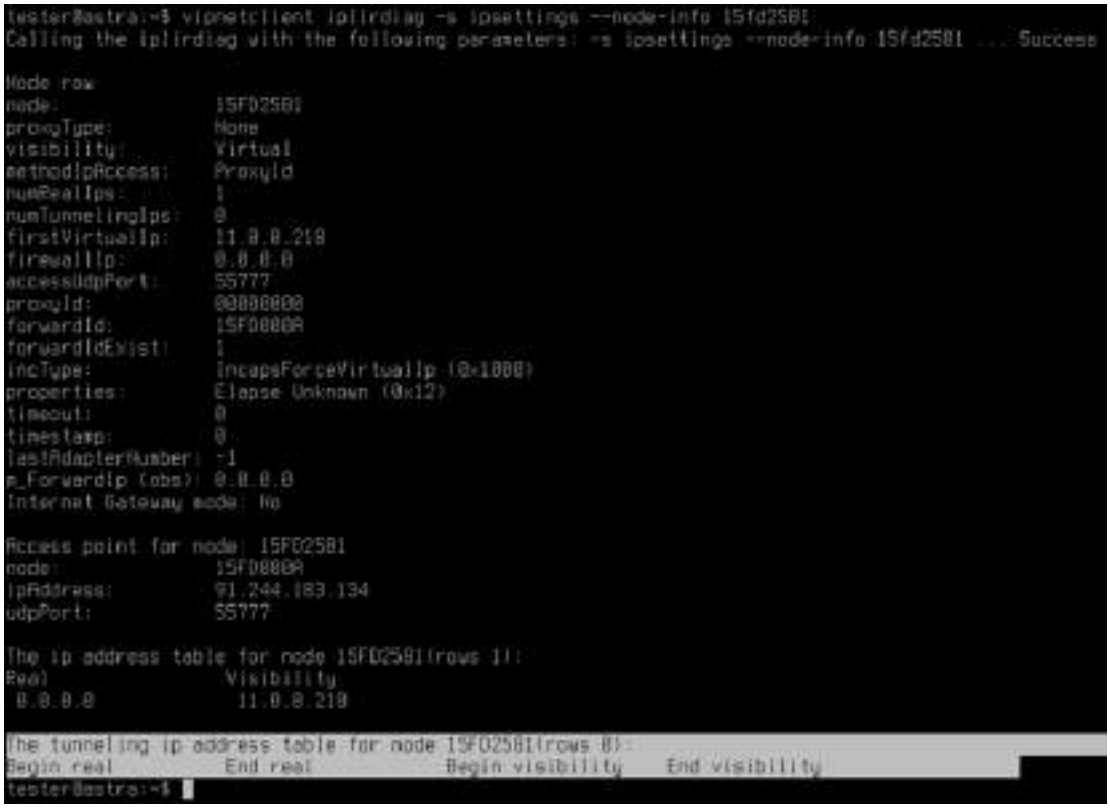

Рисунок 5. Просмотр информации о защищенном узле

Просмотр информации о своем узле и версии программы ViPNet Client 4U for Linux

Вы можете просмотреть информацию о своем сетевом узле ViPNet и версию программы ViPNet Client 4U for Linux, установленную на компьютере. Для этого выполните следующие действия:

1 Войдите в консоль ОС Linux с правами пользователя.

2 Выполните команду:

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

В результате отобразится версия программы ViPNet Client 4U for Linux и информация о вашем сетевом узле (его имя и идентификатор, информация о сети ViPNet и о лицензии, ваш уровень полномочий в программе ViPNet Client 4U for Linux, идентификаторы ролей узла, уровень журналирования событий и другие параметры работы программы ViPNet Client 4U for Linux).

Примечание. Информацию о версии программы ViPNet Client 4U for Linux вы также можете просмотреть с помощью команды:
`user@host:~$ vipnetclient --version`

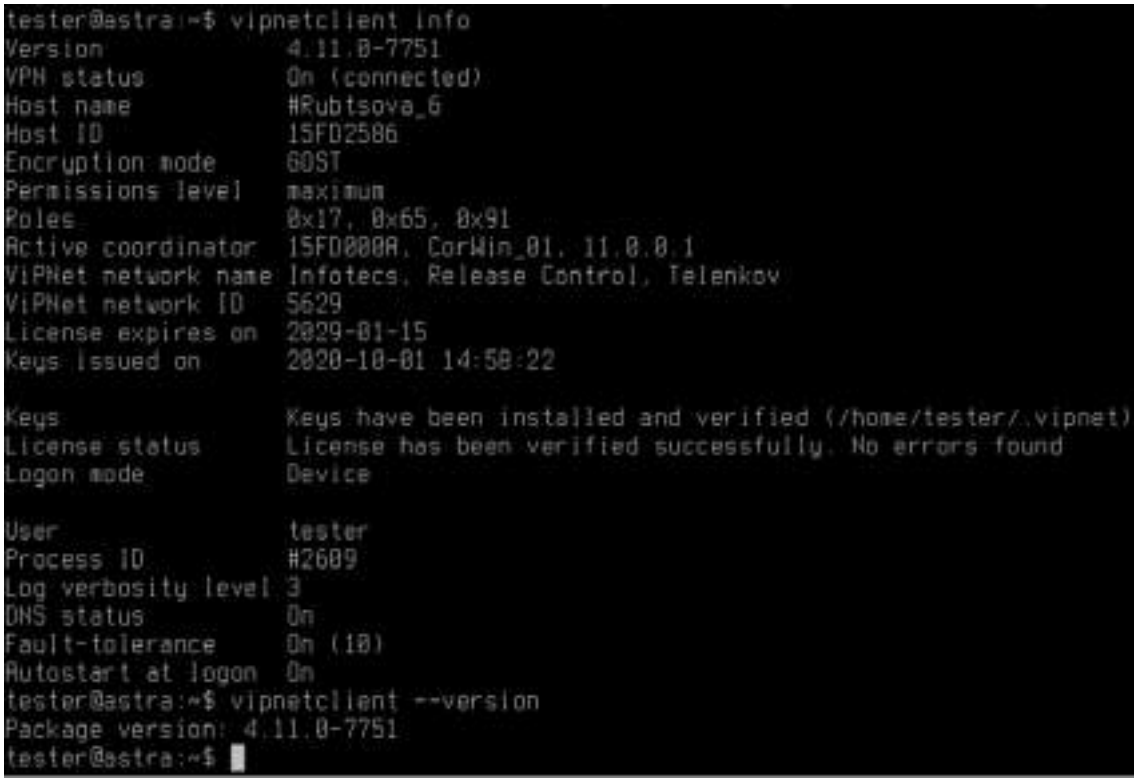

Рисунок 6. Просмотр информации о своем узле и версии программы ViPNet Client 4U for Linux

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

Если разница во времени на клиенте с программой ViPNet Client 4U for Linux 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.

Обращение в службу технической поддержки

В случае возникновения ошибок в работе программы ViPNet Client 4U for Linux вы можете обратиться в ИнфоТеКС. Для этого выполните следующие действия:

1. Войдите в консоль ОС Linux с правами пользователя.
2. Создайте отчет со служебной информацией о работе программы ViPNet Client 4U for Linux. Для этого выполните команду:

   ```
   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 укажите 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`.
3. Подождите, пока будет создан отчет о работе программы ViPNet Client 4U for Linux. Выполнение команды может занять некоторое время.

   В результате будет создан архив с отчетом о работе программы ViPNet Client 4U for Linux в формате ZIP.
4. Создайте электронное письмо с описанием проблемы и обстоятельствами ее возникновения. Прикрепите к письму архив с отчетом о работе программы ViPNet Client 4U for Linux.
5. Отправьте письмо в ИнфоТеКС (на стр. 9).

Работа с программой ViPNet Client 4U for Linux в графическом интерфейсе

Установка ключей

Чтобы установить дистрибутив ключей на компьютер с программой ViPNet Client 4U for Linux, выполните следующие действия:

Примечание. Вы можете сразу перейти к установке дистрибутива ключей, дважды щелкнув файл `*.dst` в файловом менеджере. В результате автоматически откроется окно **Установка ключей**. Если в программе ViPNet Client 4U for Linux уже установлен другой набор ключей, то отобразится уведомление о невозможности установить новый дистрибутив ключей. В этом случае следуйте указаниям раздела Обновление ключей (на стр. 28).

---

1. Если в программе ViPNet Client 4U for Linux будет использоваться аутентификация пользователя по персональному ключу на внешнем устройстве (см. Способы аутентификации в программе ViPNet Client 4U for Linux на стр. 13), подключите внешнее устройство к компьютеру.
2. Откройте программу ViPNet Client 4U for Linux. Для этого выполните одно из действий:
   - Войдите в консоль ОС Linux с правами пользователя и выполните следующую команду:
     ```
     user@host:~$ vipnetclient-gui
     ```
   - В списке установленных на компьютере программ щелкните значок ViPNet Client 4U for Linux  .
3. В главном окне программы ViPNet Client 4U for Linux нажмите кнопку **Добавить ключи**.

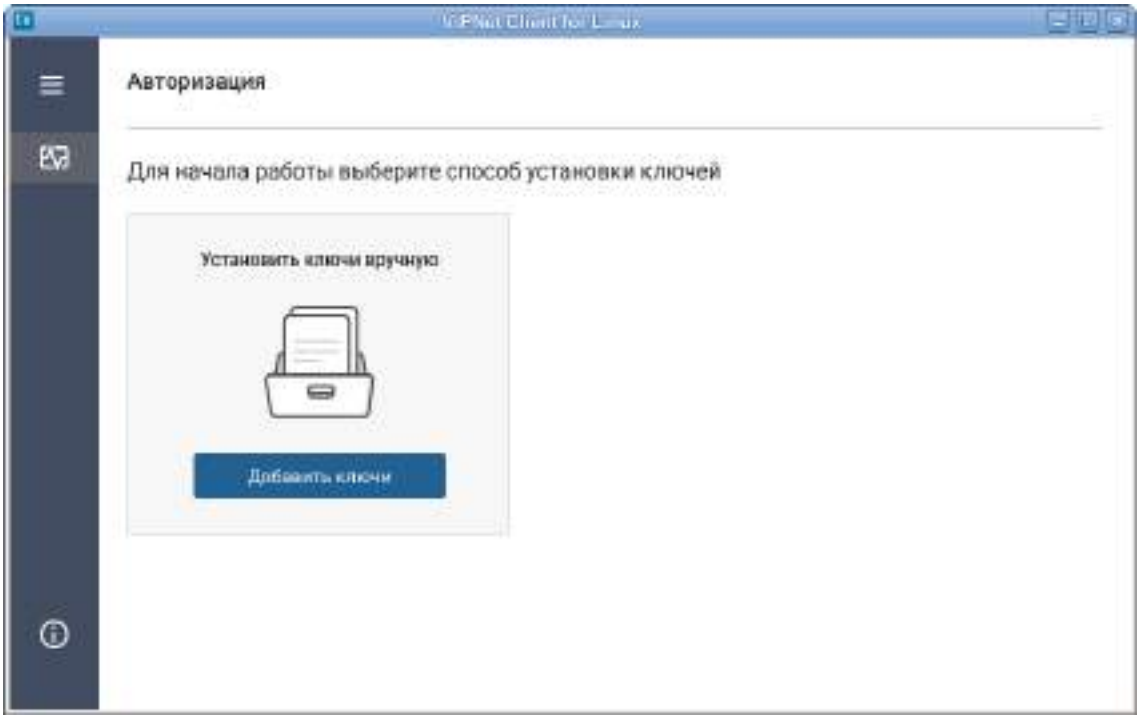

Рисунок 7. Установка дистрибутива ключей

4 В открывшемся окне выберите файл дистрибутива ключей (`*.dst`). Выбранный файл будет проверен на наличие ошибок.

Если в файле будут выявлены ошибки или этот файл не будет удовлетворять требованиям к дистрибутиву ключей для программы ViPNet Client 4U for Linux, появится окно с информацией об этом. Обратитесь к администратору сети ViPNet для устранения причины ошибок, а затем установите новый дистрибутив ключей.

5 В окне **Установка ключей** отобразится информация о дистрибутиве ключей.

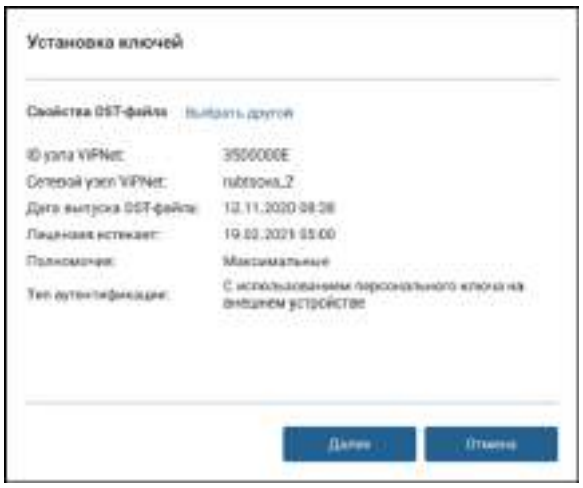

Рисунок 8. Просмотр информации о дистрибутиве ключей

В зависимости от способа аутентификации в программе ViPNet Client 4U for Linux выполните одно из действий:

- При аутентификации по паролю — введите пароль к дистрибутиву ключей, который вам сообщил администратор сети, и нажмите кнопку **Далее**.

Примечание. При использовании аутентификации пользователя по персональному ключу на внешнем устройстве пароль от дистрибутива ключей потребуется ввести, если администратор сети ViPNet назначил вам максимальный или средний уровень полномочий. Если вы обладаете минимальным уровнем полномочий, вводить пароль при установке ключей не потребуется.

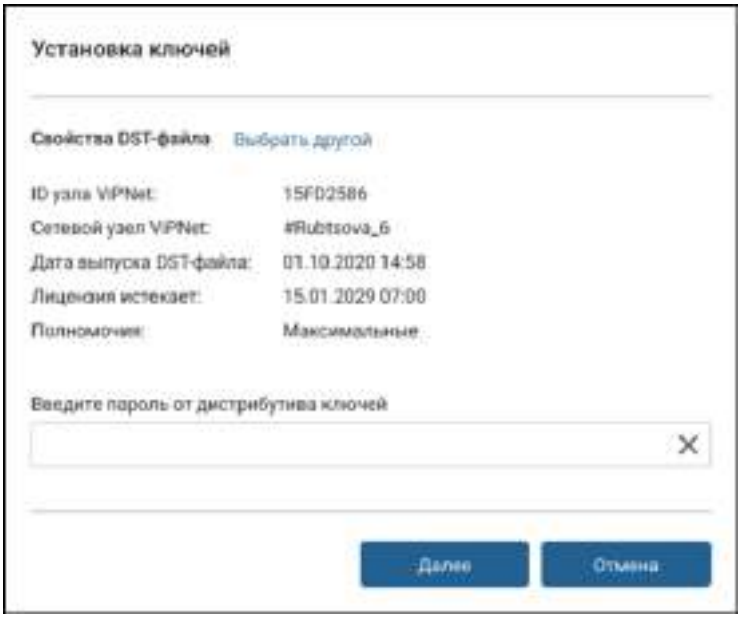

Рисунок 9. Ввод пароля к дистрибутиву ключей

- При аутентификации по персональному ключу на внешнем устройстве:
  - Нажмите кнопку **Далее**.
  - Если к компьютеру подключено несколько устройств, выберите нужное устройство в списке и нажмите кнопку **Далее**.

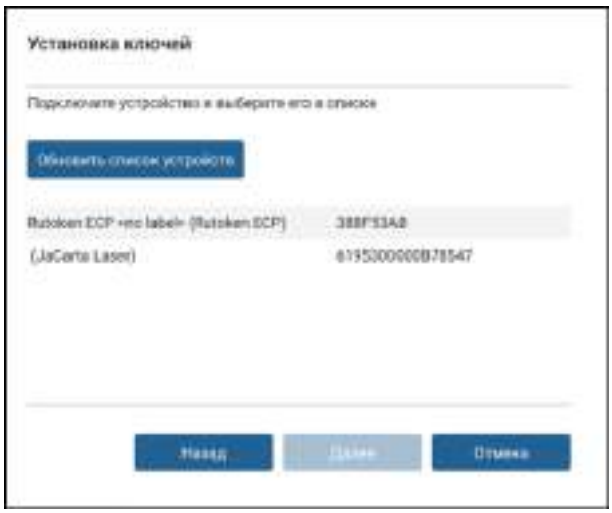

Рисунок 10. Выбор внешнего устройства для аутентификации

- Введите ПИН-код от внешнего устройства и нажмите кнопку **Далее**.

Рисунок 11. Ввод ПИН-кода к внешнему устройству

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

После установки ключей будет автоматически включено VPN-соединение, и вы сможете подключаться к защищенным узлам вашей сети ViPNet. Если используется аутентификация пользователя по персональному ключу на внешнем устройстве, включите VPN-соединение вручную (см. Запуск и завершение работы на стр. 29).

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. 42). 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 по каким-либо причинам не могут быть переданы по сети, вы можете обновить их вручную. Также обновления ключей может потребоваться устанавливать вручную, если произошла смена мастер-ключей в сети. Для этого выполните следующие действия:

1 Удалите ключи, установленные на устройстве.

2 Установите новые ключи (см. Установка ключей на стр. 25).

Ключи будут обновлены, и вы сможете продолжить работу в сети ViPNet.

Удаление ключей

При необходимости вы можете удалить ключи, установленные на компьютере. Это может понадобиться, например, при обновлении ключей (см. Обновление ключей на стр. 28) или же в случае передачи компьютера для работы другому пользователю ViPNet.

Чтобы удалить установленные на компьютере ключи:

1 В главном окне программы ViPNet Client 4U for Linux выключите соединение с сетью ViPNet (см. Запуск и завершение работы на стр. 29).

2 На панели навигации выберите раздел **Профиль** и на панели просмотра нажмите кнопку **Удалить набор ключей**.

Рисунок 12. Удаление ключей

3 В окне с запросом подтвердите удаление ключей.

Запуск и завершение работы

Запуск программы ViPNet Client 4U for Linux и подключение к защищенной сети ViPNet позволяют вам получить доступ к корпоративным ресурсам, обмениваться информацией с пользователями ViPNet и выполнять другие задачи в корпоративной сети.

Для запуска программы ViPNet Client 4U for Linux и подключения к сети ViPNet выполните следующие действия:

1 Если в программе ViPNet Client 4U for Linux используется аутентификация пользователя по персональному ключу на внешнем устройстве (см. Способы аутентификации в программе ViPNet Client 4U for Linux на стр. 13), подключите внешнее устройство к компьютеру.

2 Выполните одно из действий:

- Войдите в консоль ОС Linux с правами пользователя и выполните следующую команду:

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

- o В списке установленных на компьютере программ щелкните значок ViPNet Client 4U for Linux  .

3 В главном окне программы ViPNet Client 4U for Linux нажмите кнопку **Включить**.

4 Если потребуется, то в открывшемся окне введите пароль пользователя ViPNet (пароль от дистрибутива ключей) или ПИН-код от внешнего устройства с персональным ключом и нажмите кнопку **ОК**.

Примечание. Необходимость вводить пароль или ПИН-код определяется уровнем полномочий пользователя, заданным администратором сети ViPNet:

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

---

5 Подождите, пока VPN-соединение будет включено. Это может занять некоторое время.

В результате будет выполнено подключение к защищенной сети ViPNet. При этом будет проверено соединение с координатором текущего клиента (см. Проверка связи с координатором на стр. 31). Если соединение установлено, вы сможете работать с корпоративными ресурсами.

Чтобы завершить работу с сетью ViPNet, в главном окне программы ViPNet Client 4U for Linux нажмите кнопку **Выключить**.

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

Интерфейс программы ViPNet Client 4U for Linux

Главное окно программы ViPNet Client 4U for Linux представлено на следующем рисунке:

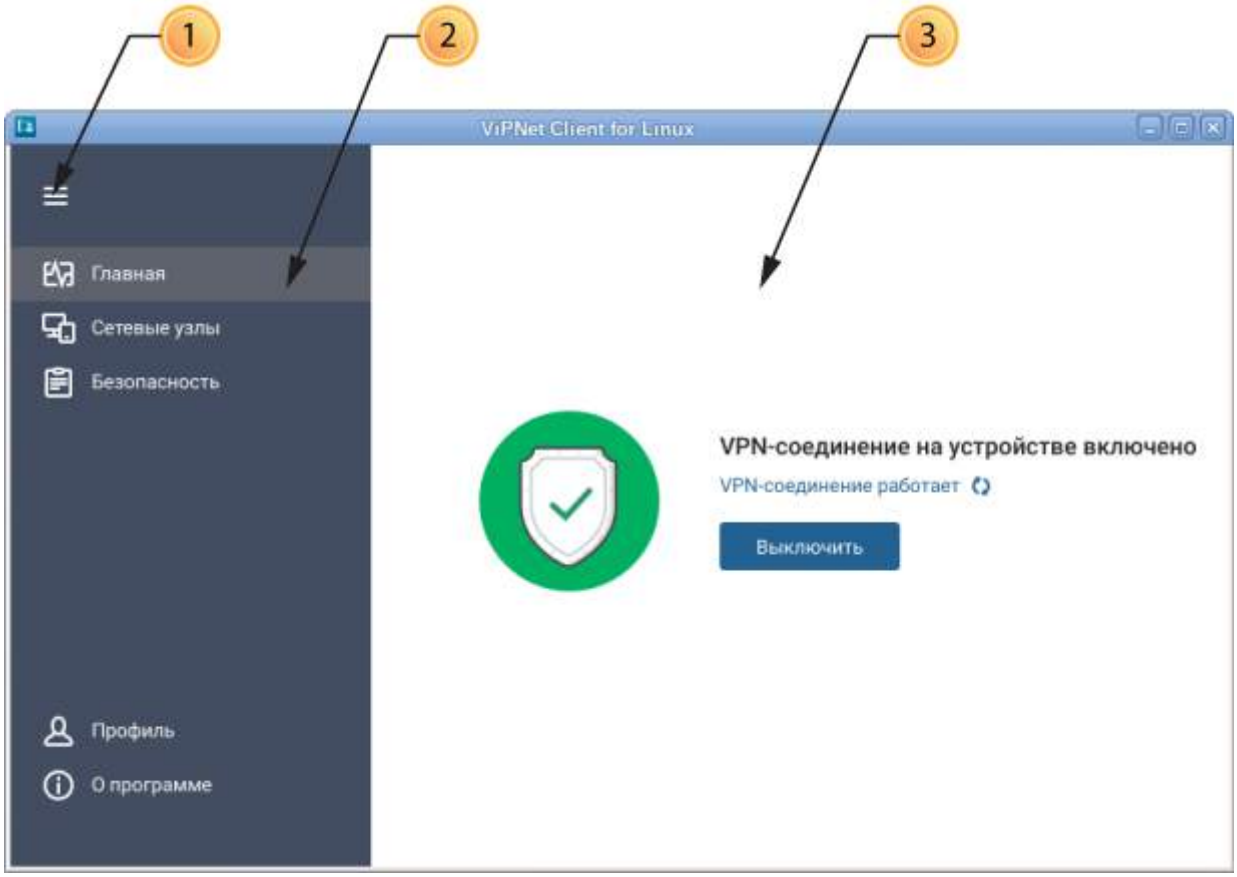

Рисунок 13. Интерфейс программы ViPNet Client 4U for Linux

Цифрами на рисунке обозначены:

1. Кнопка для сворачивания и разворачивания панели навигации. Вы можете сворачивать панель навигации, чтобы выделить в окне программы ViPNet Client 4U for Linux больше места для панели просмотра, например при просмотре списка защищенных узлов (см. Просмотр списка защищенных узлов и поиск узла на стр. 33).
2. Панель навигации. С помощью данной панели вы можете переключаться между разделами программы ViPNet Client 4U for Linux.
3. Панель просмотра. Содержимое панели просмотра зависит от раздела, выбранного на панели навигации.

Проверка связи с координатором

При включении защищенного соединения с сетью ViPNet (см. Запуск и завершение работы на стр. 29) программой ViPNet Client 4U for Linux автоматически будет проверена связь с координатором, являющимся сервером соединений (см. глоссарий, стр. 42) для данного клиента. Если координатор доступен, то защищенное соединение с сетью ViPNet считается установленным. Если же координатор недоступен, взаимодействие с другими узлами сети ViPNet будет 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. Чтобы проверить связь с координатором, в главном окне программы ViPNet Client 4U for Linux нажмите кнопку и дождитесь установления соединения с координатором. Если связь с координатором отсутствует, повторите попытку через некоторое время.

Примечание. Если разница во времени на клиенте с программой ViPNet Client 4U for Linux и координаторе, который является сервером соединений, больше разрешенной на координаторе, взаимодействие между ними невозможно. В этом случае в интерфейсе ViPNet Client 4U for Linux будет отображаться оповещение о разнице во времени и рекомендация перевести часы на компьютере.

Смена способа аутентификации

В программе ViPNet Client 4U for Linux вы можете сменить способ аутентификации (см. Способы аутентификации в программе ViPNet Client 4U for Linux на стр. 13) — с аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве. Для этого:

1. Подключите внешнее устройство к компьютеру.
2. В главном окне программы ViPNet Client 4U for Linux на панели навигации выберите раздел **Профиль** .
3. На панели просмотра щелкните ссылку **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 кнопку **Далее**.

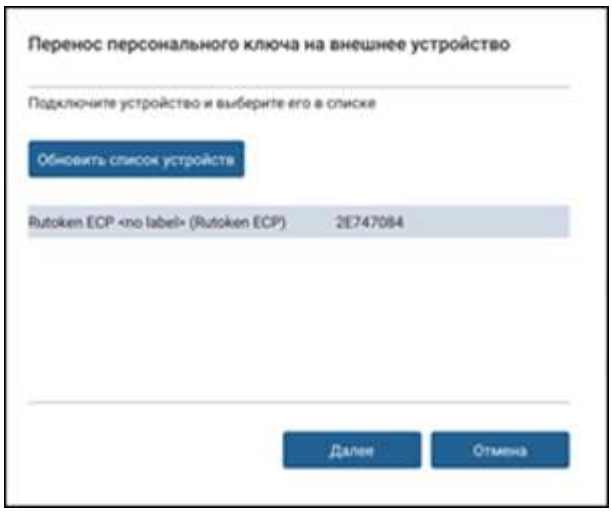

Рисунок 14. Выбор внешнего устройства для переноса персонального ключа

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

Просмотр информации о своем сетевом узле и версии программы ViPNet Client 4U for Linux

Вы можете просмотреть информацию о своем сетевом узле ViPNet и версию программы ViPNet Client 4U for Linux, установленную на компьютере. Для этого выполните следующие действия:

1. В главном окне программы ViPNet Client 4U for Linux на панели навигации выберите раздел **Профиль**  . На панели просмотра вы увидите следующую информацию:
   - Имя вашего сетевого узла.
   - Идентификатор вашего сетевого узла.
   - Номер сети ViPNet, в которую входит ваш узел.
   - Назначенные вашему узлу роли.
   - Ваш уровень полномочий.
   - Дата выпуска дистрибутива ключей.
   - Срок действия лицензии на использование программы ViPNet Client 4U for Linux (если она имеет ограниченный срок действия).
   - Способ аутентификации в программе ViPNet Client 4U for Linux.
2. Для просмотра номера версии программы ViPNet Client 4U for Linux на панели навигации выберите раздел **О программе**  . Кроме номера версии, на панели просмотра также отобразится контактная информация для связи с представителями компании ИнфоТеКС.

Просмотр списка защищенных узлов и поиск узла

Вы можете просмотреть, с какими другими защищенными узлами сети ViPNet (клиентами и координаторами) связан ваш узел. Также в свойствах координаторов вы можете просмотреть туннелируемые координатором IP-адреса открытых узлов (см. глоссарий, стр. 42), с которыми вы можете взаимодействовать в рамках сети ViPNet.

Чтобы просмотреть список защищенных узлов сети ViPNet, связанных с вашим узлом, выполните следующие действия:

1. В главном окне программы ViPNet Client 4U for Linux на панели навигации выберите раздел **Сетевые узлы**  .
2. Подождите завершения выполнения операции. Это может занять некоторое время.

На панели просмотра отобразится список защищенных узлов, с которыми ваш узел может взаимодействовать в рамках сети ViPNet.

3 Чтобы найти определенный узел, на панели просмотра в поле поиска начните вводить имя или идентификатор нужного узла. Отобразятся все узлы, отвечающие заданным критериям.

4 Чтобы отобразить только список координаторов, в списке **Все узлы** выберите **Координаторы**.

5 Чтобы просмотреть подробную информацию об узле, выберите его в списке узлов. Справа появится панель информации об узле, где вы увидите идентификатор узла и его IP-адрес видимости. Для координаторов также отображаются туннелируемые ими IP-адреса открытых узлов.

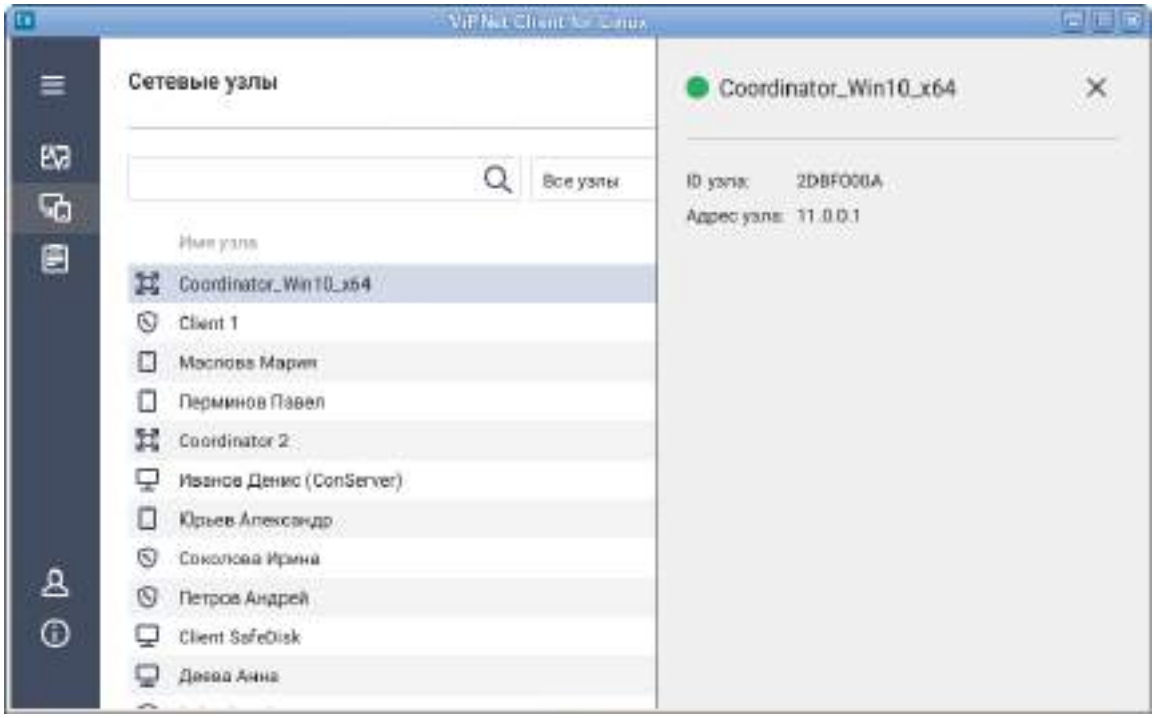

Рисунок 15. Просмотр информации о защищенном узле

Контроль целостности и работоспособности

В рамках эксплуатации программы ViPNet Client 4U for Linux системному администратору, администратору безопасности или самому пользователю рекомендуется выполнять следующие проверки программы:

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

Для проведения проверки целостности и работоспособности выполните следующие действия:

1 В главном окне программы ViPNet Client 4U for Linux на панели навигации выберите раздел **Безопасность** и на панели просмотра нажмите кнопку **Начать проверку**.

2 Дождитесь завершения проверки, это может занять несколько минут. Результат проверки будет отображен на панели просмотра.

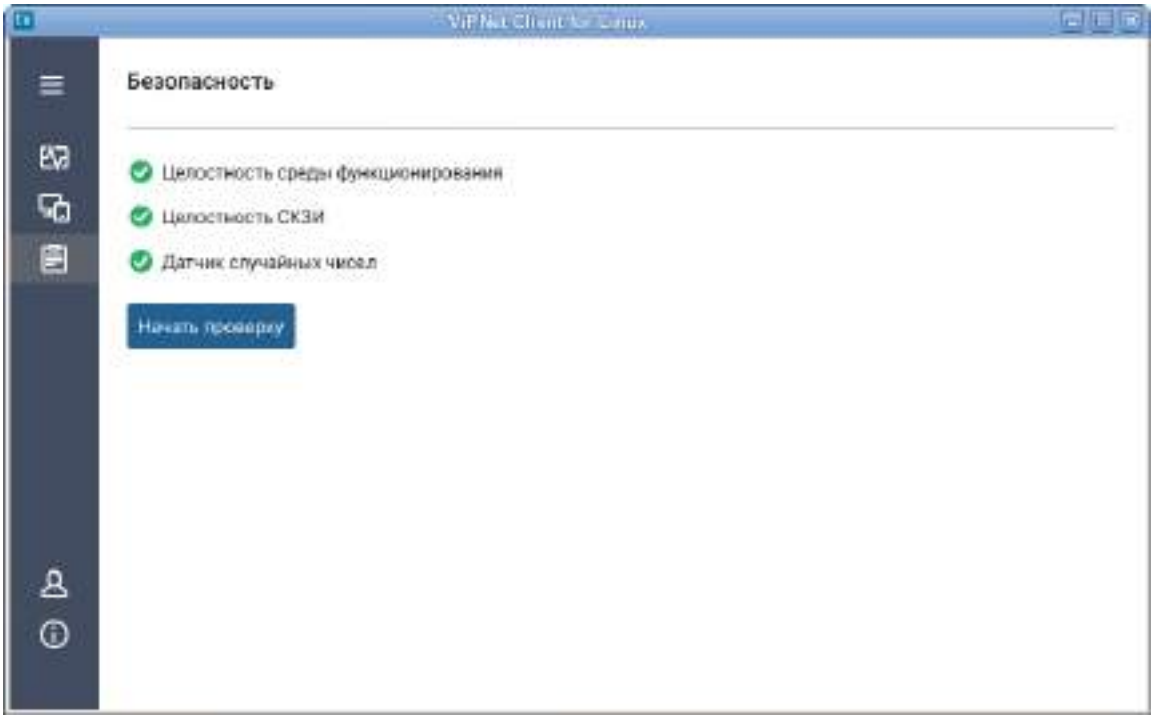

Рисунок 16. Просмотр результатов проверки целостности и работоспособности

В случае нарушения целостности или при неработоспособности компонентов программы ViPNet Client 4U for Linux, 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 программы ViPNet Client 4U for Linux вы можете обратиться в ИнфоТеКС. Для этого выполните следующие действия:

1 В главном окне программы ViPNet Client 4U for Linux на панели навигации выберите раздел **О программе**.

2 Нажмите кнопку **Создать отчет об ошибке**.

3 В открывшемся окне опишите проблему и обстоятельства ее возникновения и с помощью кнопки **Обзор** укажите папку для сохранения отчета со служебной информацией о работе программы ViPNet Client 4U for Linux. Затем нажмите кнопку **Сохранить**.

4 Подождите, пока будет создан отчет о работе программы ViPNet Client 4U for Linux, это может занять некоторое время.

   В результате будет создан архив с отчетом о работе программы ViPNet Client 4U for Linux в формате ZIP.

5 Создайте электронное письмо и прикрепите к нему архив с отчетом о работе программы ViPNet Client 4U for Linux.

6 Отправьте письмо в ИнфоТеКС (на стр. 9).

История версий

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

Новые возможности версии 4.11

Ниже представлен краткий обзор изменений и новых возможностей программы ViPNet Client 4U for Linux версии 4.11 по сравнению с версией 4.10.

Аутентификация с помощью внешних устройств

Раньше в программе ViPNet Client 4U for Linux использовалась только однофакторная аутентификация пользователя по паролю. В новой версии программы ViPNet Client 4U for Linux реализована двухфакторная аутентификация пользователя с помощью персонального ключа на внешнем устройстве и ПИН-кода к нему (см. Способы аутентификации в программе ViPNet Client 4U for Linux на стр. 13). Способ аутентификации выбирает администратор сети ViPNet при создании дистрибутива ключей.

Новые возможности версии 4.10

Ниже представлен краткий обзор изменений и новых возможностей программы ViPNet Client 4U for Linux версии 4.10 по сравнению с версией 4.9.

- **Увеличение производительности**

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

- **Исправление ошибок**

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

Новые возможности версии 4.9

Ниже представлен краткий обзор изменений и новых возможностей программы ViPNet Client 4U for Linux версии 4.9 по сравнению с версией 4.8.

Поддержка ViPNet Connect for Linux

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

Новые возможности версии 4.8

Ниже представлен краткий обзор изменений и новых возможностей программы ViPNet Client 4U for Linux версии 4.8 по сравнению с версией 4.6.

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

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

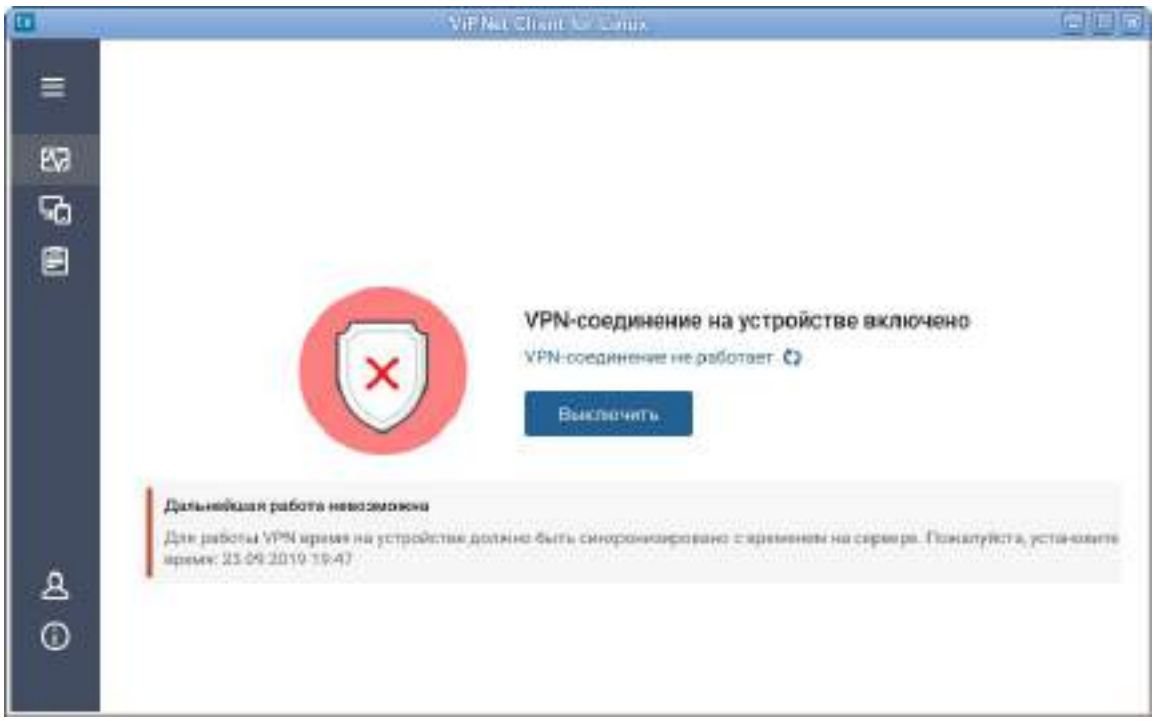

Рисунок 17. Уведомление о разнице во времени с координатором

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

  В новой версии программы ViPNet Client 4U for Linux 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 for Linux, о неудавшемся обновлении программы ViPNet Client 4U for Linux.

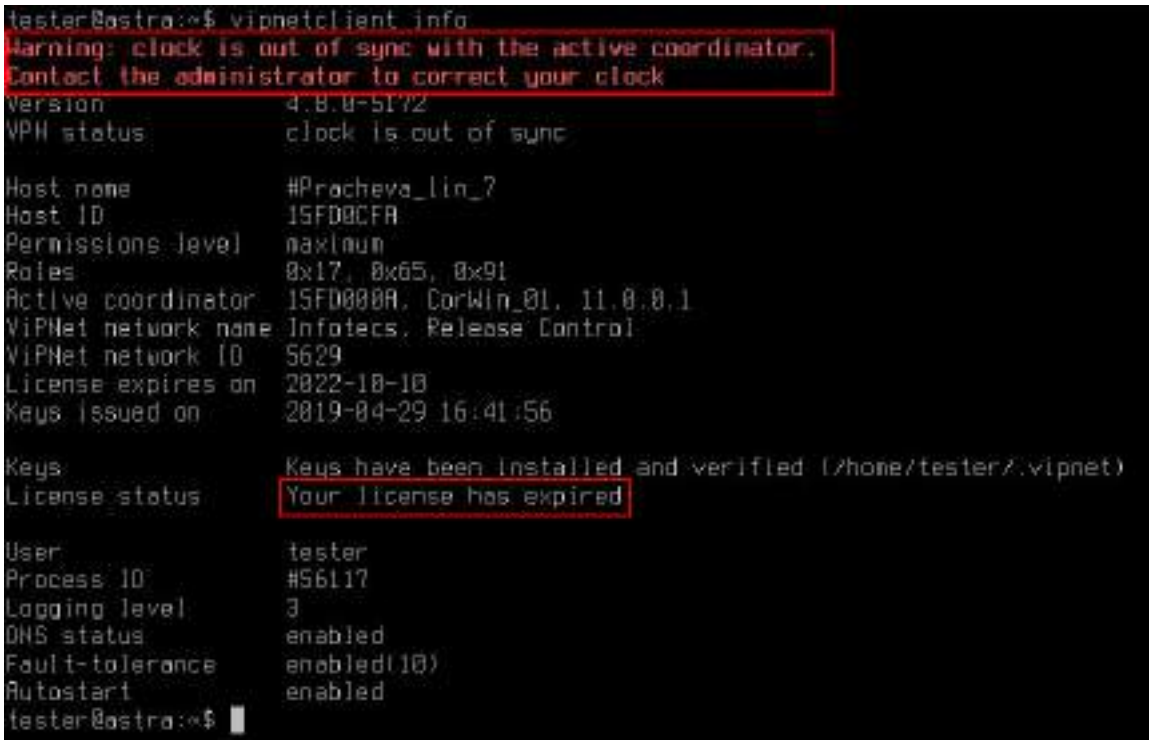

Рисунок 18. Уведомления о разнице во времени с координатором и просроченной лицензии

- **Предупреждение об установке неподписанной сборки программы ViPNet Client 4U for Linux 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 for Linux. Если вы установите неподписанный пакет программы ViPNet Client 4U for Linux, то при включении мандатного контроля программа работать не будет. Во время установки неподписанного пакета программы ViPNet Client 4U for Linux отображается уведомление об этом.

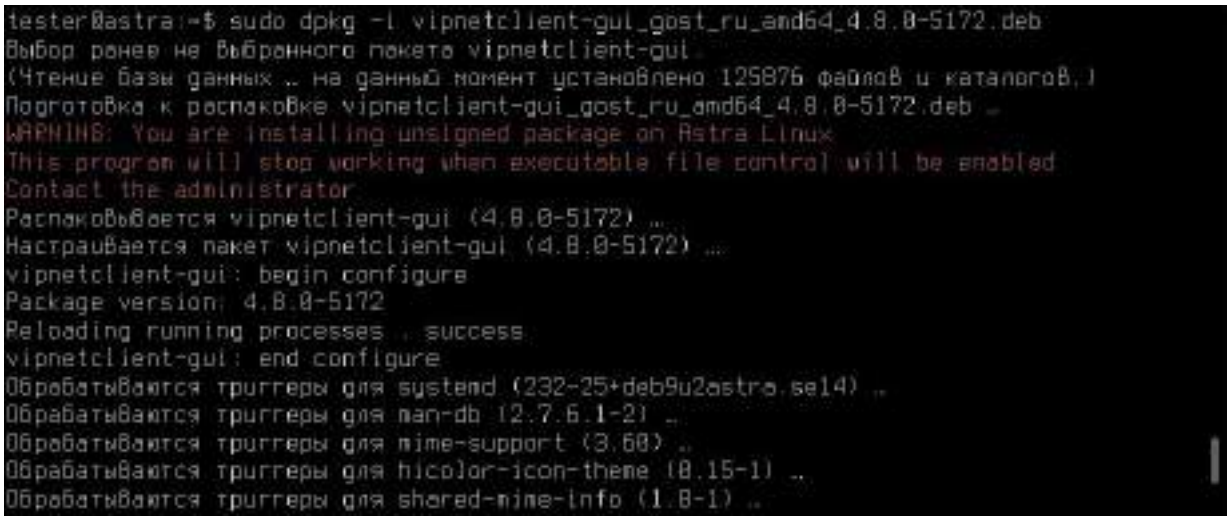

Рисунок 19. Уведомление об установке неподписанной сборки ViPNet Client 4U for Linux

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

  Раньше создание отчета о работе программы ViPNet Client 4U for Linux для отправки в ИнфоТеКС выполнялось только в командной строке. Теперь вы можете создать отчет и с помощью интерфейса ViPNet Client 4U for Linux (см. Обращение в службу технической поддержки на стр. 35).

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

  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 for Linux вы можете управлять количеством потоков, используемых драйверной частью программы ViPNet Client 4U for Linux. Увеличение количества используемых потоков позволяет повысить скорость обработки IP-трафика. По умолчанию программа ViPNet Client 4U for Linux 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.

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 УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

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, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator) или программно-аппаратный комплекс. В рамках 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.

Открытый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Роль

Некоторая 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 сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее устройствами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

Симметричный ключ

Последовательность битов заданной длины (для алгоритма ГОСТ 28147-89 — 256 бит), используемая как для зашифрования, так и для расшифрования информации.

В программном обеспечении ViPNet симметричные ключи используются для зашифрования и расшифрования IP-трафика, информации приложений (в том числе почтовой), служебных и прикладных конвертов.

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. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.