



ViPNet Client 5 for Linux

Руководство пользователя

Версия продукта: 5.1.4

© АО «ИнфоТеКС», 2025

ФРКЕ.00380-01 34 01

Версия продукта 5.1.4

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.

Все условия эксплуатации и ограничения на использование ViPNet Client 5 for Linux приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Client 5 for Linux.

АО «ИнфоТеКС»

125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

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.....	6
Соглашения документа.....	6
О программе	7
Что нового в версии 5.1.4	8
Обратная связь.....	9
 Глава 1. Общие сведения	10
Для чего нужно устанавливать ключи.....	11
Способы аутентификации.....	12
 Глава 2. Работа в командной строке	13
Установка ключей	14
Обновление ключей.....	17
Удаление ключей	18
Запуск и завершение работы.....	19
Несколько профилей на устройстве.....	21
Проверка VPN-соединения.....	24
Смена способа аутентификации.....	25
Смена сервера соединений	27
Экспериментальные настройки	27
Просмотр списка узлов.....	28
Просмотр информации о своём узле и о VipNet Client 5.....	30
Смена пароля.....	31
Обращение в службу технической поддержки	33
 Глава 3. Работа в графическом интерфейсе	34
Установка ключей	36
Обновление ключей.....	40
Удаление ключей	41
Запуск и завершение работы.....	42
Многофакторная аутентификация.....	44
Способы многофакторной аутентификации.....	46
Многофакторная аутентификация до входа в Linux.....	47
Несколько профилей на устройстве.....	49

Добавление профиля	49
Смена профиля.....	50
Удаление профиля	51
Смена имени профиля.....	52
Проверка VPN-соединения.....	53
Смена сервера соединений	54
Экспериментальные настройки	55
Смена пароля.....	56
Смена способа аутентификации.....	59
Просмотр списка узлов.....	60
Просмотр информации о своём узле и о ViPNet Client 5	61
Контроль целостности и работоспособности.....	62
Обращение в службу технической поддержки	63
Приложение А. Возможные неполадки и способы их устранения.....	64
Проблемы с отображением графического интерфейса ViPNet Client 5 в ОС Ubuntu 22.04 LTS	64
Нарушена целостность компонентов программы ViPNet Client 5 или связанных системных библиотек	65
Долгие ответы на команду ping	65
В списке приложений Astra Linux нет ViPNet Client 5.....	66
Приложение В. История версий	67
Что нового в версии 5.1.3.....	67
Что нового в версии 5.0.1	70
Приложение С. Политика конфиденциальности	73
Приложение D. Термины и сокращения	79



Введение

О документе	6
О программе	7
Что нового в версии 5.1.4	8
Обратная связь	9

О документе

Документ поможет вам начать использовать ViPNet Client 5 for Linux (далее — ViPNet Client 5) для защиты информации, которой вы обмениваетесь с другими пользователями защищённой сети.

Предполагается, что вы обладаете навыками пользования операционной системой GNU/Linux (далее — ОС Linux).

Соглашения документа

Обозначение	Описание
Название	Название элемента интерфейса: окна, вкладки, поля, кнопки, ссылки
Клавиша+Клавиша	Сочетание клавиш: нажмите первую клавишу и, не отпуская её, нажмите вторую
Меню > Команда	Последовательность элементов или действий
Код	Имя файла, путь, фрагмент кода или команда в командной строке



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

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

ViPNet Client 5 защищает трафик на компьютерах с Linux путём шифрования IP-пакетов.

С помощью ViPNet Client 5 ваше устройство станет [узлом защищённой сети](#) (далее — узел). Вы сможете подключаться к другим узлам или [туннелируемым узлам](#) по защищённому каналу через координатор и получать доступ к размещённым на этих узлах ресурсам: корпоративным веб-порталам, электронной почте, системе IP-телефонии и другим корпоративным сервисам. К открытым ресурсам интернета вы будете подключаться напрямую по незащищённому каналу.

Чтобы общаться с пользователями сети ViPNet по защищённому каналу, установите на устройство с ViPNet Client 5 программы ViPNet CSS Connect и ViPNet Деловая почта.

ViPNet Client 5 поставляется в одном из вариантов:

- Консольная версия, с которой можно работать только из командной строки.
- Графическая версия, с которой можно работать в командной строке и в графическом интерфейсе.

Установка, обновление и удаление ViPNet Client 5 на компьютер выполняются администратором, так как для этого требуются права суперпользователя ОС (root). Подробнее см. руководство администратора, глава «Установка, обновление и удаление ViPNet Client 5».

Что нового в версии 5.1.4

- **Повышение безопасности при обновлении**

Теперь при обновлении ViPNet Client 5 проверяется электронная подпись файла. Это позволяет подтвердить подлинность обновления и безопасно его установить.

- **Сохранение имени доменной учётной записи для многофакторной аутентификации**

Теперь [при многофакторной аутентификации](#) вы можете выбрать **Сохранить имя**, чтобы не вводить его при каждой аутентификации.

- **Отправка писем пользователям без ViPNet Client для Windows**

Раньше вы не могли отправлять письма из ViPNet Деловая почта для Linux пользователям ViPNet Деловая почта для Windows, у которых не установлен ViPNet Client. После установки ViPNet Client 5 for Linux версии 5.1.4 вы сможете отправлять письма этим пользователям.

Обратная связь

Контактная информация

- 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.
Телеграм-канал поддержки: t.me/vhd21.
Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Дополнительная информация на сайте ИнфоТеКС

- [О продуктах ViPNet.](#)
- [О решениях ViPNet.](#)
- [Часто задаваемые вопросы.](#)
- [Форум пользователей продуктов ViPNet.](#)

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



1

Общие сведения

Для чего нужно устанавливать ключи	11
Способы аутентификации	12

Для чего нужно устанавливать ключи

Перед использованием ViPNet Client 5 установите на компьютер ключи. С помощью этих ключей шифруется IP-трафик при соединениях с другими узлами защищённой сети. Без этого работа ViPNet Client 5 в защищённой сети будет невозможна.

Установка ключей компьютер выполняется с помощью дистрибутива ключей (файла *.dst или *.ds5) и пароля пользователя ViPNet. Вы можете получить их лично или другим доверенным способом у администратора.

Для установки ключей потребуется ввести пароль пользователя или PIN-код от устройства. Их также может потребоваться вводить при включении VPN в зависимости от уровня полномочий, назначенного вам администратором:

- Минимальный уровень полномочий — ввод пароля или PIN-кода требуется всегда.
- Максимальный, средний и специальный уровни полномочий — ввод пароля не требуется ни при каких условиях. Ввод PIN-кода требуется только при первом подключении внешнего устройства после смены PIN-кода на нём.

Способы аутентификации

ViPNet Client 5 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 PIN-код. Работает только с ключами *.dst на устройствах с архитектурой процессора x86-64.



Примечание. Вы можете изменить PIN-код от внешнего устройства средствами производителя. После этого при первом подключении внешнего устройства потребуется ввести новый PIN-код.

Подключать к компьютеру внешнее устройство с персональным ключом и вводить PIN-код к нему в ViPNet Client 5 потребуется при установке ключей, смене PIN-кода, а также при каждом включении VPN (при этом вводить PIN-код потребуется, только если вы обладаете минимальным уровнем полномочий). Без этого работа в защищённой сети будет невозможна.

Способ аутентификации задаёт администратор сети ViPNet.

Также в процессе работы с ViPNet Client 5 вы можете самостоятельно [сменить способ аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве](#).

Для доступа к корпоративным ресурсам администратор может дополнительно назначить вам [многофакторную аутентификацию](#).

2

Работа в командной строке



Внимание! Для работы ViPNet Client 5 на устройстве ОС Astra Linux Special Edition при аутентификации в ОС выберите атрибут безопасности **Уровень конфиденциальности** — 0.

Для работы с ViPNet Client 5 с правами суперпользователя (root) на устройстве ОС EMIAS OS 1.0 и ЗОС СинтезМ войдите в ОС под учётной записью root.

Установка ключей	14
Обновление ключей	17
Удаление ключей	18
Запуск и завершение работы	19
Несколько профилей на устройстве	21
Проверка VPN-соединения	24
Смена способа аутентификации	25
Смена сервера соединений	27
Просмотр списка узлов	28
Просмотр информации о своём узле и о ViPNet Client 5	30
Смена пароля	31
Обращение в службу технической поддержки	33

Установка ключей

Установка ключей при аутентификации по паролю

- 1 Если вы устанавливаете ключи под учётной записью `root`, укажите путь к рабочему каталогу ViPNet в файле `/etc/vipnet.conf` в параметре `config_dir` (см. руководство администратора, раздел «Настройки в файле `vipnet.conf`»). Это нужно для работы с ViPNet CSS Connect и ViPNet Деловая почта.

- 2 Выполните:

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

где:

- `psw` — пароль пользователя ViPNet (если используется аутентификация пользователя по паролю). 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 параметров 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 5 и её автоматического запуска в случае нештатного завершения работы. Для более надёжной работы ViPNet Client 5 применять этот параметр не рекомендуется. По умолчанию счётчик попыток восстановления работоспособности ViPNet Client 5 выставлен на 10 попыток, на промышленных контроллерах — на бесконечное число попыток.
- `no-autostart` — отключение автоматического запуска ViPNet Client 5 и включения VPN-соединения после аутентификации пользователя в ОС. Для более надёжной работы ViPNet Client 5 применять этот параметр не рекомендуется.



Примечание. Если ключи устанавливались под учётной записью `root`, то автоматический запуск ViPNet Client 5 и подключение к защищённой сети после аутентификации пользователя в ОС отключить невозможно.

- `no-start` — отказ автоматического подключения к защищённой сети после установки ключей.

- 3 Если пароль не был указан в команде, введите пароль пользователя и нажмите **Enter**.
- 4 Подождите, пока ключи будут установлены. Выполнение команды может занять некоторое время.

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

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](#)).

Установка ключей при аутентификации с помощью внешнего устройства

1 Если вы устанавливаете ключи под учётной записью `root`, укажите путь к рабочему каталогу ViPNet в файле `/etc/vipnet.conf` в параметре `config_dir` (см. руководство администратора, раздел «Настройки в файле `vipnet.conf`»). Это нужно для работы с ViPNet CSS Connect и ViPNet Деловая почта.

2 В консоли ОС Linux выполните:

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

где:

- `pin` — PIN-код от внешнего устройства с персональным ключом пользователя (если используется аутентификация пользователя по персональному ключу на внешнем устройстве). Чтобы снизить риск компрометации PIN-кода, применять параметр `--pin` не рекомендуется, так как при этом PIN-код отображается в консоли в явном виде. Вводите PIN-код по запросу во время выполнения команды.
- `psw` — пароль пользователя ViPNet (если назначен не минимальный уровень полномочий). 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 параметров и содержит спецсимволы, используйте экранирование спецсимволов. Подробнее см. в справочных материалах используемого командного интерпретатора (например, `man bash`).

- `token-select` — поиск (по любой части названия) и выбор внешнего устройства, если к компьютеру подключено несколько внешних устройств. Если конкретное внешнее устройство не будет указано с помощью этого параметра, в консоли отобразится список подключённых внешних устройств и предложение выбрать одно из них.
- `no-failprotect` — отключение ежеминутной проверки работоспособности ViPNet Client 5 и её автоматического запуска в случае нештатного завершения работы. Для более надёжной работы ViPNet Client 5 применять этот параметр не рекомендуется. По умолчанию счётчик попыток восстановления работоспособности ViPNet Client 5 выставлен на 10 попыток, на промышленных контроллерах — на бесконечное число попыток.
- `no-autostart` — отключение автоматического запуска ViPNet Client 5 и включения VPN-соединения после аутентификации пользователя в ОС. Для более надёжной работы ViPNet Client 5 применять этот параметр не рекомендуется.



Примечание. Если ключи устанавливались под учётной записью `root`, то автоматический запуск ViPNet Client 5 и подключение к защищённой сети после аутентификации пользователя в ОС отключить невозможно.

- o `no-start` — отказ автоматического подключения к защищённой сети 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 PIN-код не был указан в команде, введите PIN-код 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.

```
user@host:~$ vipnetclient installkeys abn_000a.dst
Verifying the "/home/user/abn_000a.dst" key set file ... Success
Your key set requires Logon Device
Please make sure that your Logon Device is connected 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 ..... 40f3664a
State ..... OK
Pin ..... OK

Device 2:
Module ..... JaCarta(slot:0001FFFF)
Model ..... PRO
Label .....
Manufacturer ..... Aladdin R.D.
Serial ..... 4E46002161633932
State ..... OK
Pin ..... OK

... Success
Please type a device number and press Enter: 1
Type VPN user PIN:
Type VPN user password:
Installing keys of the "user" user ... Success
Turning on VPN autostart at "user" logon ... Success
Logging on as "user" ... Success
```

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](#)).

Обновление ключей

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

Если на защищённый узел пришли некорректные обновления, которые не проходят проверки целостности и подлинности, они не применяются. Клиент блокирует подозрительные конверты и отправляет уведомление об этом на узел с ViPNet ЦУС или с центром управления ViPNet Prime.

Если ключи не удалось установить автоматически, и администратор передал вам новый дистрибутив ключей, установите их вручную. Для этого:

- 1 [Удалите установленные ключи.](#)
- 2 [Установите новые ключи.](#)

Удаление ключей

Если вы используете несколько профилей, см. [Удаление профиля](#).

1 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 5 и включение VPN-соединения выполняются автоматически после установки ключей и при каждой аутентификации в ОС пользователя, установившего ключи.

Автоматический запуск программы и включение VPN-соединения после аутентификации пользователя в ОС не выполняются в следующих случаях:

- Если пользователь обладает минимальными полномочиями.
- Если используется [аутентификация пользователя по персональному ключу на внешнем устройстве](#) и внешнее устройство не подключено к компьютеру.
- Если при установке ключей был указан параметр `--no-autostart`.



Примечание. При повторном подключении внешнего устройства VPN-соединение запускается автоматически для пользователей с не минимальными полномочиями. Включить VPN-соединение вручную и ввести PIN-код от внешнего устройства потребуется, если:

- пользователь обладает минимальными полномочиями;
- внешнее устройство подключается впервые после смены PIN-кода.

Чтобы запустить ViPNet Client 5 и включить VPN-соединение вручную:

- 1 Если в ViPNet Client 5 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 <PIN-код>] | [--psw  
<пароль_от_дистрибутива_ключей>]] [--token-select <часть_названия>]  
[--no-failprotect]
```

где:

- `pin` — PIN-код от внешнего устройства с персональным ключом пользователя (если используется аутентификация пользователя по персональному ключу на внешнем устройстве). Чтобы снизить риск компрометации PIN-кода, применять параметр `--pin` не рекомендуется, так как при этом PIN-код отображается в консоли в явном виде. Вводите PIN-код по запросу во время выполнения команды. Требуется вводить только при минимальном уровне полномочий пользователя.
- `psw` — пароль пользователя ViPNet (если используется аутентификация пользователя по паролю). 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. Требуется вводить только при минимальном уровне полномочий пользователя.



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

- o `token-select` — поиск (по любой части названия) и выбор внешнего устройства, если к компьютеру подключено несколько внешних устройств. Если конкретное внешнее устройство не будет указано с помощью этого параметра, в консоли отобразится список подключённых внешних устройств и предложение выбрать одно из них.
 - o `no-failprotect` — отключение ежеминутной проверки работоспособности ViPNet Client 5 и её автоматического запуска в случае нештатного завершения работы. Для более надёжной работы ViPNet Client 5 применять этот параметр не рекомендуется. По умолчанию счетчик попыток восстановления работоспособности ViPNet Client 5 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 При необходимости введите пароль пользователя или PIN-код и нажмите **Enter**.
 - 5 Подождите, пока VPN-соединение будет включено. Выполнение команды может занять некоторое время.

Завершение работы

Чтобы остановить ViPNet Client 5 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.

Работа нескольких пользователей ОС

Если ViPNet Client 5 используют несколько пользователей ОС, меняйте пользователя одним из способов:

- выключите VPN-соединение и завершите сессию,
- перезагрузите ОС.

После смены пользователя включите VPN-соединение вручную.

Несколько профилей на устройстве

Вы можете установить до десяти дистрибутивов ключей в ViPNet Client 5 для каждого пользователя ОС. Для каждого дистрибутива ключей будет создан отдельный профиль. Профили можно настроить по-разному и переключаться между ними, например, чтобы работать в разных сетях ViPNet.

Вы можете установить в одном ViPNet Client 5 ключи из разных сетей и с разными:

- форматами (DST и DS5) и криптографией,
- уровнями полномочий,
- способами аутентификации.

Это экспериментальная функция. Особенности:

- Если вы используете ViPNet CSS Connect версии 2.x, то когда вы добавите новый профиль, в текущем профиле удалится история чатов. Чтобы её сохранить, создайте резервную копию в ViPNet CSS Connect. См. руководство пользователя ViPNet CSS Connect.
- Работа с ViPNet Administrator, Policy Manager и ViPNet Деловая почта может быть ограничена.

Добавление профиля



Внимание! В ViPNet CSS Connect версии 2.x удалится история чатов текущего профиля, когда вы добавите новый профиль. Чтобы сохранить историю чатов, создайте резервную копию в ViPNet CSS Connect.

Вы можете добавить до 10 профилей для каждого пользователя ОС.

1 В командной строке выполните:

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

где:

- `pin` — PIN-код от внешнего устройства с персональным ключом пользователя (если используется аутентификация пользователя по персональному ключу на внешнем устройстве). Чтобы снизить риск компрометации PIN-кода, применять параметр `--pin` не рекомендуется, так как при этом PIN-код отображается в консоли в явном виде. Вводите PIN-код по запросу во время выполнения команды.
- `psw` — пароль пользователя ViPNet (если используется аутентификация пользователя по паролю). 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.

- o `token-select` — поиск (по любой части названия) и выбор внешнего устройства, если к компьютеру подключено несколько внешних устройств. Если конкретное внешнее устройство не будет указано с помощью этого параметра, в консоли отобразится список подключённых внешних устройств и предложение выбрать одно из них.
- o `no-start` — отказ автоматического подключения к защищённой сети после установки ключей.

2 Если вы добавляете профиль первый раз, ознакомьтесь с особенностями использования нескольких профилей на устройстве и подтвердите добавление профиля.

3 Если пароль не был указан в команде, введите его и нажмите **Enter**.

Вы автоматически перейдёте в созданный профиль. Если вы не указывали параметр `no-start`, в профиле будет включено VPN-соединение. По умолчанию имя профиля совпадает с именем узла. Вы можете изменить имя профиля.

Смена профиля



Внимание! В ViPNet CSS Connect версии 2.x удалится история чатов текущего профиля, когда вы смените профиль. Чтобы сохранить историю чатов, создайте резервную копию в ViPNet CSS Connect.

Выполните:

```
user@host:~$ vipnetclient profile switch <идентификатор узла>
```

После смены профиля [включите VPN-соединение вручную](#).

Удаление профиля

Чтобы удалить текущий профиль:

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

Чтобы удалить другой профиль:

```
user@host:~$ vipnetclient profile deletekeys <идентификатор узла> [--skip-accept]
```

где:

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

Будут удалены профиль и ключи его узла.

Смена имени профиля

Имя профиля отображается только на вашем устройстве. По умолчанию оно совпадает с именем узла.

Вы можете изменить имя текущего профиля. Для этого выполните:

```
user@host:~$ vipnetclient profile set --alias <новое имя профиля>
```

Длина нового имени профиля должна быть от 1 до 120 символов.

Чтобы вернуть имя профиля по умолчанию:

```
user@host:~$ vipnetclient profile set --no-alias
```

Просмотр списка профилей

Выполните:

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

Отобразится информация о профилях:

- # — порядковый номер профиля. Список отсортирован по идентификатору узла в порядке возрастания.
- Host ID — идентификатор узла,
- Keys — формат ключей (DST или DS5. Если для аутентификации используется внешнее устройство, после формата ключей будет написано AD),
- Permissions — уровень полномочий узла,
- Profile — имя профиля,
- Network — номер и название ViPNet-сети.

Перед текущим профилем будет написано `active`.

```
user@host:~$ vipnetclient list --profiles
Requesting profiles list ... Success
```

	#	Host ID	Keys	Permissions	Profile	Network
	1	22E11738	DST	maximum	Перминов Павел	8929 Сеть организации
active:	2	22E1772E	DST+AD	maximum	Перминов Павел (token)	8929 Сеть организации
	3	508805DB	DS5	minimum	Перминов Павел	20616 Minimum

Рисунок 2: Список профилей

Проверка VPN-соединения

При [включении VPN-соединения](#) ViPNet Client 5 автоматически проверяет связь с координатором, являющимся [сервером соединений](#) для вашего узла. Если координатор недоступен, VPN-соединение не будет работать, и вы не сможете подключаться к другим узлам защищённой сети. Обратитесь к администратору.

Вы можете проверить VPN-соединение вручную. Например, если прервалась связь с какими-либо ресурсами защищённой сети. Для этого выполните:

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

Если VPN-соединение отсутствует, повторите попытку через некоторое время или обратитесь к администратору.



Примечание. Вы можете проверить связь с другими узлами:

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

Идентификатор узла можно [посмотреть в списке узлов](#).

Смена способа аутентификации



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами *.dst на устройствах с архитектурой x86_64.

В ViPNet Client 5 вы можете сменить **способ аутентификации** с аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве.

1 Подключите внешнее устройство к компьютеру.

2 Выполните:

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

где:

- o `pin` — PIN-код от внешнего устройства с персональным ключом пользователя (если используется аутентификация пользователя по персональному ключу на внешнем устройстве). Чтобы снизить риск компрометации PIN-кода, применять параметр `--pin` не рекомендуется, так как при этом PIN-код отображается в консоли в явном виде. Вводите PIN-код по запросу во время выполнения команды.
- o `token-select` — поиск (по любой части названия) и выбор внешнего устройства, если к компьютеру подключено несколько внешних устройств. Если конкретное внешнее устройство не будет указано с помощью этого параметра, в консоли отобразится список подключённых 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 PIN-код не был указан в команде, введите PIN-код 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 изменён.

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

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

Device 1:
Module ..... ruToken(slot:00000000)
Model ..... Rutoken ECP
Label ..... Rutoken
Manufacturer ..... Aktiv Co.
Serial ..... 40f3664a
State ..... OK
Pin ..... OK

Device 2:
Module ..... JaCarta(slot:0001FFFF)
Model ..... PRO
Label .....
Manufacturer ..... Aladdin R.D.
Serial ..... 4E46002161633932
State ..... OK
Pin ..... OK

... Success
Please type a device number and press Enter: 2
Type VPN user PIN:
Changing the logon mode to Logon Device ... Success
```

Рисунок 3. Смена способа аутентификации



Примечание. Вы можете изменить PIN-код от внешнего устройства средствами производителя. После этого при первом подключении внешнего устройства потребуется ввести новый PIN-код.

Если не удастся изменить способ аутентификации при использовании внешнего устройства JaCarta с версией «ПК Единый Клиент JaCarta» 3.0 см. руководство администратора, раздел «Возможные неполадки и способы их устранения».

Смена сервера соединений

В ViPNet Client 5 for Linux вы можете сменить координатор, используемый в качестве сервера соединений. Например, если текущий сервер соединений недоступен. В качестве сервера соединений рекомендуется использовать координатор из собственной сети ViPNet.

В качестве сервера соединений нельзя выбрать координаторы, для которых не указан IP-адрес или доменное имя. Если включена настройка **Группа серверов**, выбирайте координатор только из собственной сети ViPNet.

Чтобы сменить сервер соединений, выполните:

```
user@host:~$ vipnetclient debug --active-server <идентификатор_координатора_ViPNet>
[--insist]
```

где

`--insist` — режим выбора сервера соединений при получении справочников и ключей из управляющего ПО:

- Если эта опция задана, сервером соединений будет оставаться координатор, выбранный вручную в ViPNet Client 5.
- Если опция не задана, сервером соединений будет назначаться координатор, заданный в управляющем ПО.



Внимание! Задавайте режим выбора сервера соединений каждый раз, когда вручную меняете сервер соединений. Если вы выполните команду без опции `--insist`, то после обновления справочников и ключей, сервером соединений будет назначаться координатор, заданный в управляющем ПО.

Экспериментальные настройки

Автоматический выбор сервера соединений

- Чтобы ViPNet Client 5 автоматически переключался на другой сервер соединений, если ваш активный координатор недоступен, выполните:

```
user@host:~$ vipnetclient debug --connect-server-group
```

Когда ваш активный координатор станет доступен, ViPNet Client 5 переключится обратно на него.

Эта настройка по умолчанию включена для клиентов с ключами `*ds5`.

- Чтобы выключить автоматический выбор сервера соединений, выполните:

```
user@host:~$ vipnetclient debug --no-connect-server-group
```

Просмотр списка узлов

- 1 Чтобы просмотреть список защищённых узлов, выполните:

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

Отобразится список узлов, с которыми ваш узел может взаимодействовать в защищённой сети:

- Идентификатор узла содержится в столбце ID.
- Типы узлов отмечены как `client` (клиент, компьютер пользователя) и `server` (координатор).
- Координатор, выполняющий функции сервера IP-адресов для вашего компьютера, отмечен в списке символом `*`.

```
user@host:~$ vipnetclient list --nodes
ID      Type    Access IP      Name
22E11732 server*  7.0.23.50      Координатор Москва
22E11733 client  7.0.23.51      Юрьев Александр
22E11734 client  7.0.23.52      Фёдоров Алексей
22E11735 client  7.0.23.53      Соколова Ирина
22E11736 client  7.0.23.54      Сидоров Андрей
22E11737 client  7.0.23.55      Петров Алексей
22E11738 client  7.0.23.56      Перминов Павел
22E11739 client  7.0.23.57      Николаев Александр
22E1173A client  7.0.23.58      Маслова Мария
22E1173B client  7.0.23.59      Максимов Олег
22E1173C client  7.0.23.60      Иванов Денис
user@host:~$
```

Рисунок 4. Просмотр списка узлов

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

```
user@host:~$ vipnetclient vpndiag -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 vpndiag -s ipsettings --node-info 22E11732
Calling the "vpndiag" with the following parameters: -s ipsettings
--node-info 22E11732 ... Success
Node IP settings

accessPoint:
  Encapsulation: Udp
  Type: Direct
  ip: 81.30.192.133
  node: 22E11732
  port: 58867
accessPoints:
  default:
    Id: 22E11732
    Ip: 81.30.192.133
    Port: 58867
  endpoints:
    81.30.192.133:58867
    10.10.88.67:58867
    10.2.0.67:58867
  firewall:
    Id: 22E11732
    Ip: 81.30.192.133
    Port: 58867
  multicast:
    <empty>
  proxy:
    Id: FFFFFFFE
baseVirtualIp: 11.0.0.1
cipher: 0
ips:

```

Рисунок 5. Просмотр подробной информации об узле

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



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

Для проверки доступности ресурсов через команду ping, используйте флаг -n. Например:

```

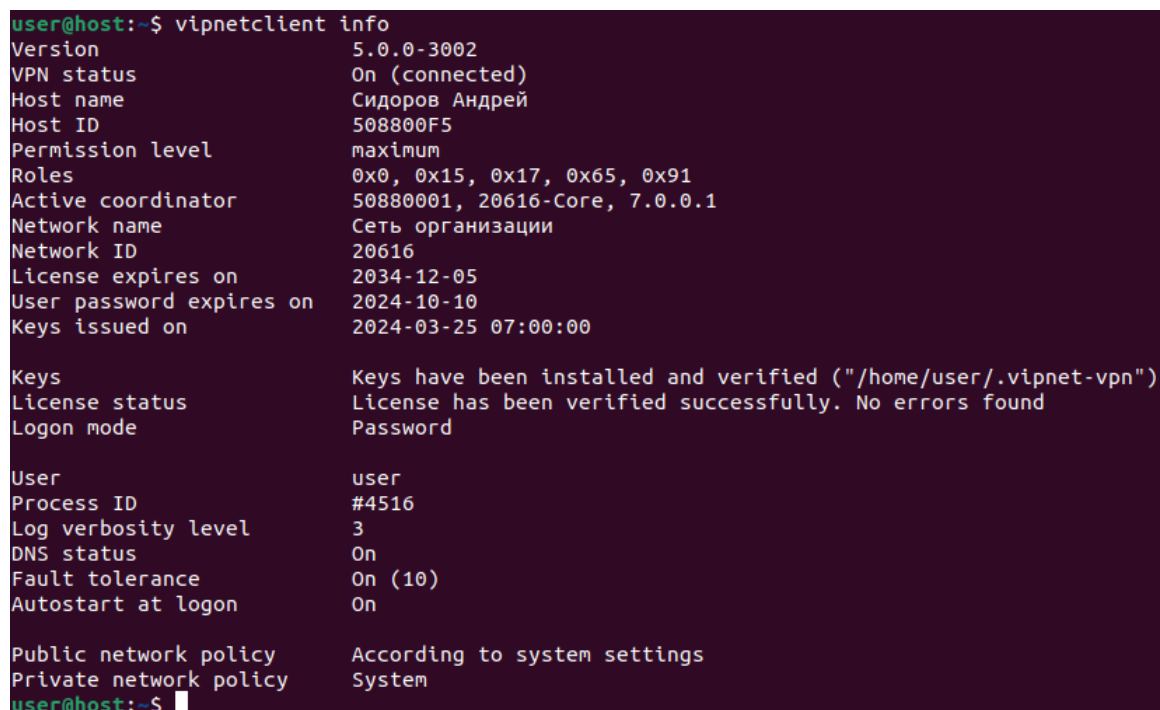
ping -n <ID узла>.vipnet
ping -n ya.ru

```

Просмотр информации о своём узле и о ViPNet Client 5

- 1 Чтобы просмотреть информацию о своём узле и версии ViPNet Client 5, выполните:

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



```
user@host:~$ vipnetclient info
Version                5.0.0-3002
VPN status              On (connected)
Host name              Сидоров Андрей
Host ID                508800F5
Permission level        maximum
Roles                  0x0, 0x15, 0x17, 0x65, 0x91
Active coordinator      50880001, 20616-Core, 7.0.0.1
Network name           Сеть организации
Network ID              20616
License expires on      2034-12-05
User password expires on 2024-10-10
Keys issued on          2024-03-25 07:00:00

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

User                   user
Process ID              #4516
Log verbosity level     3
DNS status              On
Fault tolerance         On (10)
Autostart at logon      On

Public network policy   According to system settings
Private network policy   System
user@host:~$
```

Рисунок 6. Просмотр информации о своём узле

- 2 Чтобы просмотреть информацию только о версии ViPNet Client 5, выполните:

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

В ОС отсутствует доступ до корпоративных ресурсов по доменным именам или не работает доменная зона .vipnet, следуйте указаниям раздела «Нарушена работа программы ViPNet Client 5 с DNS» руководства администратора.

Если разница во времени на вашем компьютере и координаторе, который является сервером соединений, больше разрешённой 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 для обновления лицензии.

Если отображается `User traffic status Blocked`, обратитесь к администратору.

Смена пароля



Примечание. Смена пароля доступна только клиентам с ключами *.ds5.

Чтобы обезопасить свои данные, рекомендуется менять пароль не реже, чем раз в полгода, после установки ключей и после каждого обновления мастер-ключей в организации. Когда срок действия пароля истечёт, появится напоминание о необходимости сменить пароль.

1 Выполните:

```
user@host:~$ vipnetclient auth --change-user-password [--user-psw <текущий_пароль>]
[--new-psw <новый_пароль>] [--confirm <новый_пароль>]
```

где:

- o user-psw — текущий пароль пользователя,
- o new-psw — новый пароль пользователя,
- o confirm — повтор нового пароля.

Чтобы снизить риск компрометации пароля, применять эти параметры 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 параметров и содержит спецсимволы, используйте экранирование спецсимволов. Подробнее см. в справочных материалах используемого командного интерпретатора (например, `man bash`).

2 Если пароль не был указан в команде:

2.1 Введите текущий пароль и нажмите **Enter**.

2.2 Введите новый пароль и нажмите **Enter**.

Длина пароля должна быть латинскими буквами — от 6 до 31 символа, русскими — от 6 до 16.

Пароль должен содержать:

- o строчные буквы,
- o заглавные буквы,
- o цифры.

Пароль может содержать символы `!"#$%&*()_-=@;:.,^'[]{}/|\><`~.`

Пароль не должен содержать:

- o пробелы,
- o один и тот же символ три и более раза подряд.

2.1 Повторите новый пароль и нажмите **Enter**.

Просмотр срока действия пароля

Выполните:

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

Срок действия пароля отобразится в строке `User password expires on`.

Если требуется сменить пароль, в строке `Logon mode` отобразится статус `change required`.

Обращение в службу технической поддержки

В случае возникновения ошибок в работе ViPNet Client 5, создайте и передайте отчёт о работе программы в ИнфоТекС:

- 1 Создайте отчёт о работе ViPNet Client 5. Для этого выполните:

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

где:

--output — параметр для указания имени отчёта и каталога, в который будет сохранен файл отчёта. Если в команде вы не укажете каталог и имя отчёта, то отчёт будет сохранен в каталоге, в котором была выполнена команда `vipnetclient report`, с именем `report_linux_<версия_клиента>_<дата>_<время>.zip`.

Будет создан ZIP-архив с отчётом о работе ViPNet Client 5. Если в клиенте используется [несколько профилей](#), в архиве будут только общие файлы и файлы для текущего профиля.

- 2 Создайте электронное письмо с описанием проблемы и прикрепите к письму архив с отчётом о работе ViPNet Client 5. Опишите проблему и обстоятельства её возникновения.
- 3 Отправьте письмо в [ИнфоТекС](#).

3

Работа в графическом интерфейсе



Внимание! Для работы ViPNet Client 5 на устройстве ОС Astra Linux Special Edition при аутентификации в ОС выберите атрибут безопасности **Уровень конфиденциальности — 0**.
Для работы с ViPNet Client 5 с правами суперпользователя (root) на устройстве ОС EMIAS OS 1.0 и ЗОС СинтезМ войдите в ОС под учётной записью root.

Установка ключей	36
Обновление ключей	40
Удаление ключей	41
Запуск и завершение работы	42
Многофакторная аутентификация	44
Несколько профилей на устройстве	49
Проверка VPN-соединения	53
Смена сервера соединений	54
Смена пароля	56
Смена способа аутентификации	59
Просмотр списка узлов	60

Просмотр информации о своём узле и о ViPNet Client 5	61
Контроль целостности и работоспособности	62
Обращение в службу технической поддержки	63

Установка ключей

Установка ключей при аутентификации по паролю

- 1 Если вы устанавливаете ключи под учётной записью root, укажите путь к рабочему каталогу ViPNet в файле `/etc/vipnet.conf` в параметре `config_dir` (см. руководство администратора, раздел «Настройки в файле `vipnet.conf`»). Это нужно для работы с ViPNet CSS Connect и ViPNet Деловая почта.
- 2 Откройте ViPNet Client 5 одним из способов:
 - Выполните:

```
user@host:~$ vipnetclient-gui
```
 - В списке установленных на компьютере программ щёлкните значок ViPNet Client for Linux .
- 3 В ViPNet Client 5 нажмите **Добавить ключи**.

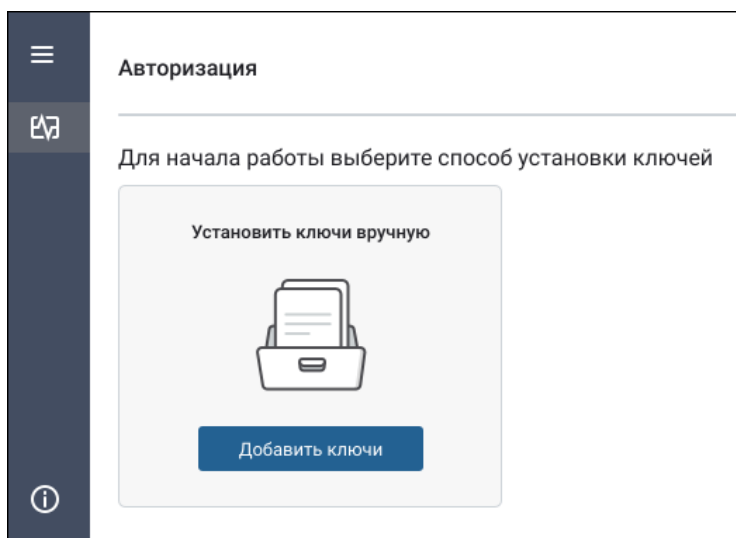


Рисунок 7. Установка дистрибутива ключей

- 4 Выберите дистрибутив ключей.

5 В окне **Установка ключей** введите пароль и нажмите **Далее**.

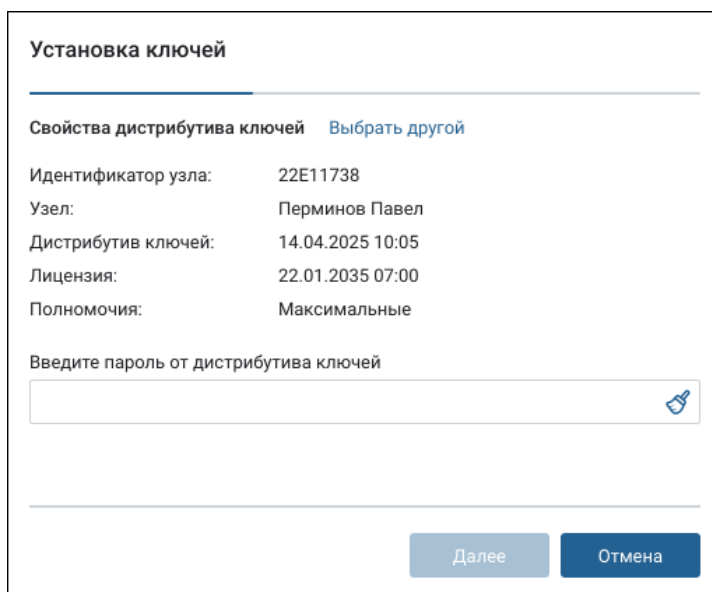


Рисунок 8. Установка ключей при аутентификации по паролю

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 Если вы устанавливаете ключи под учётной записью root, укажите путь к рабочему каталогу ViPNet в файле `/etc/vipnet.conf` в параметре `config_dir` (см. руководство администратора, раздел «Настройки в файле `vipnet.conf`»). Это нужно для работы с ViPNet CSS Connect и ViPNet Деловая почта.
- 2 Подключите внешнее устройство к компьютеру.
- 3 Откройте ViPNet Client 5 одним из способов:
 - В консоли ОС Linux выполните:

```
user@host:~$ vipnetclient-gui
```
 - В списке установленных на компьютере программ щёлкните значок ViPNet Client 5 .
- 4 В ViPNet Client 5 нажмите **Добавить ключи**.
- 5 Выберите дистрибутив ключей.

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

6 В окне **Установка ключей** нажмите **Далее**.

Установка ключей

Свойства дистрибутива ключей [Выбрать другой](#)

Идентификатор узла:	56C70013
Узел:	Сидоров Андрей
Дистрибутив ключей:	26.03.2024 15:21
Лицензия:	27.12.2024 07:00
Полномочия:	Максимальные
Способ аутентификации:	С использованием персонального ключа на внешнем устройстве

[Далее](#) [Отмена](#)

Рисунок 9. Установка ключей при аутентификации с помощью внешнего устройства

7 Выберите устройство в списке и нажмите **Далее**.

Установка ключей

Подключите устройство и выберите его в списке

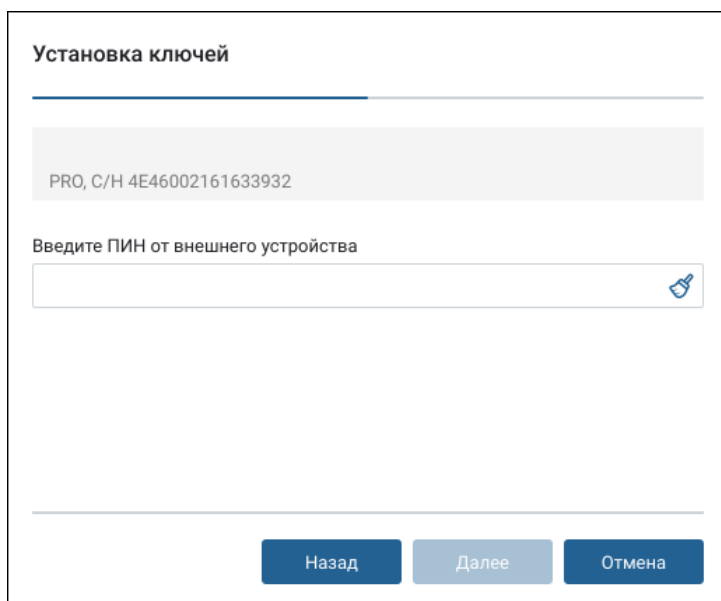
[Обновить список устройств](#)

- Rutoken ECP <no label>
- Rutoken ECP, C/H 40f3668a
- PRO, C/H 4E46002161633932

[Назад](#) [Далее](#) [Отмена](#)

Рисунок 10. Выбор внешнего устройства

- 8 Введите PIN-код от внешнего устройства и нажмите **Далее**.



Установка ключей

PRO, C/H 4E46002161633932

Введите ПИН от внешнего устройства

Назад Далее Отмена

Рисунок 11. Ввод PIN-кода к внешнему устройству

- 9 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.
- 10 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 защищённой сети или свойства сетевых узлов, а также в случае смены [мастер-ключей](#). Администратор создаёт новые ключи и централизованно отправляет их на узлы, где они будут приняты и установлены автоматически, без участия пользователя.

Если на защищённый узел пришли некорректные обновления, которые не проходят проверки целостности и подлинности, они не применяются. Клиент блокирует подозрительные конверты и отправляет уведомление об этом на узел с ViPNet ЦУС или с центром управления ViPNet Prime.

Если ключи не удалось установить автоматически, и администратор передал вам новый дистрибутив ключей, установите их вручную:

- 1 [Удалите установленные ключи.](#)
- 2 [Установите новые ключи.](#)

Удаление ключей

Чтобы удалить ключи (например, [при обновлении ключей](#) или в случае смены компьютера):

- 1 В ViPNet Client 5 выберите Профиль  и нажмите Удалить профиль.

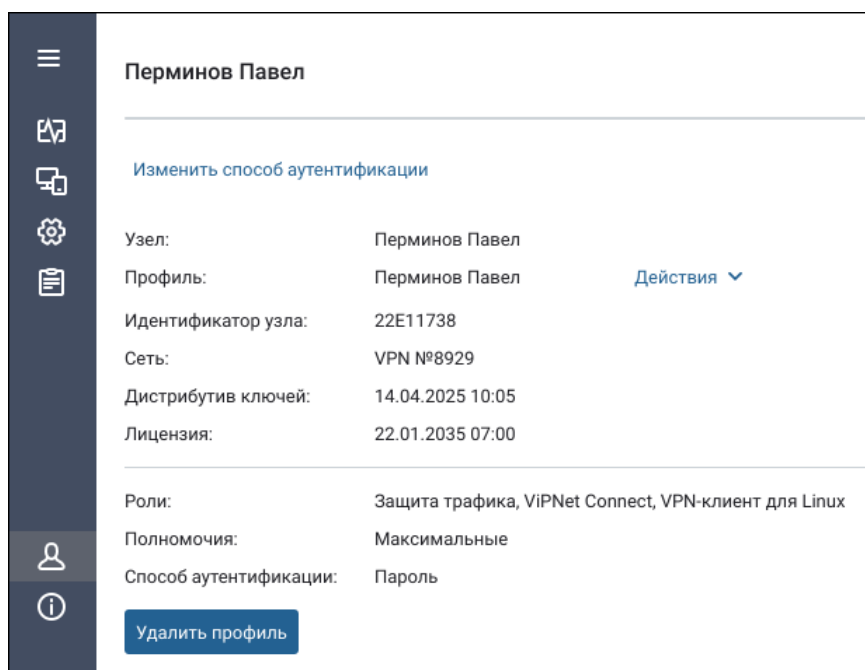


Рисунок 12. Удаление ключей

- 2 Подтвердите удаление.

Запуск и завершение работы

Запуск всех компонентов ViPNet Client 5 и включение VPN-соединения выполняются автоматически после установки ключей и при каждой аутентификации в ОС пользователя, установившего ключи.

Автоматический запуск программы и включение VPN-соединения после аутентификации пользователя в ОС не выполняются в следующих случаях:

- Если пользователь обладает минимальными полномочиями.
- Если используется [аутентификация пользователя по персональному ключу на внешнем устройстве](#) и внешнее устройство не подключено к компьютеру.
- Если при установке ключей был указан параметр `--no-autostart`.

Чтобы запустить ViPNet Client 5 и включить VPN-соединение вручную:

- 1 Если для аутентификации используется внешнее устройство, подключите его.
- 2 Выполните одно из действий:
 - В консоли ОС Linux выполните:

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

При включении VPN-соединения будет [проверено соединение с вашим координатором](#). Если соединение установлено, вы сможете работать с корпоративными ресурсами.



Примечание. При повторном подключении внешнего устройства VPN-соединение запускается автоматически для пользователей с не минимальными полномочиями. Включить VPN-соединение вручную и ввести PIN-код от внешнего устройства потребуются, если:

- пользователь обладает минимальными полномочиями;
- внешнее устройство подключается впервые после смены PIN-кода.

Аутентификация до авторизации в ОС

Если администратор настроил аутентификацию в ViPNet Client 5 до авторизации в ОС:

- 1 Если для аутентификации используется внешнее устройство, подключите его.
- 2 [При необходимости](#) введите пароль или PIN-код от внешнего устройства с персональным ключом и нажмите **Войти**.
- 3 Если вам назначена многофакторная аутентификация, [пройдите её](#).
- 4 Подождите, пока VPN-соединение будет включено. Это может занять некоторое время.
Когда VPN-соединение будет включено, в окне появится информация об этом. Закройте это окно.
- 5 Войдите в учётную запись.



Примечание. Если окно аутентификации в ViPNet Client 5 до авторизации в ОС не отобразилось на главном экране, переключите виртуальный терминал переднего плана (tty). Для этого используйте комбинацию клавиш `Ctrl+Alt+<F1-F12>`. Переключайте терминалы, пока не отобразится окно аутентификации в ViPNet Client 5.

Завершение работы

Чтобы выключить VPN-соединение, в ViPNet Client 5 нажмите **Отключить**.

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

Работа нескольких пользователей ОС

Если ViPNet Client 5 используют несколько пользователей ОС, меняйте пользователя одним из способов:

- выключите VPN-соединение и завершите сессию,
- перезагрузите ОС.

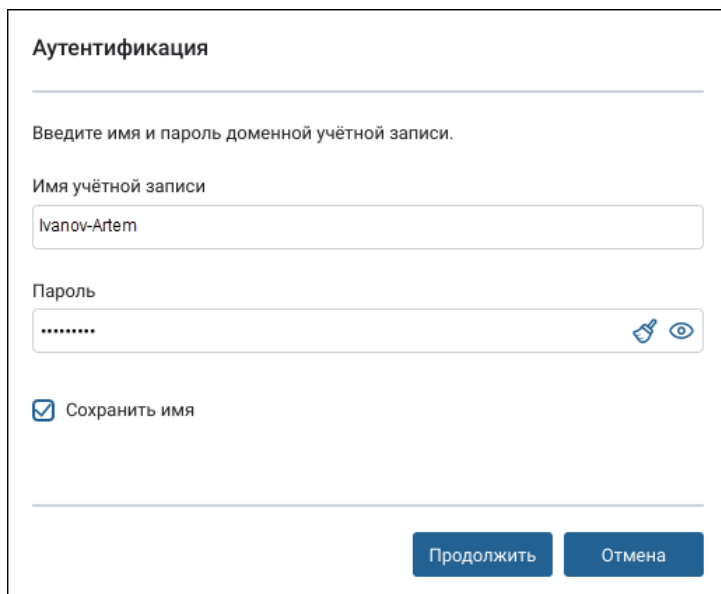
После смены пользователя включите VPN-соединение вручную.

Многофакторная аутентификация

Если администратор назначил вам многофакторную аутентификацию, она начнётся автоматически после установки ключей, включения VPN-соединения или входа в ОС.

- 1 Введите имя и пароль доменной учётной записи и нажмите **Продолжить**.

Выберите **Сохранить имя**, чтобы не вводить имя доменной учётной записи при каждой аутентификации.



Аутентификация

Введите имя и пароль доменной учётной записи.

Имя учётной записи

Ivanov-Artem

Пароль

.....

☒ Сохранить имя

Продолжить Отмена

Рисунок 13. Вход в доменную учётную запись

- 2 Если администратор заранее сообщил вам [способ аутентификации](#):
 - перейдите в приложение для аутентификации и подтвердите вход в уведомлении;
 - введите код в ViPNet Client 5 и нажмите **Подтвердить**.



Примечание. Если для аутентификации используется одноразовый код, появится окно ввода кода. Если для аутентификации используется подтверждение в любом стороннем приложении, перейдите в это приложение и подтвердите вход. Пока вы не подтвердите вход, в ViPNet Client 5 будет отображаться уведомление **Выполняется аутентификация**.

Если вам доступен выбор [способа аутентификации](#), выберите его из списка и нажмите **Продолжить**.

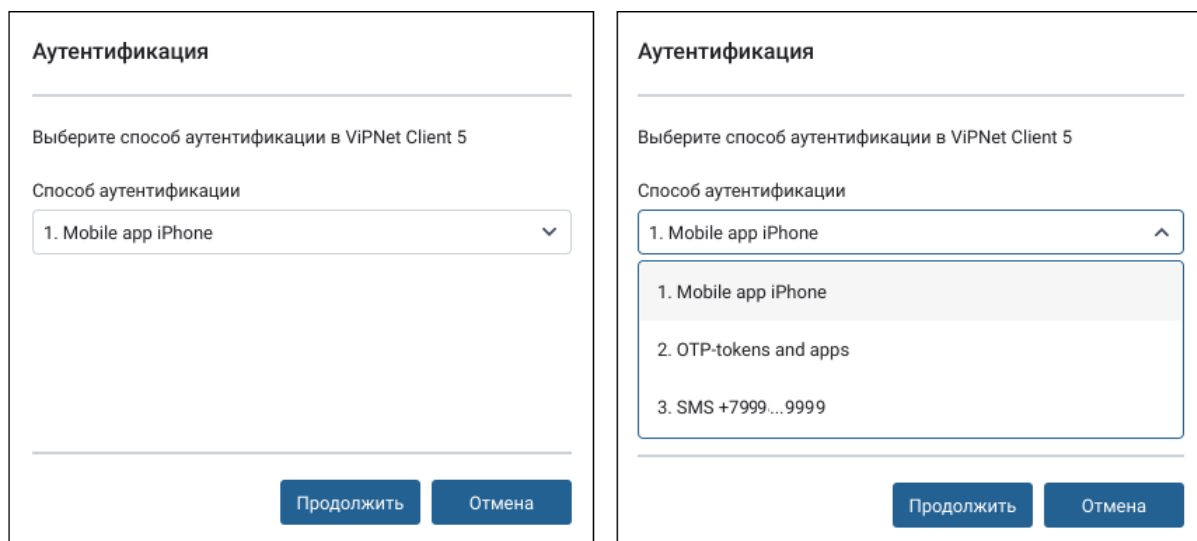


Рисунок 14. Выбор способа аутентификации

- перейдите в приложение для аутентификации и подтвердите вход в уведомлении;
- введите код в ViPNet Client 5 и нажмите **Подтвердить**.



Примечание. Если для аутентификации используется одноразовый код, появится окно ввода кода. Если для аутентификации используется подтверждение в любом стороннем приложении, перейдите в это приложение и подтвердите вход. Пока вы не подтвердите вход, в ViPNet Client 5 будет отображаться уведомление **Выполняется аутентификация**.

Если аутентификация пройдена, вы подключитесь к защищённой сети и сможете работать с корпоративными ресурсами.

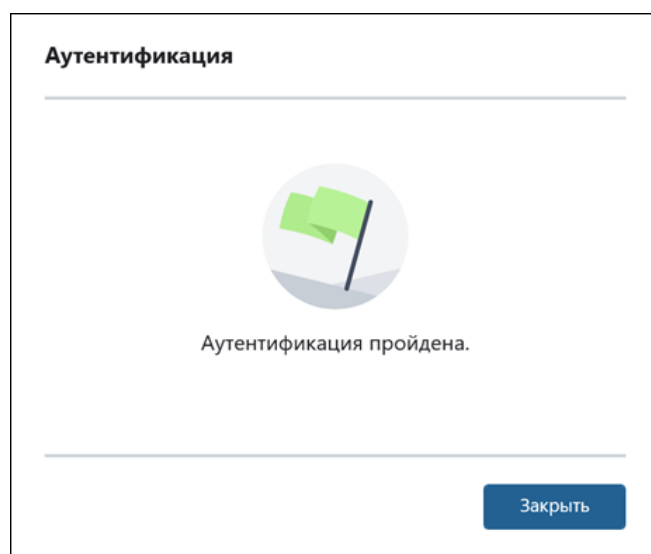


Рисунок 15. Аутентификация пройдена

Если аутентификация не пройдена, вы подключитесь к защищённой сети, но не сможете работать с корпоративными ресурсами. Появится уведомление об этом. Нажмите **Пройти** и пройдите аутентификацию заново.

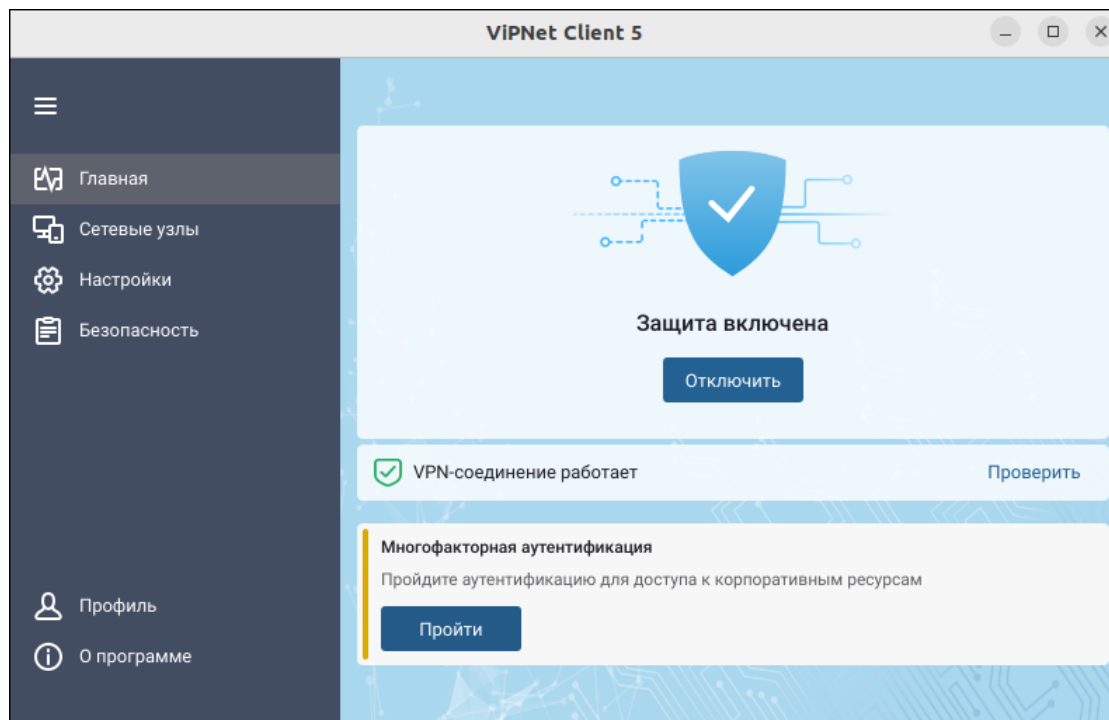


Рисунок 16. Аутентификация не пройдена

Способы многофакторной аутентификации

ViPNet Client 5 for Linux поддерживает несколько способов многофакторной аутентификации. Администратор может:

- разрешить выбирать способ аутентификации при каждом подключении к защищённой сети;
- назначить единственный способ аутентификации;
- назначить аутентификацию только по имени и паролю доменной учётной записи.

Mobile app

Мобильное приложение, которое используется в организации для аутентификации.

- 1 Узнайте у администратора, какое приложение используется в вашей организации и правила работы с ним.
- 2 Перейдите в приложение из шага 1.
- 3 В зависимости от настроек приложения:
 - подтвердите вход в уведомлении;
 - посмотрите одноразовый код и введите его в ViPNet Client 5 for Linux.

Telegram

- 1 Узнайте у администратора, как настроить подтверждение через Telegram.
- 2 Откройте Telegram.
- 3 Подтвердите вход в чате с ботом.

OTP-tokens and apps

Мобильное приложение, которое создаёт одноразовые коды для аутентификации.

- 1 Узнайте у администратора, какое приложение используется в вашей организации: Google Authenticator или Яндекс.Ключ, и правила работы с ним.
- 2 Перейдите в приложение Google Authenticator или Яндекс.Ключ.
- 3 Посмотрите одноразовый код и введите его в ViPNet Client 5 for Linux.

SMS

Введите в ViPNet Client 5 for Linux код из SMS.

Многофакторная аутентификация до входа в Linux

Если администратор назначил вам многофакторную аутентификацию, перед входом в Linux:

- 1 Если вам назначены минимальные полномочия, введите пароль или PIN-код и нажмите **Войти**.
- 2 Введите имя и пароль доменной учётной записи и нажмите **Продолжить**.
Выберите **Сохранить имя**, чтобы не вводить имя доменной учётной записи при каждой аутентификации.
- 3 Если администратор заранее сообщил вам [способ аутентификации](#):
 - перейдите в приложение для аутентификации и подтвердите вход в уведомлении;
 - введите код в ViPNet Client 5 for Linux и нажмите **Подтвердить**.



Примечание. Если для аутентификации используется одноразовый код, появится окно ввода кода. Если для аутентификации используется подтверждение в любом стороннем приложении, перейдите в это приложение и подтвердите вход. Пока вы не подтвердите вход, в ViPNet Client 5 for Linux будет отображаться уведомление **Выполняется аутентификация**.

Если вам доступен выбор [способа аутентификации](#), выберите его из списка и нажмите **Продолжить**.

- перейдите в приложение для аутентификации и подтвердите вход в уведомлении;
- введите код в ViPNet Client 5 for Linux и нажмите **Подтвердить**.



Примечание. Если для аутентификации используется одноразовый код, появится окно ввода кода. Если для аутентификации используется подтверждение в любом стороннем приложении, перейдите в это приложение и подтвердите вход. Пока вы не подтвердите вход, в ViPNet Client 5 for Linux будет отображаться уведомление **Выполняется аутентификация**.

Если аутентификация пройдена, вы подключитесь к защищённой сети и сможете работать с корпоративными ресурсами.

Если аутентификация не пройдена, вы подключитесь к защищённой сети, но не сможете работать с корпоративными ресурсами. Появится уведомление об этом. Нажмите **Пройти** и пройдите аутентификацию заново.

Несколько профилей на устройстве

Вы можете установить до десяти дистрибутивов ключей в ViPNet Client 5 для каждого пользователя ОС. Для каждого дистрибутива ключей будет создан отдельный профиль. Профили можно настроить по-разному и переключаться между ними, например, чтобы работать в разных сетях ViPNet.

Вы можете установить в одном ViPNet Client 5 ключи из разных сетей и с разными:

- форматами (DST и DS5) и криптографией,
- уровнями полномочий,
- способами аутентификации.

Это экспериментальная функция. Особенности:

- Если вы используете ViPNet CSS Connect версии 2.x, то когда вы добавите новый профиль, в текущем профиле удалится история чатов. Чтобы её сохранить, создайте резервную копию в ViPNet CSS Connect. См. руководство пользователя ViPNet CSS Connect.
- Работа с ViPNet Administrator, Policy Manager и ViPNet Деловая почта может быть ограничена.

Добавление профиля



Внимание! В ViPNet CSS Connect версии 2.x удалится история чатов текущего профиля, когда вы добавите новый профиль. Чтобы сохранить историю чатов, создайте резервную копию в ViPNet CSS Connect.

Вы можете добавить до 10 профилей для каждого пользователя ОС.

- 1 Если вы хотите установить ключи с аутентификацией с помощью внешнего устройства, подключите внешнее устройство к компьютеру.
- 2 В ViPNet Client 5 for Linux выберите  **Профиль**.
- 3 В строке **Профиль** нажмите **Действия** > **Добавить профиль**.
- 4 Если вы добавляете профиль первый раз, ознакомьтесь с особенностями использования нескольких профилей на устройстве и нажмите **Добавить профиль**.
- 5 Выберите дистрибутив ключей.
- 6 Введите пароль или PIN-код от внешнего устройства и нажмите **Далее**.

Вы автоматически перейдёте в созданный профиль. В профиле будет включено VPN-соединение. По умолчанию имя профиля совпадает с именем узла. Вы можете [изменить имя профиля](#).

Смена профиля



Внимание! В ViPNet CSS Connect версии 2.x удалится история чатов текущего профиля, когда вы смените профиль. Чтобы сохранить историю чатов, создайте резервную копию в ViPNet CSS Connect.

Чтобы сменить профиль на главном экране:

- 1 Нажмите **Сменить профиль**.

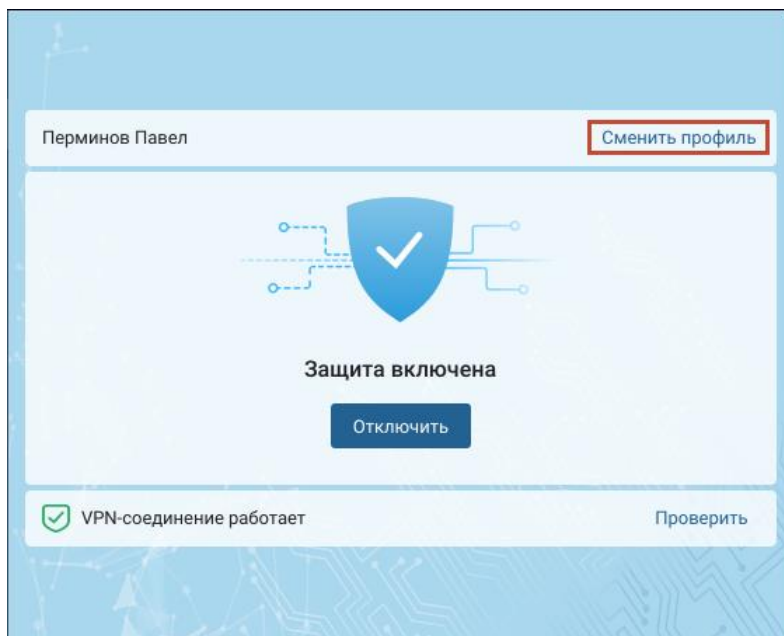


Рисунок 17. Смена профиля

- 2 Выберите профиль и нажмите **Войти**.

Чтобы сменить профиль из вкладки  **Профиль**:

- 1 В строке **Профиль** нажмите **Действия** > **Сменить профиль**.
- 2 Выберите профиль и нажмите **Войти**.

После смены профиля [включите VPN-соединение вручную](#).

Удаление профиля

При удалении профиля **удалятся ключи его узла**.

- 1 В ViPNet Client 5 for Linux выберите  **Профиль**.
- 2 Нажмите **Удалить профиль**.
- 3 Выберите профиль и нажмите **Удалить**.

Удаление профиля

Выберите профиль, который хотите удалить. При удалении профиля удалятся ключи его узла.

Текущий профиль
Перминов Павел
Minimum, Сеть 20616

Перминов Павел
Сеть организации, Сеть 8929

Перминов Павел (token)
Сеть организации, Сеть 8929

УдалитьОтмена

Рисунок 18. Выбор профиля для удаления

- 4 Если вы удаляете текущий профиль, подтвердите удаление.

Профиль и ключи его узла будут удалены из ViPNet Client 5 for Linux.

После удаления текущего профиля вы переключитесь на последний активный профиль.

Смена имени профиля

Имя профиля отображается только на вашем устройстве. По умолчанию оно совпадает с именем узла.

- 1 В ViPNet Client 5 for Linux выберите  Профиль.
- 2 В строке Профиль нажмите Действия > Изменить имя профиля.
- 3 Задайте имя профиля.

Изменение имени профиля

Имя узла

Перминов Павел

Имя профиля: [?](#)

Перминов Павел (ds5) [Сбросить](#)

Сохранить

Отмена

Рисунок 19. Изменение имени профиля

- 4 Нажмите Сохранить.

Проверка VPN-соединения

При [подключении к сети ViPNet](#) программа ViPNet Client 5 автоматически проверяет связь с координатором, являющимся [сервером соединений](#) для вашего узла. Если координатор недоступен, VPN-соединение не работает и взаимодействие с корпоративными ресурсами невозможно.

Вы можете проверить VPN-соединение вручную. Например, если прервалась связь с какими-либо ресурсами защищенной сети. Для этого на главном экране ViPNet Client 5 нажмите **Проверить**. Если нет VPN-соединения, повторите попытку через некоторое время или обратитесь к администратору.



Примечание. Если разница во времени на вашем компьютере и координаторе, который является сервером соединений, больше разрешённой на координаторе, взаимодействие между ними невозможно. В этом случае в ViPNet Client 5 появится уведомление о разнице во времени и рекомендация перевести часы на компьютере.

Смена сервера соединений

Если ваш текущий сервер соединений недоступен, выберите другой координатор в качестве сервера соединений:

- 1 Убедитесь, что [включено VPN-соединение](#).
- 2 Выберите  **Сетевые узлы**.
- 3 В списке узлов выберите координатор.



Примечание. В качестве сервера соединений можно выбрать координатор, для которого указаны IP-адрес или доменное имя. Рекомендуется использовать координатор из собственной сети ViPNet. Если включена настройка **Группа серверов**, выбирайте координатор только из собственной сети ViPNet.

- 4 Нажмите **Сделать активным**.

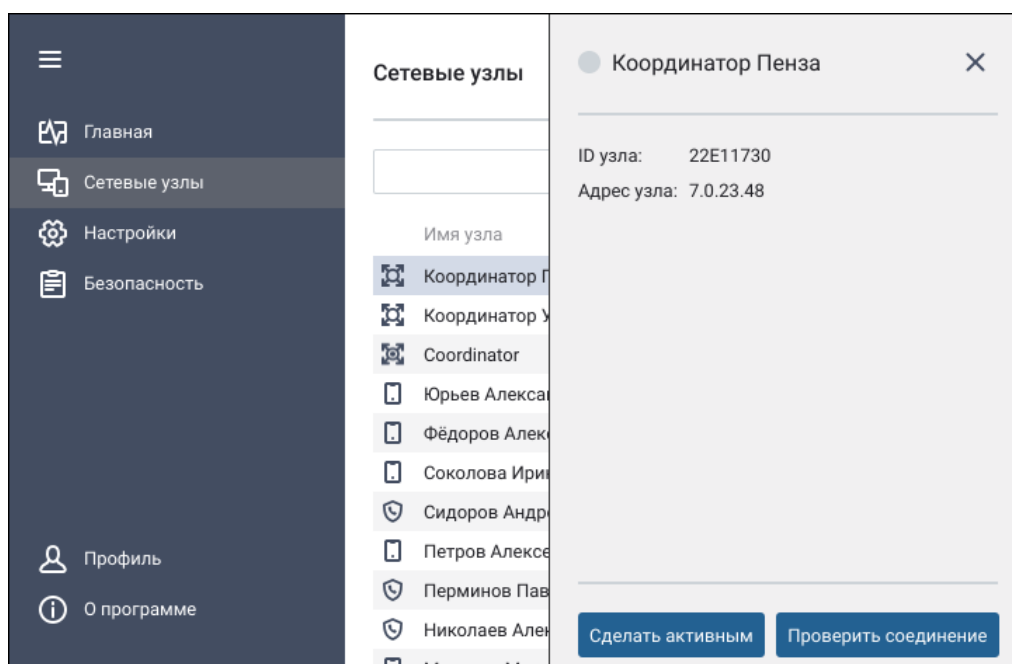


Рисунок 20. Смена сервера соединений

После обновления справочников и ключей в ViPNet Client 5 активным снова станет координатор, заданный в управляющем ПО. Чтобы после обновления активным оставался координатор, выбранный вручную в ViPNet Client 5, [включите настройку Сохранять выбор сервера](#).

Экспериментальные настройки

Чтобы использовать функции, которые ещё тестируются и будут дорабатываться в следующих версиях ViPNet Client 5 for Linux, перейдите в  **Настройки**.

Автоматический выбор сервера соединений



Внимание! В связях узла не должно быть координаторов HW10 и HW50, чтобы настройка **Группа серверов** работала корректно.

Чтобы клиент автоматически переключался на другой сервер соединений вашей сети, если ваш активный координатор недоступен:

- 1 Откройте **Настройки**.
- 2 В разделе **Экспериментальные** включите **Группа серверов**.

Когда ваш активный координатор станет доступен, клиент переключится обратно на него.

Эта настройка по умолчанию включена для клиентов с ключами `*ds5`.

Сохранение выбора сервера соединений

Чтобы у клиента с ключами `*.dst` при получении новых справочников и ключей из управляющего ПО, сервером соединений оставался координатор, выбранный в ViPNet Client 5 for Linux:

- 1 Откройте **Настройки**.
- 2 В разделе **Экспериментальные** включите **Сохранять выбор сервера**.

Если настройка выключена, то при получении новых справочников и ключей сервером соединений будет выбран координатор, заданный в управляющем ПО.

Настройка **Сохранение выбора сервера** отображается только у клиентов с ключами `*.dst`. Чтобы включить сохранение выбора сервера для клиентов с ключами `*.ds5`, [настройте сервер соединений](#) с опцией `--insist` из командной строки.

Смена пароля



Примечание. Смена пароля доступна только клиентам с ключами *.ds5.

Чтобы обезопасить свои данные, рекомендуется менять пароль не реже, чем раз в полгода, после установки ключей и после каждого обновления мастер-ключей в организации. Когда срок действия пароля истечёт, появится напоминание о необходимости сменить пароль.

1 Нажмите **Сменить**.

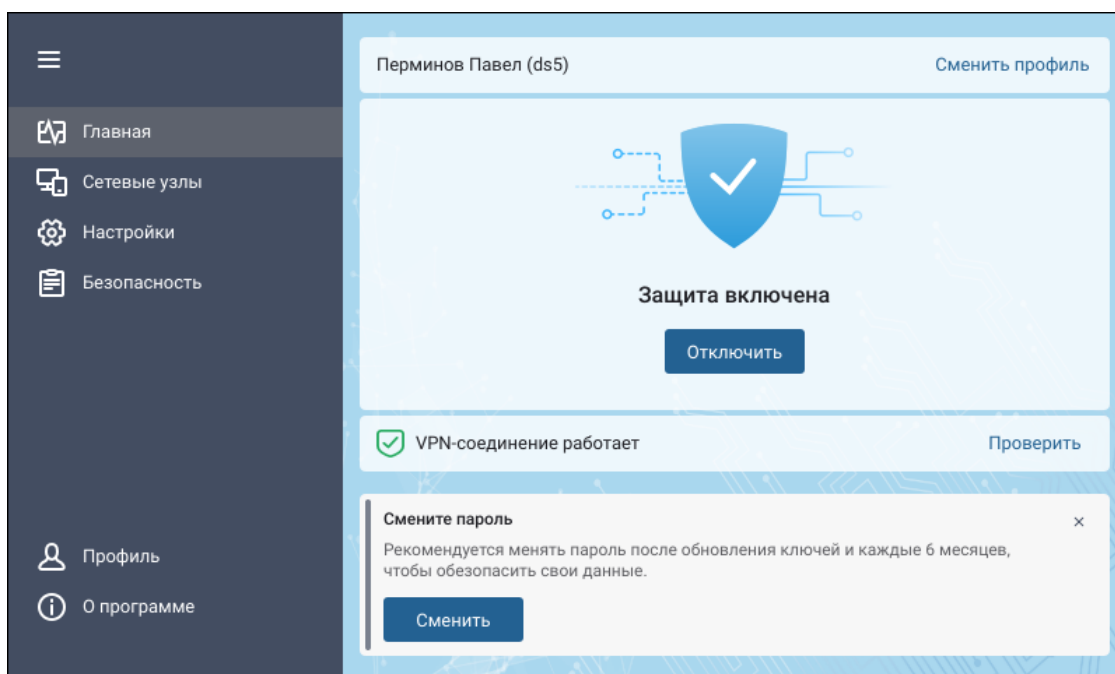


Рисунок 21. Напоминание о смене пароля

2 Выберите **Сменить** и нажмите **Продолжить**.

Смена пароля

Смените пароль узла Сидоров Андрей.

☒

 Сменить

☐

 Отложить на месяц

☐

 Отложить на 6 месяцев

Продолжить

Отмена

Рисунок 22. Смена пароля

3 Введите текущий пароль узла и нажмите **Продолжить**.

4 Задайте новый пароль и нажмите **Продолжить**.

Длина пароля должна быть: латинскими буквами — от 6 до 31 символа, русскими — от 6 до 16.

Пароль должен содержать:

- строчные буквы,
- заглавные буквы,
- цифры.

Пароль может содержать символы !"#%&*()_-=@;:.,^'~?{}[]/|\><`~.

Пароль не должен содержать:

- пробелы,
- один и тот же символ три и более раз подряд.

5 Повторите новый пароль.

6 Когда пароль будет изменён, нажмите **Заккрыть**.

Вы также можете самостоятельно сменить пароль в любое время:

1 [Включите VPN-соединение](#).

2 В ViPNet Client 5 выберите **Профиль** .

3 Нажмите **Сменить пароль**.

4 Введите текущий пароль узла и нажмите **Продолжить**.

5 Задайте новый пароль и нажмите **Продолжить**.

Длина пароля должна быть: латинскими буквами — от 6 до 31 символа, русскими — от 6 до 16.

Пароль должен содержать:

- строчные буквы,
- заглавные буквы,
- цифры.

Пароль может содержать символы !"#%&*()_ -+=@;:.,^' ? { } [] / | \ > < ` ~ .

Пароль не должен содержать:

- пробелы,
- один и тот же символ три и более раза подряд.

6 Повторите новый пароль.

7 Когда пароль будет изменён, нажмите **Заккрыть**.

Просмотр срока действия пароля

Срок действия пароля отображается во вкладке **Профиль** в строке **Пароль**.

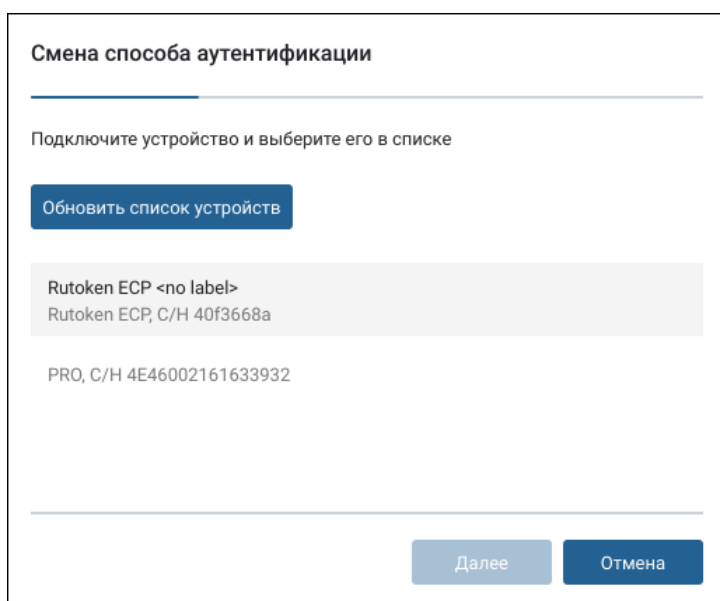
Смена способа аутентификации



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами *.dst на устройствах с архитектурой x86_64.

В ViPNet Client 5 вы можете сменить **способ аутентификации** с аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве. Для этого:

- 1 Подключите внешнее устройство к компьютеру.
- 2 В ViPNet Client 5 выберите **Профиль** .
- 3 Нажмите **Изменить способ аутентификации**.
- 4 Если к компьютеру подключено несколько устройств, в окне **Смена способа аутентификации** выберите нужное устройство в списке и нажмите **Далее**.



Смена способа аутентификации

Подключите устройство и выберите его в списке

Обновить список устройств

Rutoken ECP <no label>
Rutoken ECP, C/H 40f3668a

PRO, C/H 4E46002161633932

Далее Отмена

Рисунок 23. Смена способа аутентификации

- 5 Введите PIN-код 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 изменён.



Примечание. Вы можете изменить PIN-код от внешнего устройства средствами производителя. После этого при первом подключении внешнего устройства потребуются ввести новый PIN-код.

Если не удаётся изменить способ аутентификации при использовании внешнего устройства JaCarta с версией «ПК Единый Клиент JaCarta» 3.0 см. руководство администратора, раздел «Возможные неполадки и способы их устранения».

Просмотр списка узлов

- 1 В ViPNet Client 5 выберите раздел **Сетевые узлы** .

Отобразится список защищённых узлов, с которыми ваш узел может взаимодействовать в защищённой сети.

- 2 Чтобы найти узел в списке, в поле поиска начните вводить его имя или идентификатор.

- 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.

- 5 Чтобы проверить соединение с узлом, выберите его в списке узлов. На панели справа нажмите **Проверить соединение**.

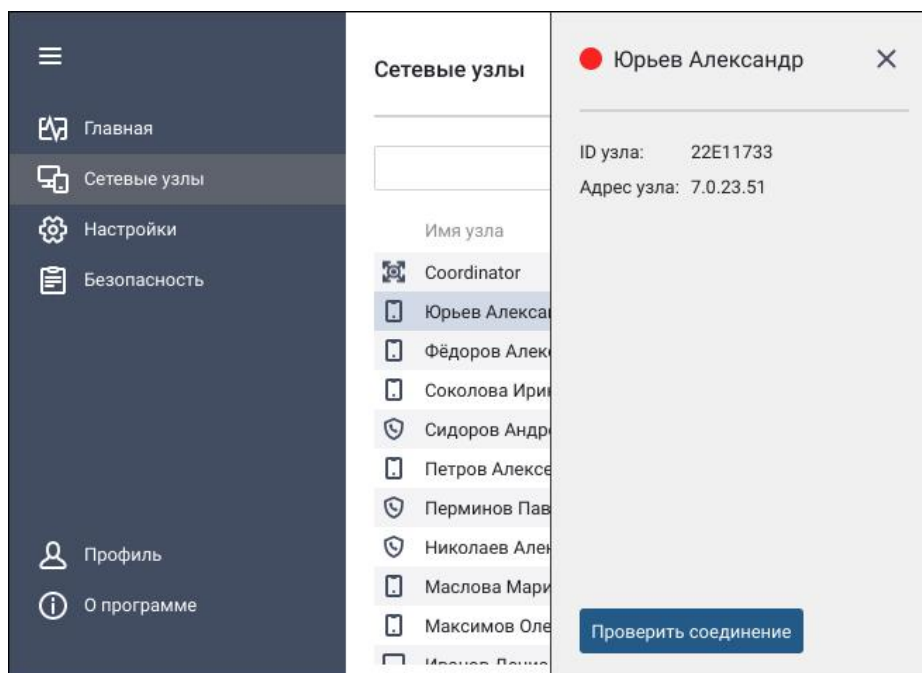


Рисунок 24. Просмотр информации об узлах

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



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

Для проверки доступности ресурсов с помощью команды ping используйте флаг -n. Например:

```
ping -n <ID узла>.vipnet
ping -n ya.ru
```

Просмотр информации о своём узле и о ViPNet Client 5

- 1 Чтобы просмотреть информацию о своём узле, выберите **Профиль** .
- 2 Чтобы просмотреть лицензионное соглашение, выберите **О программе**  > **Лицензионное соглашение**.
- 3 Чтобы просмотреть версию ViPNet Client 5, выберите **О программе** .

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 5 проверку:

- среды функционирования,
- целостности,
- криптографических функций.

Для проверки:

- 1 В ViPNet Client 5 выберите **Безопасность**  и нажмите **Начать проверку**.
- 2 Дождитесь завершения проверки, это может занять несколько минут.

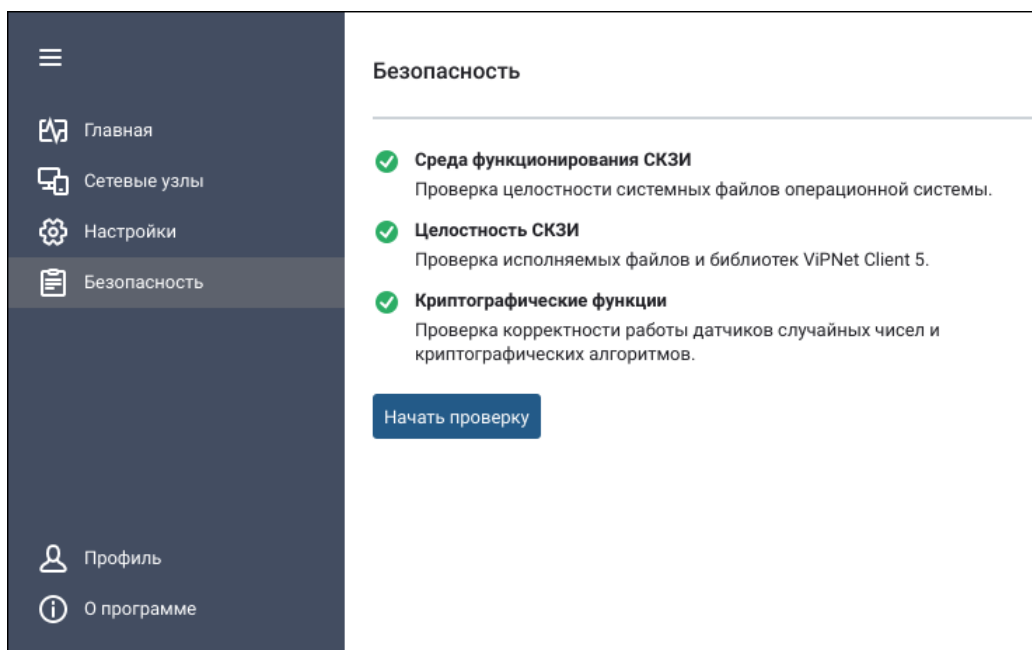


Рисунок 25. Просмотр результатов контроля целостности и работоспособности

В случае нарушения целостности или при неработоспособности компонентов ViPNet Client 5, например, в результате вмешательства посторонних лиц, работа с программой будет невозможна. Обратитесь к администратору для восстановления работоспособности программы.

Обращение в службу технической поддержки

В случае возникновения ошибок в работе ViPNet Client 5, создайте и передайте отчёт о работе программы в ИнфоТеКС:

- 1 В ViPNet Client 5 выберите **О программе** .
- 2 Нажмите **Создать отчет об ошибке**. Опишите проблему и обстоятельства её возникновения и нажмите **Сохранить**.
- 3 Будет создан ZIP-архив с отчётом о работе ViPNet Client 5. Вы можете **Открыть папку** с архивом. Если в клиенте используется несколько профилей, в архиве будут только общие файлы и файлы для текущего профиля.
- 4 Создайте электронное письмо и прикрепите к нему архив с отчётом о работе ViPNet Client 5.
- 5 Отправьте письмо в [ИнфоТеКС](#).



Возможные неполадки и способы их устранения

Проблемы с отображением графического интерфейса ViPNet Client 5 в ОС Ubuntu 22.04 LTS

Если в ОС Ubuntu 22.04 LTS с оконным интерфейсом Wayland некорректно отображается ViPNet Client 5:

- 1 Убедитесь, что в ОС включён оконный интерфейс Wayland.

Для этого перейдите в настройки ОС во вкладку **О системе**. В строке **Оконный интерфейс** должен быть указан "Wayland".

- 2 Переключите оконный интерфейс на Xorg|X11.

Для этого в конфигурационном файле `/etc/gdm3/custom.conf` раскомментируйте строку `#WaylandEnable = false` и перезагрузите ОС.

или:

- 2.1 Завершите текущий сеанс пользователя Linux.
- 2.2 В окне аутентификации выберите пользователя и введите пароль.
- 2.3 В правом нижнем углу нажмите  и выберите **Ubuntu on Xorg**.
- 2.4 Выполните аутентификацию в ОС.

Нарушена целостность компонентов программы ViPNet Client 5 или связанных системных библиотек

Если нарушена:

- целостность исполняемых файлов или библиотек ViPNet Client 5,
- работа датчиков случайных чисел или криптографических алгоритмов,

переустановите ViPNet Client 5:

- 1 Удалите ViPNet Client 5.
- 2 Установите ViPNet Client 5.

Если нарушена целостность справочников:

- 1 Удалите ключи.
- 2 Установите ключи. См. руководство пользователя.

Если одновременно нарушена целостность исполняемых файлов или библиотек ViPNet Client 5, целостность справочников и работа датчиков случайных чисел или криптографических алгоритмов:

- 1 Удалите ключи.
- 2 Удалите ViPNet Client 5.
- 3 Установите ViPNet Client 5.
- 4 Установите ключи в командной строке.

Долгие ответы на команду ping

Если при обращении к корпоративным и открытым ресурсам по доменному имени или через DNS-зону `.vipnet` наблюдаются долгие ответы на команду `ping`, используйте флаг `-n`:

```
user@host:~$ ping -n <доменное_имя_ресурса>
```

Например:

```
user@host:~$ ping -n ya.ru
```

```
user@host:~$ ping -n <идентификатор_узла>.vipnet
```

В списке приложений Astra Linux нет ViPNet Client 5

Обновите меню **Пуск**:

- Из командной строки:

```
root@host:~# fly-wmfunc FLYWM_UPDATE_STARTMENU
```

- Из графического интерфейса:

Правой кнопкой мыши щёлкните меню **Пуск** и выберите **Обновить меню Пуск**.



История версий

В приложении описаны основные изменения в предыдущих версиях ViPNet Client 5 for Linux.

Что нового в версии 5.1.3

- **Несколько профилей на устройстве**

Если пользователю нужно работать в разных сетях ViPNet, вы можете [создать несколько профилей](#) в одном приложении ViPNet Client 5. Установите несколько дистрибутивов ключей и для каждого будет создан отдельный профиль. Профили можно настроить по-разному и переключаться между ними. При смене профиля удаляется история чатов в ViPNet CSS Connect.

- **Взаимодействие с узлами без участия координатора**

Теперь вы можете задать узлы, с которыми клиент будет взаимодействовать напрямую, в режиме «точка-точка». Это экспериментальная функция, которая поможет:

- гибко организовывать топологию сети и оптимизировать маршруты между узлами,
- снизить нагрузку на координаторы, к которым регулярно подключается большое количество узлов в сети.

Например, чтобы снизить нагрузку на координатор, который используется для подключения к серверу ViPNet CSS FileExchange, вы можете настроить подключение клиентов к серверу ViPNet CSS FileExchange напрямую.

- **Обмен межсетевой информацией с доверенными сетями**

Раньше с сетью, в которой на компьютере с центром управления ViPNet Prime установлен клиент с ключами *.ds5, обмениваться межсетевой информацией можно было только вручную. Теперь, если для межсетевого взаимодействия используется шифрование по

алгоритму ГОСТ 28147-89, вы можете настроить автоматический обмен межсетевой информацией.

- **Названия способов аутентификации**

Теперь **при выборе способа аутентификации** вы будете видеть, куда придёт код или уведомление. Изменились названия способов аутентификации:

Прежнее название	Новое название
Приложение для аутентификации	Mobile app <устройство с приложением Multifactor>
Telegram	Telegram <имя пользователя в Telegram>
Google Authenticator или Яндекс.Ключ	OTP-tokens and apps
СМС	SMS <номер телефона, на который придёт код>

- **Изменения поддерживаемых ОС**

Поддержка:

- Устройство MIG T8W ITAM-301807 с ОС специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7 в мобильном режиме).
- Операционная система общего назначения «ОСнова» ДВНБ.10001-01 в режиме замкнутой программной среды.

Прекращение поддержки устройства сбора и передачи данных МИРТ-881-D6.1.

- **Поддержка Winbind для Active Directory**

Раньше работу под доменным пользователем вы могли настроить только с помощью SSSD, теперь вы можете использовать Winbind.

- **Возможность запретить менять расширенные настройки локально**

Теперь в управляющем ПО вы можете запретить пользователям изменять расширенные настройки на устройстве. Задайте эти настройки в секции secured, и они будут иметь приоритет над настройками, заданными по умолчанию и вручную. Эти настройки можно будет изменить только из управляющего ПО.

- **Установка через репозиторий ALD Pro**

Теперь вы можете установить ViPNet Client 5 на устройства с Astra Linux Special Edition, введённой в домен ALD Pro, с помощью репозитория.

- **Дополнительная проверка служебных конвертов**

Теперь ViPNet Client 5 проводит больше проверок, чтобы подтвердить подлинность служебных конвертов. Некорректные конверты не обрабатываются и не применяются. Клиент блокирует их и отправляет уведомление о таких конвертах на узел с ViPNet ЦУС или с центром управления ViPNet Prime. Вы можете посмотреть эту информацию в журнале клиента, установленного на этом узле. Рекомендуется регулярно отслеживать попытки доставить подозрительные служебные конверты на защищённые узлы.

Внимание! Если на узле с ViPNet ЦУС или с центром управления ViPNet Prime:

- в вашей сети установлена актуальная версия ViPNet Client,
- в доверенной сети установлена прошлая версия ViPNet Client,

В вашей сети перестанут автоматически приниматься обновления справочников, полученные из этой доверенной сети. Остальное межсетевое взаимодействие не нарушится.



Чтобы обновления справочников принимались, попросите администраторов доверенной сети установить на узле с ViPNet ЦУС или с центром управления ViPNet Prime актуальную версию ViPNet Client:

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

До установки актуальной версии в доверенной сети вы можете установить обновления вручную. Для этого получите от администратора доверенной сети обновления доверенным способом.

- **Изменения в контроле защищённого трафика**

Клиент проверяет целостность входящих пакетов и их актуальность, чтобы поддерживать уровень безопасности в защищённой сети. Если какой-то узел отправляет пакеты, целостность которых нарушена, клиент временно блокирует трафик от этого узла. Если пакет устарел, клиент не принимает его. Теперь в расширенных настройках клиента администратор может управлять блокировкой трафика от отправителя некорректных пакетов и задавать допустимый интервал времени между отправлением и получением пакета.

- **Исключения из блокировки пользовательского трафика**

Из управляющего ПО вы можете задать узлы, на которых будет разрешён пользовательский трафик, даже если его блокирует сторонний процесс или не пройдены многофакторная аутентификация и проверка политики ZTNA. Перечислите эти узлы в секции policies в расширенных настройках.

- **Лицензионное соглашение**

Чтобы использовать ViPNet Client 5, нужно принять лицензионное соглашение.

- **ViPNet Client 5 SDK**

Добавлены новые функции. Подробнее см. справочник разработчика.

Что нового в версии 5.0.1

- **Новое поколение ViPNet Client 5**

Новая версия ViPNet Client 5 относится к пятому поколению продуктов ViPNet:

- Добавлена возможность установить ключи в формате DS5.
При этом ключи в формате DST продолжают поддерживаться.
- Поддержана универсальная лицензия для клиентов пятого поколения.
- Добавлены новые протоколы взаимодействия узлов.
- Обновлён интерфейс программы.

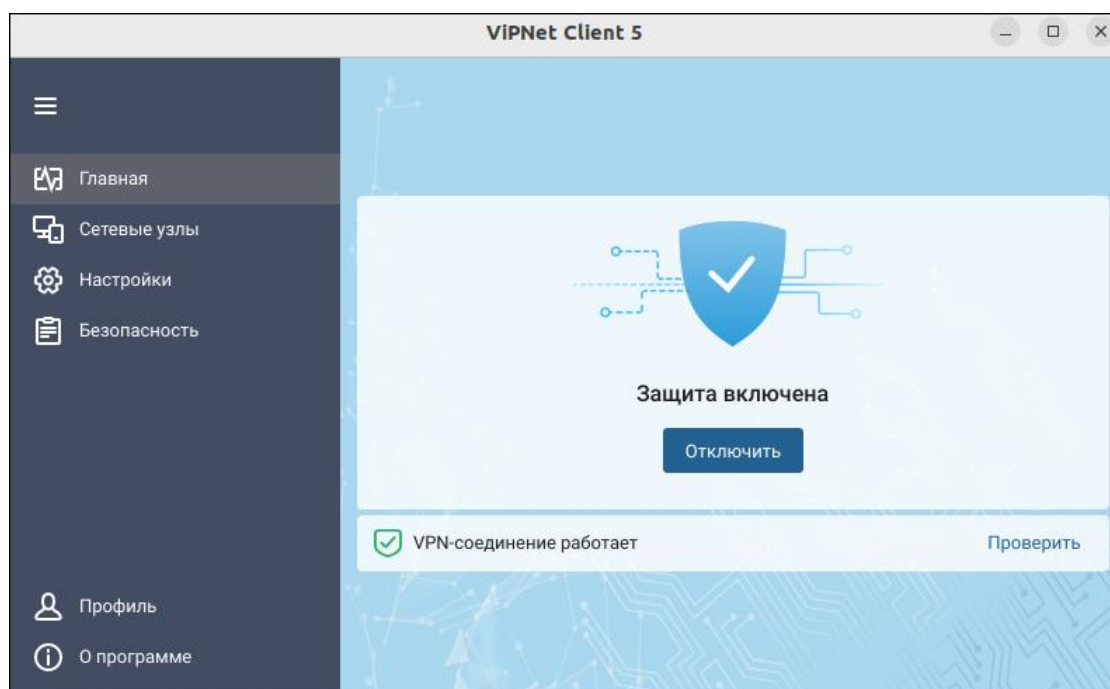


Рисунок 26. Главный экран ViPNet Client 5

- **Туннелирование устройств**

Вы можете настроить ViPNet Client 5 для туннелирования трафика таких устройств, как видеорекамеры и датчики, и для создания защищённой сети в случаях, когда нельзя использовать программно-аппаратные решения. Подробнее см. документ «ViPNet Client 5 for Linux. Использование функции туннелирования».

- **Многофакторная аутентификация**

В ViPNet Client 5 вы можете увеличить уровень безопасности защищённой сети с помощью дополнительной защиты при подключении к ней. Чтобы исключить риск несанкционированного доступа к вашим данным, [настройте многофакторную аутентификацию](#). Для доступа к корпоративным ресурсам потребуется ввести данные доменной учётной записи и использовать специальное приложение для аутентификации.

ViPNet Client 5 поддерживает [несколько приложений для аутентификации](#). В зависимости от настроек, в приложении нужно:

- Нажать кнопку в уведомлении о попытке входа, чтобы подтвердить, что это вы проходите аутентификацию. Уведомление приходит при каждой попытке входа.
- Получить одноразовый код и ввести его в ViPNet Client 5. Одноразовый код действителен ограниченное время и уникален при каждом входе.
- Экспериментальные настройки

- **Автоматический выбор сервера соединений**

Чтобы работать с корпоративными ресурсами, ViPNet Client 5 подключается к серверу соединений. Раньше, если активный сервер соединений становился недоступен, нужно было вручную назначать активным другой сервер.

Теперь, чтобы не прерывать выполнение рабочих задач для смены координатора, вы можете [включить автоматический выбор активного сервера соединений](#) из серверов вашей сети ViPNet. Если ваш сервер соединений станет недоступен, ViPNet Client 5 переключится на другой.

Для корректной работы этой функции в связях узла не должно быть координаторов HW10 и HW50.

- **Централизованное управление настройками**

Администратор может управлять расширенными настройками ViPNet Client 5 в управляющем ПО или задавать их вручную на устройстве пользователя. Они передаются на устройства в составе справочников и вступают в действие автоматически.

- **Блокировка трафика открытой сети**

Вы можете заблокировать весь открытый IP-трафик устройства, когда включено VPN-соединение. Открытый IP-трафик, необходимый для работы ОС Linux и ViPNet Client 5, при этом не блокируется.

- **Алгоритм назначения IP-адресов для узла**

Вы можете выбрать альтернативный алгоритм назначения IP-адресов. В одной сети должны использоваться одинаковые алгоритмы. Описание альтернативных алгоритмов см. в «ViPNet Administrator 4. Настройка алгоритма назначения сетевых адресов»

- **Способ выбора координатора**

Если несколько координаторов из связей клиента туннелируют одинаковые IP-адреса и связь с одним из координаторов пропадает, клиент определяет, какие IP-адреса стали недоступны, и подключается к другому координатору, который туннелирует эти IP-адреса. По умолчанию клиент выбирает координатор с меньшим идентификатором узла. Вы можете настроить выбор активного координатора из группы серверов.

- **Переключение на протокол TCP, если протокол UDP не работает**

Если провайдер блокирует передачу трафика по протоколу UDP, подключение к защищённой сети может работать нестабильно. В таких условиях вы можете настроить передачу данных по протоколу TCP, чтобы восстановить стабильную связь с координатором и защищённой сетью.

- **Защищённое взаимодействие между узлами без участия координатора**

Вы можете включить модуль `mdns`, чтобы искать узлы в локальной сети по протоколам MulticastDNS и DNS Service Discovery и взаимодействовать с ними напрямую (без участия координатора). По умолчанию в модуле `mdns` используется шифрование ГОСТ 34.12-2018 «Кузнечик».

- **Совместная работа с ViPNet Coordinator HW 5**

Обеспечено взаимодействие клиентов с ключами `*.ds5` с координаторами пятого поколения по новым протоколам с шифрованием по ГОСТ 34.12-2018 «Магма» и «Кузнечик».

- **Совместная работа с ViPNet EndPoint Protection Linux версии 1.6.0 и выше**

Обеспечена совместная работа с программой ViPNet EndPoint Protection Linux на одном компьютере для защиты информации от вредоносного ПО. Подробнее см. «ViPNet EndPoint Protection Linux. Руководство администратора».



Политика конфиденциальности

В этом разделе мы описываем меры по обеспечению безопасности персональных данных, а также меры по защите прав субъектов персональных данных, реализованные в продукте ViPNet Client 5 for Linux.

Персональные данные — это любые сведения, касающиеся физического лица, которые могут быть использованы для прямой или косвенной идентификации.

Компания ИнфоТеКС придерживается принципов соблюдения прав и свобод субъектов данных в отношении их персональных данных. Для обеспечения прав субъектов в продукте ViPNet Client 5 for Linux реализованы меры, обеспечивающие безопасность персональных данных, и функциональность, помогающая соблюсти права субъектов данных.

Ключевые принципы обработки персональных данных

Уже на этапе разработки продукта мы приняли меры, предназначенные для эффективного осуществления принципов обработки персональных данных:

- **Принцип прозрачности, справедливости и законности в обработке и использовании персональных данных.**

ИнфоТеКС предоставляет подробную информацию об обработке данных, которые могут считаться персональными. При этом учитывается баланс интересов субъекта данных и владельца продукта.

- **Принцип ограничения целью.**

Ограничение обработки персональных данных указанными, явными и законными целями. Цели обработки персональных данных явно указываются (см. «Для чего используются

персональные данные»), а обработка данных продуктами остается в пределах объема, необходимого для достижения этих целей, и не производится в иных целях.

- **Принцип минимизации данных.**

Данные, собранные и сохраненные продуктами, ограничены до разумного уровня и не превышают того, что необходимо для целей обработки.

- **Принцип точности.**

Продукты ИнфоТеКС предлагают возможность обновления, исправления или удаления личных данных, если это необходимо, при условии, что это не нарушает надлежащий баланс интересов субъекта данных и владельца продукта.

- **Принцип ограничения хранения.**

Продукты ИнфоТеКС обеспечивают процедуру, которая поддерживает своевременное и регулярное удаление личных данных с целью предотвращения неконтролируемого хранения личных данных.

- **Принцип целостности и конфиденциальности.**

Для обеспечения адекватной безопасности личных данных в продуктах используются методы для разработки безопасного программного обеспечения, которые учитывают различные аспекты, от проектирования до эксплуатации и использования продукта, с целью защиты от несанкционированного или незаконного использования, обработки и случайной потери, для защиты от непреднамеренного уничтожения или непреднамеренного повреждения личных данных.

Что является нарушением безопасности персональных данных

Нарушение безопасности персональных данных — это «нарушение безопасности, ведущее к случайному или незаконному уничтожению, потере, изменению, несанкционированному разглашению пересылаемых, хранимых или иным образом обрабатываемых персональных данных или к несанкционированному доступу к ним».

В случае нарушения безопасности персональных данных контролёр, ответственный за обработку данных, обязан:

- Немедленно сообщить о нарушении в компетентный надзорный орган, если нарушение может привести к риску для прав и свобод физических лиц.
- Немедленно сообщить субъекту данных о нарушении, если оно может привести к высокому риску для их личных прав и свобод.
- Каждое нарушение должно быть задокументировано ответственным органом независимо от каких-либо обязательств по отчетности, включая все факты, связанные с нарушением безопасности персональных данных (количество затронутых лиц, количество и категории затронутых записей данных), последствия и принятые меры.

В продуктах ИнфоТеКС, таких как ViPNet TIAS, ViPNet IDS NS, IDS HS, уже есть решения для поддержки подотчетности ответственных контролёров, оценки рисков и выявления нарушений безопасности данных.



Примечание. ViPNet Client 5 for Linux не обрабатывает конфиденциальные персональные данные («особые категории персональных данных»), такие как расовое и этническое происхождение, политические взгляды, религиозные или идеологические убеждения, членство в профсоюзах, генетические данные, биометрические данные для уникальной идентификации физического лица, данные о здоровье или данные о половой жизни или сексуальной ориентации физического лица.

Данные об активности пользователя ViPNet Client 5 for Linux

ViPNet Client 5 for Linux фиксирует локально в журнал администратора все действия пользователя по настройке ViPNet Client 5 for Linux, а также действия по проверке целостности продукта.

ViPNet Client 5 for Linux копирует в локальный журнал событий `system-journal` первые 10 Мбайт журнала операционной системы, где содержится информация о входе и выходе пользователя из операционной системы.

Данные устройства пользователя ViPNet Client 5 for Linux

Для выявления проблем в работе ViPNet Client 5 for Linux существует функция формирования отчета, которая позволяет сформировать по инициативе пользователя ViPNet Client 5 for Linux диагностическую информацию и передать её в [службу поддержки](#). В частности, отчет содержит:

- имя устройства;
- версию ОС;
- статистику загрузки памяти;
- настройки сетевых интерфейсов;
- список загруженных в память процессов.

Данные пользователя ViPNet-сети

Для защиты канала связи в процессе развертывания и работы ViPNet Client 5 for Linux получает сформированную управляющим приложением справочную информацию, включающую информацию о связанных с ним устройствах и пользователях, а именно:

- ViPNet-идентификатор устройства;
- ViPNet-адрес устройства;
- ViPNet-имя устройства — может содержать имя пользователя;
- имя пользователя;
- ViPNet-идентификатор пользователя.

Также данную информацию в виде отчета пользователь может сформировать средствами ViPNet Client 5 for Linux и передать в службу поддержки производителя.

Данные об активности устройства пользователя ViPNet-сети

ViPNet Client 5 for Linux использует встроенную функцию сетевого экрана для фильтрации трафика устройства, на котором он установлен, и фиксирует локально в журнале IP-пакетов информацию о сетевой активности устройства, содержащую:

- IP-адреса устройств отправителя и получателя.
- Интервал времени сетевой активности.
- ViPNet-имя и идентификатор ViPNet-узлов отправителя и получателя.

Также ViPNet Client 5 for Linux позволяет отобразить сетевую доступность связанных с ним устройств пользователей сети ViPNet.

Данная информация используется для диагностики состояния сети ViPNet и диагностики работы приложения ViPNet Client 5 for Linux.

Для чего используются персональные данные

Описание причин, по которым обрабатываются персональные данные	Категории персональных данных
Обеспечение защищенного канала связи	Данные пользователя сети ViPNet
Обеспечение неотказуемости действий	Данные об активности пользователя ViPNet Client 5 for Linux
Диагностика работы сети ViPNet	Данные об активности устройства пользователя сети ViPNet
Диагностика работы ViPNet Client 5 for Linux	Данные устройства пользователя сети ViPNet Данные пользователя сети ViPNet

Кому предоставляется доступ к персональным данным

В рамках процессов по обеспечению информационной безопасности, поддерживаемых ViPNet Client 5 for Linux, персональные данные могут предоставляться следующим категориям получателей.

Категория получателей	Причина предоставления доступа
Администратор сети ViPNet	Диагностика работы сети ViPNet
Пользователь	Диагностика работы ViPNet Client 5 for Linux
ViPNet Client 5 for Linux	Обеспечение защищенного канала связи

Как долго хранятся персональные данные

ViPNet Client 5 for Linux обеспечивает автоматизированные процессы удаления данных, собираемых ViPNet Client 5 for Linux и хранящихся в приложении, которые описаны ниже. Если

контролёр считает необходимым дополнительное хранение, он должен позаботиться о подходящем хранении сверх периодов, предусмотренных ViPNet Client 5 for Linux, за пределами продукта.

Место хранения	Категории персональных данных	Сроки или условия хранения
ViPNet Client 5 for Linux	- Журнал IP-пакетов, содержащий информацию о сетевой активности устройства, на котором установлен ViPNet Client 5 for Linux. Ротация журнала происходит для данных старше 7 дней. - Журнал событий ОС, содержащий информацию о входах и выходах пользователя из ОС.	Удаляется при удалении ViPNet Client 5 for Linux
	Журнал администратора, содержащий информацию о действиях пользователя по настройке ViPNet Client 5 for Linux, а также действиях по проверке целостности продукта.	Удаляется при достижении объема в 10 МБайт и при удалении ViPNet Client 5 for Linux
	Справочники, содержащие информацию о связанных с устройством пользователя ViPNet Client 5 for Linux узлов ViPNet-сети.	Не удаляются при удалении ViPNet Client 5 for Linux

Как ИнфоТеКС помогает обеспечивать права субъектов данных

ИнфоТеКС предлагает следующие инструменты и документацию для поддержки и облегчения реализации прав субъектов данных.

- **Право доступа.**

Субъект данных имеет право запрашивать у контролёра подтверждение относительно того, обрабатываются ли относящиеся к нему персональные данные, и если так, то он имеет право на доступ к персональным данным и следующей информации:

- цель обработки;
- категория персональных данных;
- получатели или категории получателей, которым были раскрыты персональные данные;
- продолжительность хранения.

Субъекты данных также могут иметь право на получение копии персональных данных, которые являются предметом обработки.

Вышеуказанная информация может быть предоставлена субъектам данных из этого раздела. Информацию о связанных с узлом пользователя узлах ViPNet, информацию о сетевой активности устройств пользователя, информацию об активности пользователя ViPNet Client 5 for Linux можно посмотреть в интерфейсе приложения (см. [Просмотр информации о своём узле и о ViPNet Client 5](#)).

- **Право на уточнение данных.**

Уточнение обрабатываемых ViPNet Client 5 for Linux данных невозможно.

- **Право на удаление данных (право на забвение).**

Субъект данных имеет право на удаление без неоправданной задержки относящихся к нему персональных данных в случае, если персональные данные больше не требуются для целей, для которых они были собраны, а также в случае, если субъект данных возражает против обработки и отсутствуют имеющие преимущественную силу легитимные основания для обработки.

Удаление данных субъекта данных происходит при удалении приложения, а также при удалении узла пользователя в управляющем приложении.

- **Право на переносимость данных.**

Право на переносимость данных может существовать в отношении данных субъекта данных, которые предоставили контроллеру и обработка которых основана на согласии на исправление или на автоматизированной процедуре. ViPNet Client 5 for Linux не включает возможность получения согласия на операции обработки данных, осуществляемых с помощью ViPNet Client 5 for Linux. Кроме того, субъекты данных не будут активно предоставлять личные данные. Соответственно, продукт не поддерживает переносимость данных.

- **Право на возражение и ограничение обработки данных.**

Право на возражение и ограничение обработки данных в контексте данного продукта может быть реализовано только с помощью удаления узла пользователя в управляющем приложении.



Термины и сокращения

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 Prime

ПО для централизованного управления решениями ViPNet. Позволяет управлять конфигурацией сети (включая устройства, пользователей и лицензии), централизованно обновлять ПО ViPNet и выполнять мониторинг состояния сети ViPNet.

Включает в себя основные функциональные модули:

- ViPNet VPN — модуль управления топологией сети, регистрирует защищаемые устройства и задаёт связи между ними.
- ViPNet Network Visibility System — модуль мониторинга состояния сети ViPNet и входящих в неё устройств.
- ViPNet Policy Management — модуль централизованного управления политиками безопасности узлов сети ViPNet.

Дистрибутив ключей

Файл с расширением *.dst или *.ds5 для каждого пользователя узла ViPNet. Создаётся в управляющем ПО ViPNet. Содержит справочники, ключи и файл лицензии для первичного запуска и последующей работы программы ViPNet на сетевом узле. Для работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Зона .vipnet

Пространство доменных имён вида <идентификатор_узла_ViPNet>.vipnet и <IP-адрес_туннеля>.<идентификатор_туннелирующего_координатора>.vipnet. Внутри ViPNet Client 5 разрешаются в IP-адреса видимости этих узлов.

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. Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в управляющем ПО ViPNet Administrator или ViPNet Prime в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Роль

Функциональность сетевого узла, которая решает целевые и служебные задачи 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.

Набор ролей для каждого сетевого узла задаёт администратор сети ViPNet в программе ViPNet Administrator.

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 управляющем ПО.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность защищённых узлов ViPNet. Сеть ViPNet имеет наложенную маршрутизацию, обеспечивающую взаимодействие узлов сети. Каждая сеть ViPNet имеет свой уникальный номер.

Суперпользователь (root)

Учётная запись в UNIX-системах, пользователь которой наделён 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 для защиты соединений между устройствами локальных сетей, которые связаны через интернет или другие публичные сети. Шифрование трафика устройств выполняется координаторами, установленными на границах локальных сетей.