



ViPNet Client 5 for Windows

Руководство пользователя

Версия продукта: 5.5

© АО «ИнфоТеКС», 2025

ФРКЕ.00403-01 34 01

Версия продукта 5.5

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 Windows приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Client 5 for Windows.

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.....	6
О документе.....	7
Соглашения документа.....	7
О программе	8
Что нового в версии 5.5.....	9
Обратная связь.....	10
 Глава 1. Подготовка к работе	11
Установка ViPNet Деловая почта	12
Переход с ViPNet Client 4.5.....	13
Доступ в ViPNet Деловая почта.....	14
Установка, обновление и удаление	15
Переустановка	15
Способы аутентификации в ViPNet Client 5.....	16
Подготовка к работе с внешними устройствами	16
Установка ключей.....	18
Обновление ключей.....	20
Удаление ключей	21
Запуск и завершение работы.....	22
 Глава 2. Работа с ViPNet Client 5	24
Многофакторная аутентификация.....	25
Способы многофакторной аутентификации.....	27
Многофакторная аутентификация до входа в Windows	28
Несколько профилей на устройстве.....	30
Добавление профиля	30
Смена профиля.....	33
Удаление профиля	34
Смена имени профиля.....	34
Просмотр информации о своём узле.....	35
Просмотр списка узлов.....	36
Поиск узлов	37
Проверка связи с координатором	38
Обращение в службу поддержки	39

Глава 3. Настройки ViPNet Client 5	40
Смена способа аутентификации в клиенте	41
Смена пароля	42
Смена сервера соединений	44
Экспериментальные настройки	45
Контроль целостности и работоспособности	46
Настройка журнала событий	47
Применение настроек из конфигурационного файла	48
Глава 4. Работа в командной строке	49
Переход с ViPNet Client 4.5	50
Доступ в ViPNet Деловая почта	50
Установка ключей	51
Обновление ключей	53
Удаление ключей	54
Запуск и завершение работы	55
Несколько профилей на устройстве	57
Проверка VPN-соединения	60
Смена способа аутентификации	61
Смена сервера соединений	63
Экспериментальные настройки	63
Просмотр информации о своём узле	64
Просмотр списка узлов	65
Поиск узлов	65
Смена пароля	66
Настройка параметров журнала событий	67
Обращение в службу поддержки	68
Приложение А. Возможные неполадки и способы их устранения	69
Нарушена целостность компонентов программы ViPNet Client 5 или связанных системных библиотек	69
Пропадает удалённое подключение к узлу	70
Изменился сервер соединений	70
Приложение В. История версий	71
Что нового в версии 5.4	71
Что нового в версии 5.2	71
Что нового в версии 5.0	73

Приложение С. Политика конфиденциальности 77

Приложение D. Термины и сокращения 83



Введение

О документе	7
О программе	8
Что нового в версии 5.5	9
Обратная связь	10

О документе

Документ поможет вам установить ViPNet Client 5 for Windows (далее — ViPNet Client 5 for Windows, клиент) на компьютеры с Windows и работать в [сети ViPNet](#).

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 только в режиме администратора, выделены красным цветом:
`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]`
- Если можно указать один из нескольких параметров, допустимые варианты заключены в фигурные скобки и разделены вертикальной чертой:
`команда {вариант-1 | вариант-2}`

О программе

ViPNet Client 5 — клиент для работы в защищённой сети. Он защищает трафик на компьютерах с Windows путём шифрования IP-пакетов.

С помощью ViPNet Client 5 ваш компьютер станет [узлом сети ViPNet](#) (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 компьютер с ViPNet Client 5 программу ViPNet CSS Connect и [ViPNet Деловая почта](#).

Что нового в версии 5.5

- **Проверка безопасности узла**

Администратор может настроить блокировку доступа к корпоративным ресурсам для узлов, которые не соответствуют требованиям безопасности. Для этого в ViPNet Prime включите **Блокировка VPN без ViPNet EPP**. Корпоративные ресурсы будут доступны, только если на компьютере установлен ViPNet EPP Агент под управлением ViPNet EPP Сервер и выполняются проверки безопасности.

Подробнее см. руководство администратора «Совместная работа с ViPNet EPP Агент».

- **Поиск координатора по туннелю**

Теперь вы можете [найти координатор](#) по реальному или виртуальному адресу узла, который он туннелирует.

- **Проверка соединения с узлом**

Раньше в графическом интерфейсе ViPNet Client 5 вы могли [проверить соединение](#) только с координатором, теперь — с любым узлом.

- **Поддержка работы с DNS-серверами из настроек ОС**

Раньше, если DNS-запросы открытой сети не удавалось разрешить на защищённых DNS-серверах, то они передавались только на доверенные DNS-серверы, заданные в расширенных настройках ViPNet Client 5. Теперь они передаются и на DNS-серверы, заданные в настройках ОС. Это повышает стабильность работы с открытыми ресурсами.

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

Подготовка к работе

Установка ViPNet Деловая почта	12
Переход с ViPNet Client 4.5	13
Установка, обновление и удаление	15
Способы аутентификации в ViPNet Client 5	16
Установка ключей	18
Обновление ключей	20
Удаление ключей	21
Запуск и завершение работы	22

Установка ViPNet Деловая почта

Чтобы обмениваться электронной почтой в защищённой сети, установите ViPNet Деловая почта. Вы можете сделать это при установке ViPNet Client 5. ViPNet Деловая почта работает только с клиентами с ключами *.dst.

Если ранее вы пользовались ViPNet Client версии 4.5.x, [перейдите в ViPNet Client 5](#).

Если ранее вы не пользовались ViPNet Client версии 4.5.x:

- 1 Получите установочный файл ViPNet Client версии 4.5.x (*.exe или *.msi) у администратора или в ИнфоТеКС.
- 2 Запустите установочный файл ViPNet Client 4.5.x.
- 3 Чтобы использовать ViPNet Деловая почта, примите условия лицензионного соглашения.
- 4 Нажмите **Компоненты и параметры**.
- 5 На странице **Изменение состава компонентов ПО ViPNet** оставьте только флажок **ViPNet Деловая почта** и нажмите **Далее**.
- 6 Нажмите **Установить**.
- 7 После установки перезагрузите компьютер.
- 8 [Установите ViPNet Client 5](#).
- 9 [Установите ключи в ViPNet Client 5](#).
- 10 [Настройте доступ в ViPNet Деловая почта](#).

Переход с ViPNet Client 4.5

Предварительные действия

- 1 Установите ViPNet Client 5 for Windows.
- 2 Запустите ViPNet Client 4.5 от имени пользователя, которого хотите перевести в ViPNet Client 5 for Windows.
- 3 Если в ViPNet Client 4.5:
 - задан способ аутентификации по сертификату на устройстве, измените способ аутентификации на **Пароль** или **Персональный ключ на устройстве**.
См. руководство пользователя ViPNet Client 4.5, раздел «Изменение способа аутентификации пользователя».
 - в пароле от дистрибутива ключей есть русские буквы, измените пароль. Можно перенести только ключи, в пароле которых нет русских букв.
См. руководство пользователя ViPNet Client 4.5, раздел «Смена пароля пользователя».
- 4 Если в ViPNet Client 4.5 используется способ аутентификации **Персональный ключ на устройстве**, подключите устройство к компьютеру.

Перенос ключей



Примечание. Чтобы сразу пользоваться корпоративными ресурсами, [переносите ключи с помощью командной строки от имени администратора](#). Иначе корпоративные ресурсы не будут доступны, пока администратор не отправит вам обновление настроек DNS.

- 1 В ViPNet Client 5 for Windows выберите **Перенести ключи из ViPNet Client 4.5**.

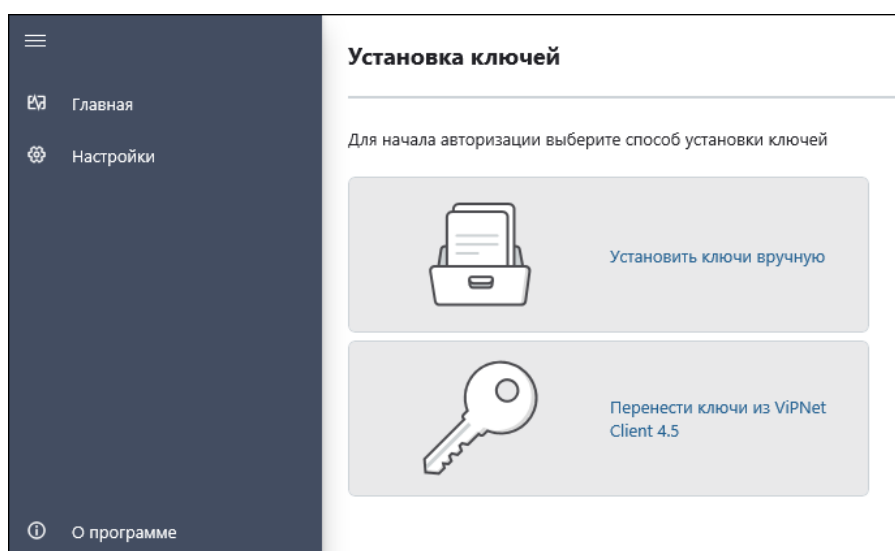


Рисунок 1. Установка ключей

- 2 Проверьте имя узла, для которого хотите перенести ключи, и нажмите **Далее**.
- 3 При необходимости введите пароль или PIN-код от внешнего устройства и нажмите **Далее**.
- 4 Подождите, пока ключи будут перенесены.
VPN-соединение включится автоматически.
- 5 В ViPNet Client 4.5 удалите компонент ViPNet Монитор, см. руководство пользователя ViPNet Client 4.5, раздел «Добавление, удаление и восстановление компонентов». Иначе может не работать VPN-соединение.
- 6 Дождитесь обновления настроек DNS или обратитесь к администратору за их обновлением.
- 7 [Настройте доступ в ViPNet Деловая почта](#).

Чтобы дополнительно защитить данные в корпоративной сети, установите на компьютер ViPNet EPP Агент. Он будет проверять безопасность компьютера и предотвращать сетевые угрозы.

Доступ в ViPNet Деловая почта

- 1 В ViPNet Client 5 for Windows выберите **Настройки**.
- 2 Нажмите **Предоставить доступ к ключам**.

Установка, обновление и удаление

Рекомендации по установке

- Обновляйте клиент тем же способом, которым устанавливали.
- Не устанавливайте другие VPN-клиенты. Совместная работа не проверялась и не гарантирована.



Внимание! Если клиент используют несколько пользователей ОС, могут быть проблемы с подключением к защищённой сети.

Установка и обновление с помощью файлов *.exe или *.msi

- 1 Запустите установочный файл *.exe или *.msi.
- 2 Чтобы использовать ViPNet Client 5, примите условия лицензионного соглашения и нажмите **Далее**.
- 3 По завершении установки нажмите **Выход**.

Удаление

- 1 В меню **Пуск** откройте **Параметры** > **Приложения** > **Приложения и возможности**.
- 2 Выберите ViPNet Client 5 for Windows и нажмите **Удалить**.

Переустановка

Вы можете переустановить ViPNet Client 5 for Windows с новыми ключами или использовать прежние ключи.

Переустановка с новыми ключами

- 1 [Удалите клиент](#).
- 2 [Заново установите клиент](#).
- 3 [Установите новые ключи](#).

Переустановка с прежними ключами

Для ViPNet Client 5 for Windows на 32- и 64-разрядных ОС:

- 1 В меню **Пуск** откройте **Параметры** > **Приложения** > **Приложения и возможности**.
- 2 Выберите ViPNet Client 5 for Windows и нажмите **Изменить**.
- 3 В мастере установки нажмите **Исправить**.

Способы аутентификации в ViPNet Client 5

Способ аутентификации	Описание	Требования
Пароль	однофакторная аутентификация, требуется ввести только пароль	• дистрибутив ключей *.dst или *.ds5; • пароль от дистрибутива ключей
Персональный ключ на внешнем устройстве	двухфакторная аутентификация, требуется подключить к компьютеру внешнее устройство с персональным ключом и ввести PIN-код. При отключении внешнего устройства VPN-соединение автоматически прерывается	• дистрибутив ключей *.dst; • пароль от дистрибутива ключей; • внешнее устройство; • PIN-код к внешнему устройству

Администратор задаёт способ аутентификации и может дополнительно [назначить пользователям многофакторную аутентификацию](#), для доступа к корпоративным ресурсам.

Пользователь может [сменить способ аутентификации](#).

Подготовка к работе с внешними устройствами



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами *.dst на устройствах с архитектурой процессора x86-64 и x86.

Если выбран способ аутентификации по персональному ключу на внешнем устройстве:

- 1 Получите у администратора:
 - дистрибутив ключей (файл *.dst);
 - пароль от дистрибутива ключей;
 - внешнее устройство и PIN-код к нему.

2 Установите драйверы для работы с внешним устройством:

- [Для устройств Rutoken.](#)
- [Для устройств JaCarta.](#)



Внимание! Для корректной работы с внешними устройствами используйте версии драйверов, которые поддерживает ваша ОС.

3 Перезагрузите компьютер.

4 Убедитесь, что ViPNet Client 5 определяет установленные библиотеки:

4.1 Проверьте, что ViPNet Client 5 включён.

4.2 Выполните:

```
vipnetclient debug --tokens
```

Если нужные библиотеки не обнаружены, отобразится сообщение об ошибке.

5 Подключите внешнее устройство к компьютеру и проверьте, определяют ли его ОС и ViPNet Client 5:

```
vipnetclient list --tokens
```



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

Чтобы задать PIN-код с русскими буквами на устройстве Рутокен, в настройках PIN-кода включите **Кодировать PIN-код в UTF-8**.

Установка ключей

Перед использованием клиента установите ключи. С помощью этих ключей шифруется трафик при соединениях с другими узлами защищённой сети. Без этого работа в защищённой сети невозможна.

Для установки потребуются:

- **Дистрибутив ключей** *.dst или *.ds5 и пароль.
- Внешнее устройство для аутентификации и PIN-код к нему, если выбрана аутентификация по внешнему устройству.

Вы можете получить их лично или другим доверенным способом у администратора. Чтобы получить информацию об альтернативном способе установки ключей, обратитесь в ИнфоТеКС.

Установка ключей при аутентификации по паролю

1 Выполните одно из действий:

- Дважды щёлкните дистрибутив ключей.
- В ViPNet Client 5 for Windows нажмите **Установить ключи вручную** и выберите дистрибутив ключей.

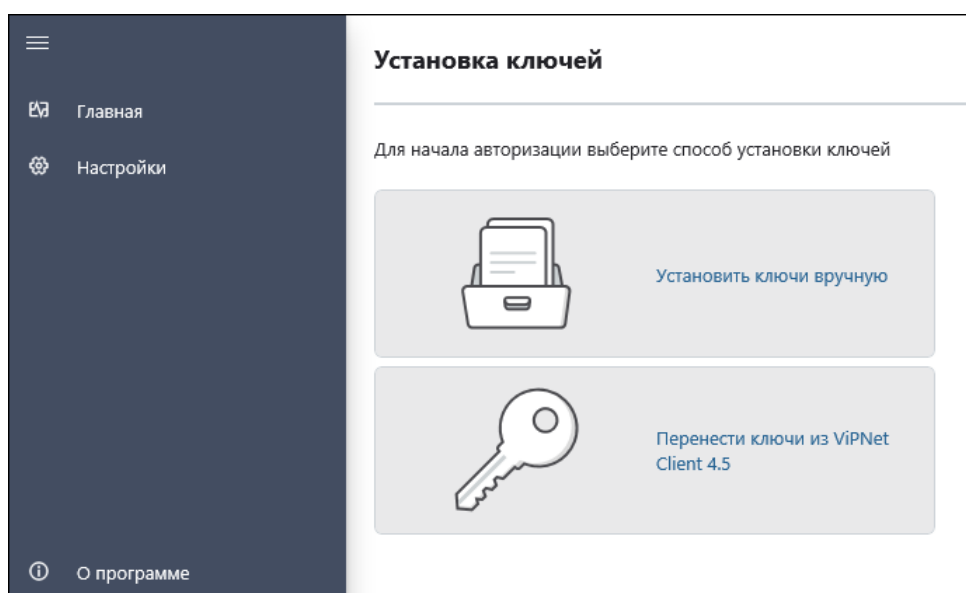
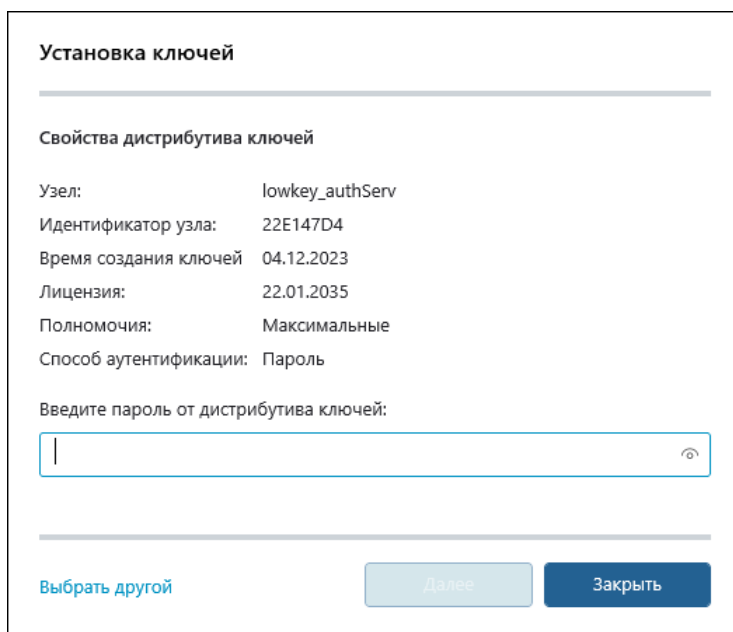


Рисунок 2. Установка ключей

2 Введите пароль и нажмите **Далее**.



Установка ключей

Свойства дистрибутива ключей

Узел: lowkey_authServ
Идентификатор узла: 22E147D4
Время создания ключей: 04.12.2023
Лицензия: 22.01.2035
Полномочия: Максимальные
Способ аутентификации: Пароль

Введите пароль от дистрибутива ключей:

[Выбрать другой](#) [Далее](#) [Заккрыть](#)

Рисунок 3. Ввод пароля к дистрибутиву ключей

3 Дождитесь установки ключей и нажмите **Заккрыть**.

После установки ключей будет **автоматически включено VPN-соединение**, и вы сможете подключаться к защищённым узлам вашей сети ViPNet.

Установка ключей при аутентификации по внешнему устройству

- 1 Подключите внешнее устройство к компьютеру.
- 2 Откройте ViPNet Client 5 for Windows.
- 3 Нажмите **Установить ключи вручную** и выберите дистрибутив ключей.
- 4 В окне **Установка ключей** нажмите **Далее**.
- 5 Если к компьютеру подключено несколько устройств, выберите устройство в списке и нажмите **Далее**.
- 6 Введите PIN-код от внешнего устройства и нажмите **Далее**.
- 7 Введите пароль и нажмите **Далее**.
- 8 Подождите, пока ключи будут установлены. Это может занять некоторое время.

После установки ключей будет **автоматически включено VPN-соединение**, и вы сможете подключаться к защищённым узлам вашей сети ViPNet.

Обновление ключей

Обновление ключей необходимо, если изменилась структура защищённой сети или свойства узлов, а также в случае смены мастер-ключей. Администратор создаёт новые ключи и централизованно отправляет их на узлы, где они принимаются и устанавливаются 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 сети передал вам новые ключи, установите их вручную:

- 1 Удалите текущие ключи.
- 2 Установите новые ключи.
- 3 Если вы используете аутентификацию по персональному ключу на внешнем устройстве и вам назначен минимальный уровень полномочий:
 - 3.1 Удалите старый персональный ключ с внешнего устройства средствами производителя.
 - 3.2 Получите от администратора новый персональный ключ или [перенесите персональный ключ на внешнее устройство самостоятельно](#).

Удаление ключей

При обновлении ключей вручную или при передаче компьютера другому пользователю:

- 1 Выберите  **Профиль** и нажмите **Удалить профиль**.

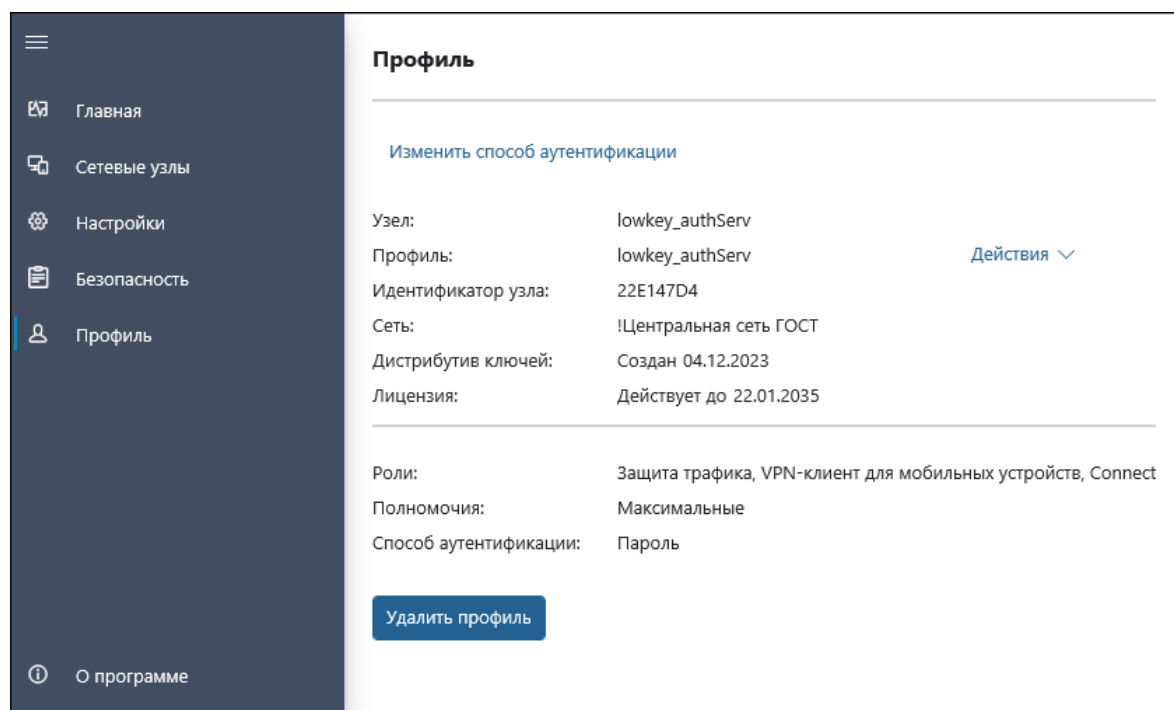


Рисунок 4. Удаление ключей

- 2 Если у вас несколько профилей, и вы удаляете текущий, подтвердите удаление.

Запуск и завершение работы

Включение VPN-соединения

Запуск клиента и подключение к защищённой сети выполняются автоматически после установки ключей и при каждой авторизации в ОС пользователя, установившего ключи.

Подключение к защищённой сети после авторизации пользователя в ОС не происходит, если:

- у пользователя минимальные полномочия;
- для аутентификации используется внешнее устройство, и оно не подключено.

Чтобы запустить клиент и включить VPN-соединение вручную:

- 1 Если для аутентификации используется внешнее устройство, подключите его к компьютеру.
- 2 Запустите клиент из меню **Пуск** или с помощью ярлыка ViPNet Client 5 .
- 3 Нажмите **Включить**.
- 4 Если вы обладаете минимальными полномочиями в клиенте, введите пароль или PIN-код от внешнего устройства и нажмите **Enter**.
- 5 После [проверки связи с координатором](#) установится защищённое VPN-соединение и вы сможете работать с корпоративными ресурсами.

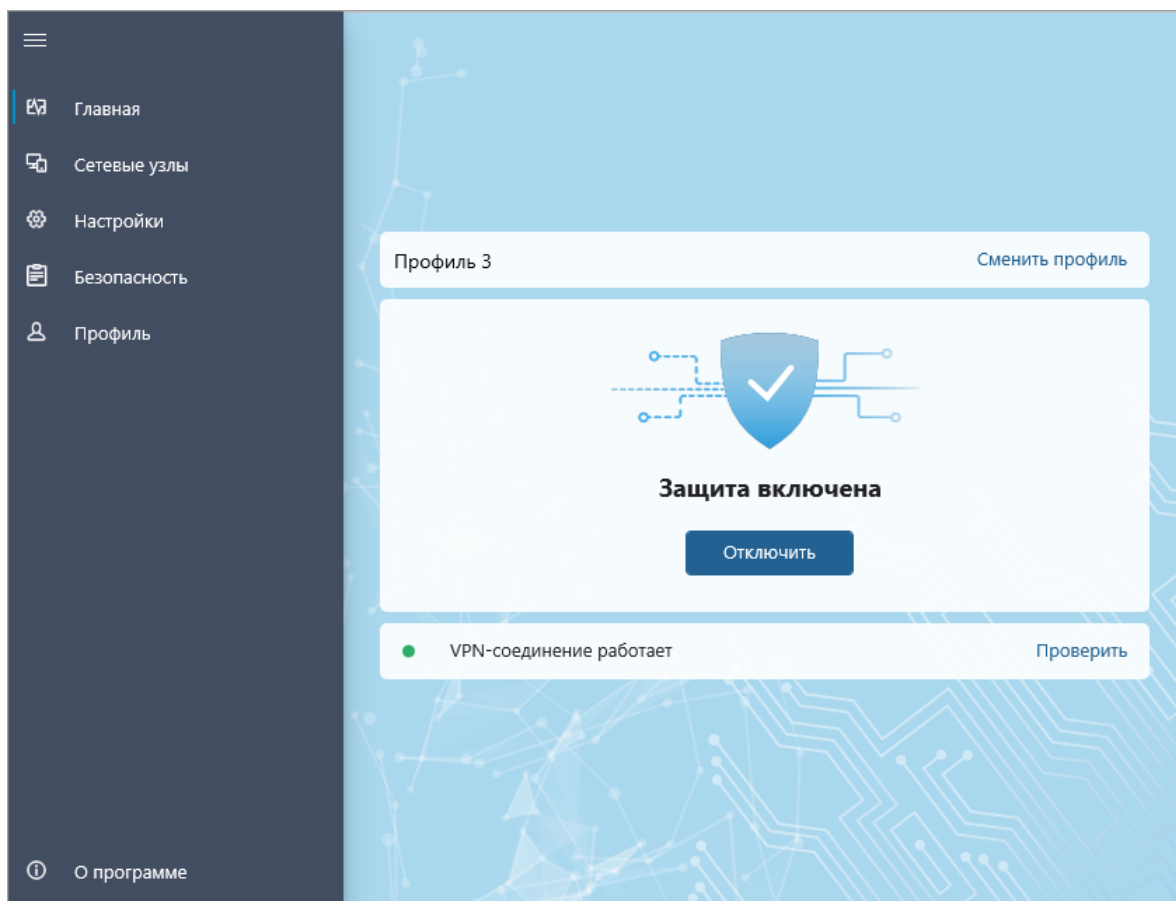


Рисунок 5. VPN-соединение включено

Выключение VPN-соединения

- Нажмите **Отключить**.
- Если вы используете для аутентификации внешнее устройство, отключите его от компьютера. VPN-соединение будет выключено автоматически.

2

Работа с ViPNet Client 5

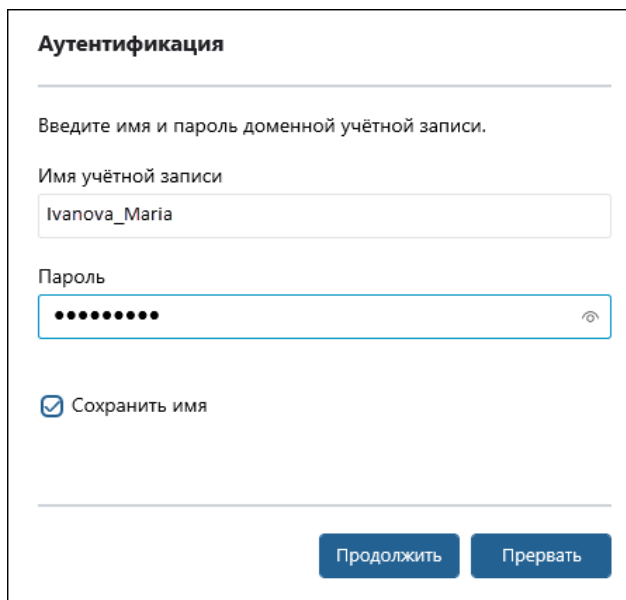
Многофакторная аутентификация	25
Несколько профилей на устройстве	30
Просмотр информации о своём узле	35
Просмотр списка узлов	36
Проверка связи с координатором	38
Обращение в службу поддержки	39

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

Ivanova_Maria

Пароль

••••••••

☒ Сохранить имя

Продолжить Прервать

Рисунок 6. 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 **Продолжить**.



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 выполняться аутентификация.

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

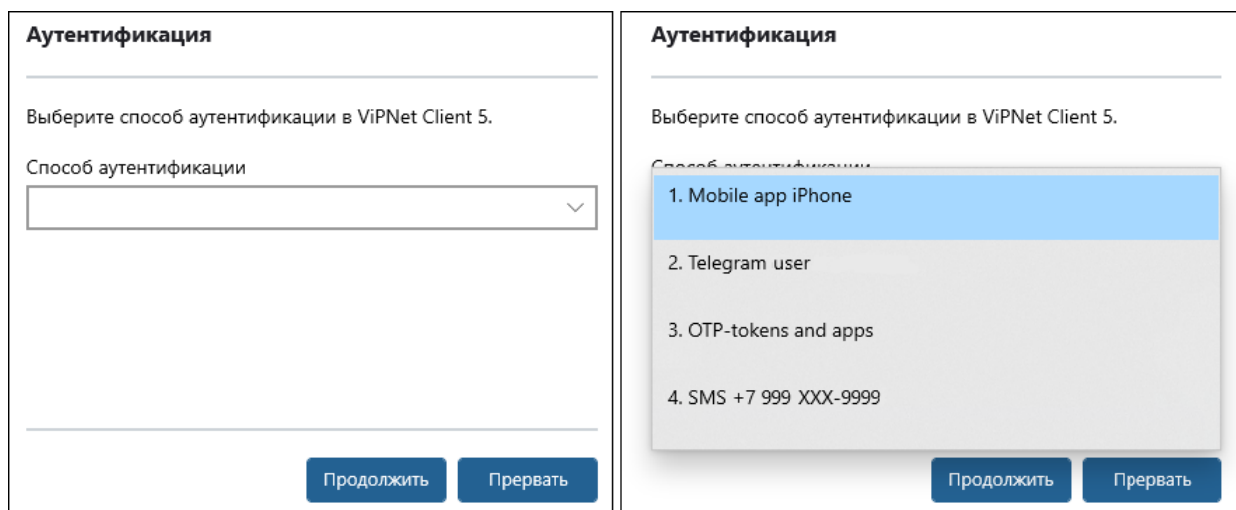


Рисунок 7. Выбор способа аутентификации

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



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 выполняться аутентификация.

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

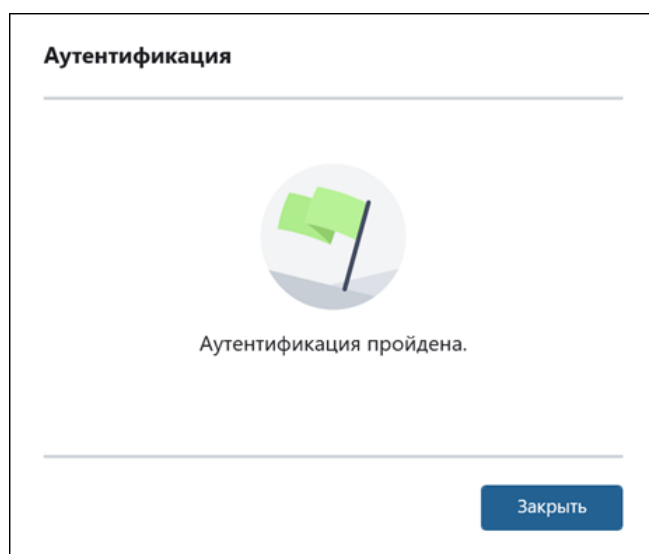


Рисунок 8. Аутентификация пройдена

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.

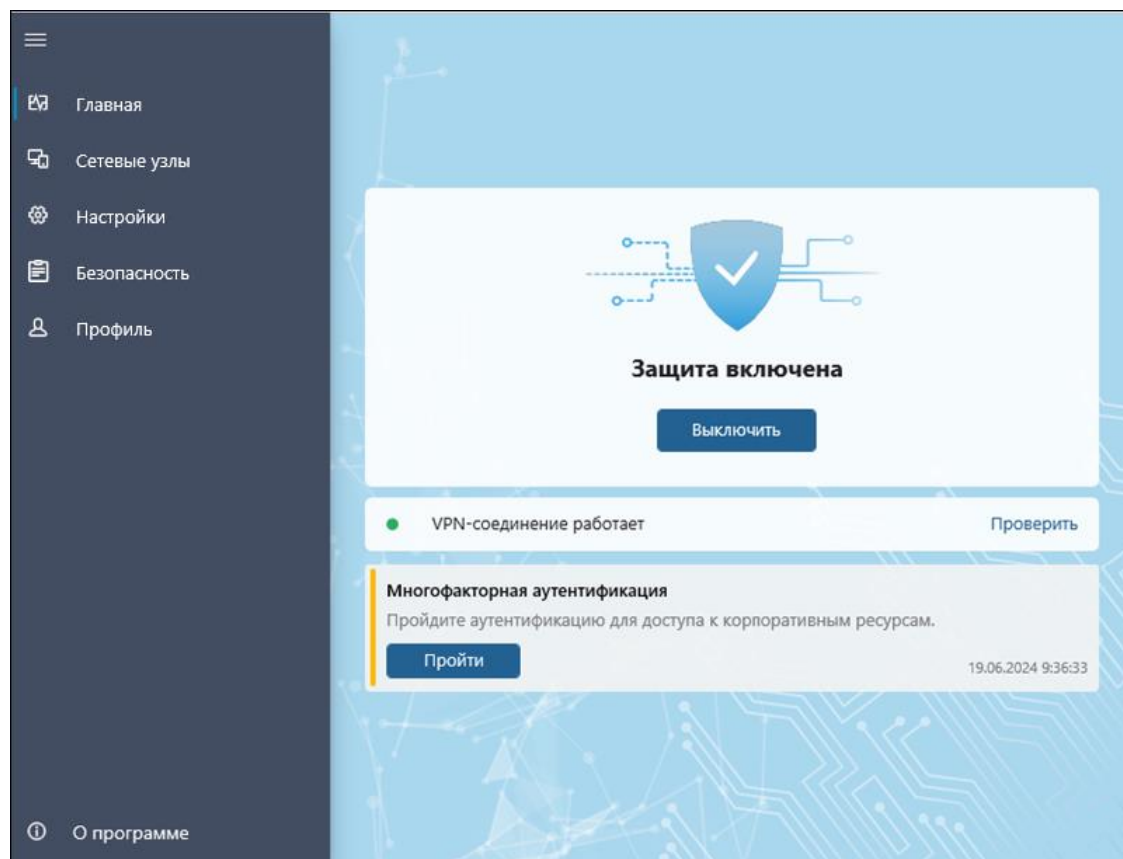


Рисунок 9. Аутентификация не пройдена

Способы многофакторной аутентификации

ViPNet Client 5 for Windows 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 Windows.

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 Windows.

SMS

Введите в ViPNet Client 5 for Windows код из SMS.

Многофакторная аутентификация до входа в Windows

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

- 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 Windows и нажмите **Продолжить**.



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 Windows будет выполняться аутентификация.

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

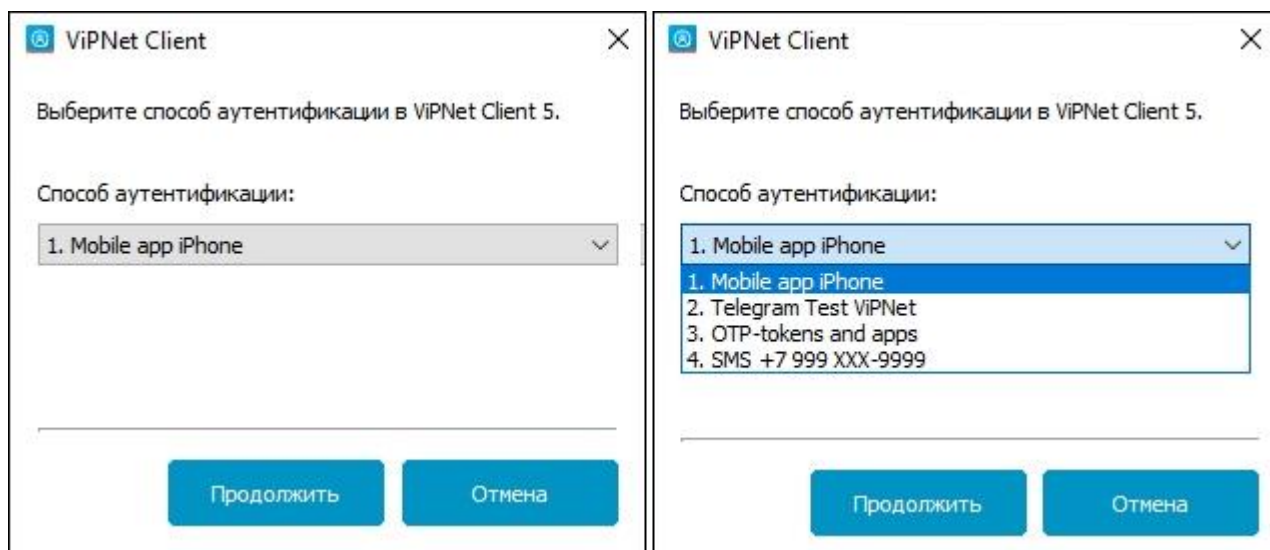


Рисунок 10. Выбор способа аутентификации

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



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 Windows будет выполняться 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 аутентификацию для доступа к корпоративным ресурсам** и пройдите аутентификацию заново.

Несколько профилей на устройстве

Вы можете установить до десяти дистрибутивов ключей в ViPNet Client 5. 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 десяти профилей.

- 1 Если вы хотите добавить профиль, в котором используется аутентификация с помощью внешнего устройства, подключите внешнее устройство к компьютеру.
- 2 В ViPNet Client 5 for Windows выберите  Профиль.

3 В строке **Профиль** нажмите **Действия** > **Добавить профиль**.

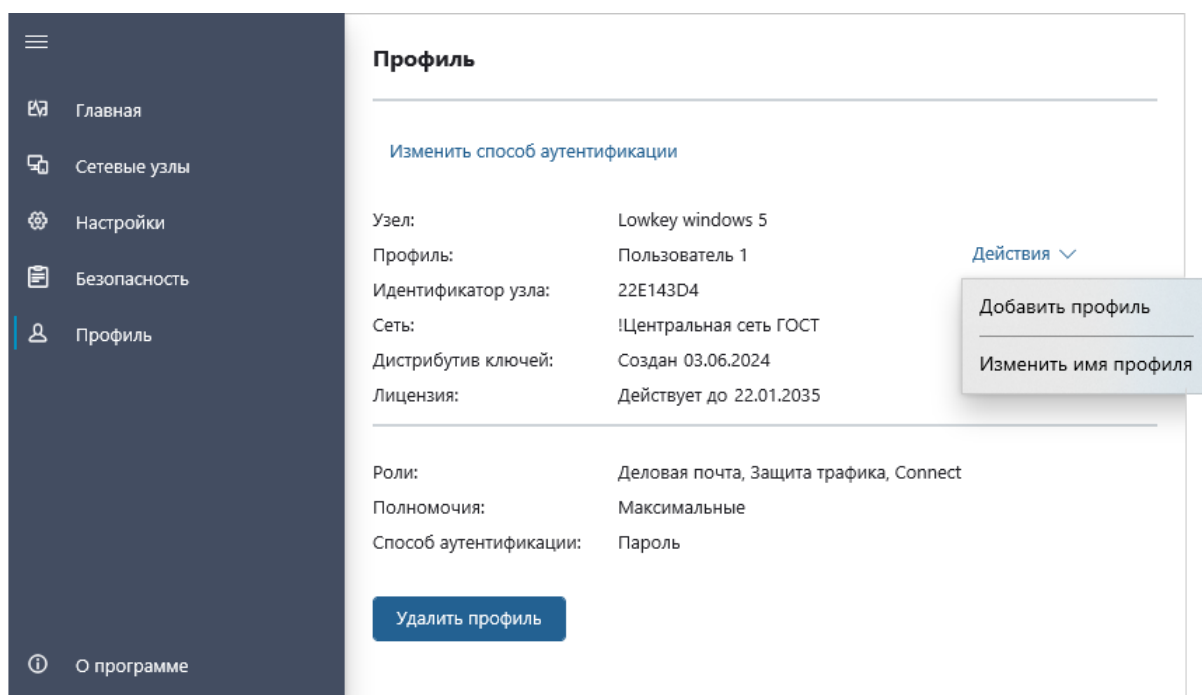


Рисунок 11. Добавление профиля

4 Если вы добавляете профиль первый раз, ознакомьтесь с особенностями использования нескольких профилей на устройстве и нажмите **Продолжить**.

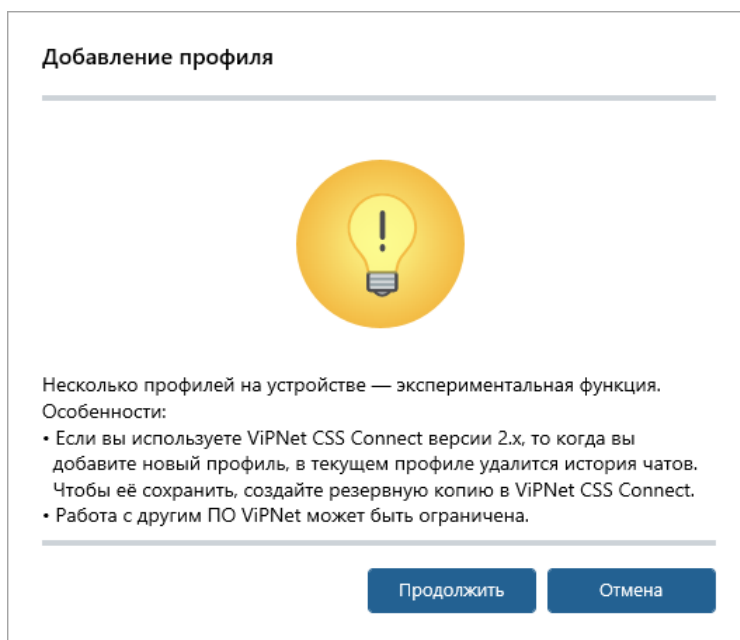


Рисунок 12. Ознакомление с особенностями многопрофильного режима работы

5 Нажмите **Установить ключи вручную** и выберите дистрибутив ключей.

Вы также можете [перенести ключи из ViPNet Client 4.5](#).

Рисунок 13. Выбор способа установки ключей

6 Введите пароль или PIN-код от внешнего устройств и нажмите **Далее**.

Вы автоматически перейдете 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**.

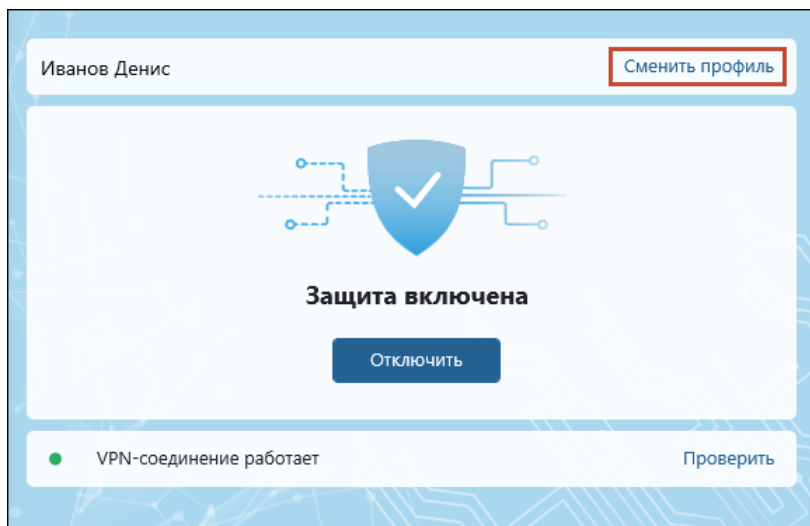


Рисунок 14. Смена профиля

- 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 Windows выберите  **Профиль**.
- 2 Нажмите **Удалить профиль**.
- 3 Выберите профиль и нажмите **Удалить**.

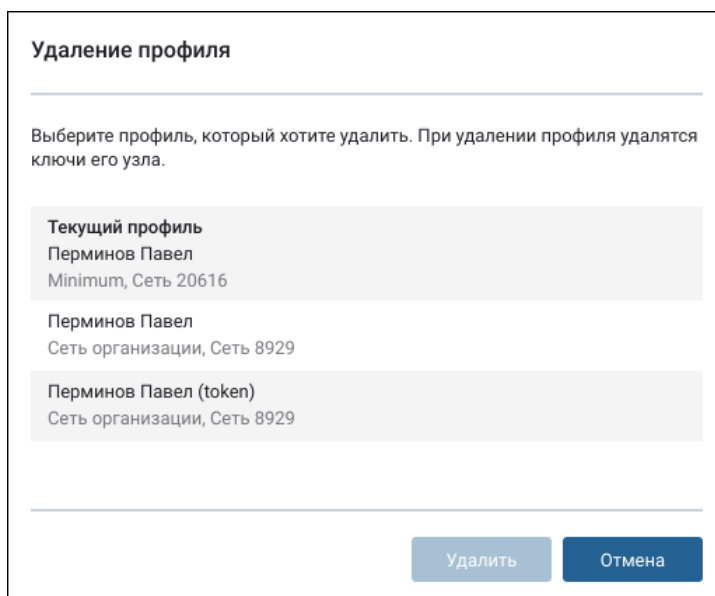


Рисунок 15. Выбор профиля для удаления

- 4 Если вы удаляете текущий профиль, подтвердите удаление.

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

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 Windows выберите  **Профиль**.
- 2 В строке **Профиль** нажмите **Действия** > **Изменить имя профиля**.
- 3 Задайте имя профиля. Длина нового имени профиля должна быть от 1 до 120 символов.
- 4 Нажмите **Сохранить**.

Просмотр информации о своём узле

Чтобы просмотреть:

- информацию о своём узле, выберите  **Профиль**;
- версию клиента и контакты ИнфоТеКС, выберите  **О программе**;
- лицензионное соглашение, выберите  **О программе** > **Лицензионное соглашение**.

Просмотр списка узлов

Выберите  **Сетевые узлы**. Отобразится список защищённых узлов, с которыми ваш компьютер может взаимодействовать.

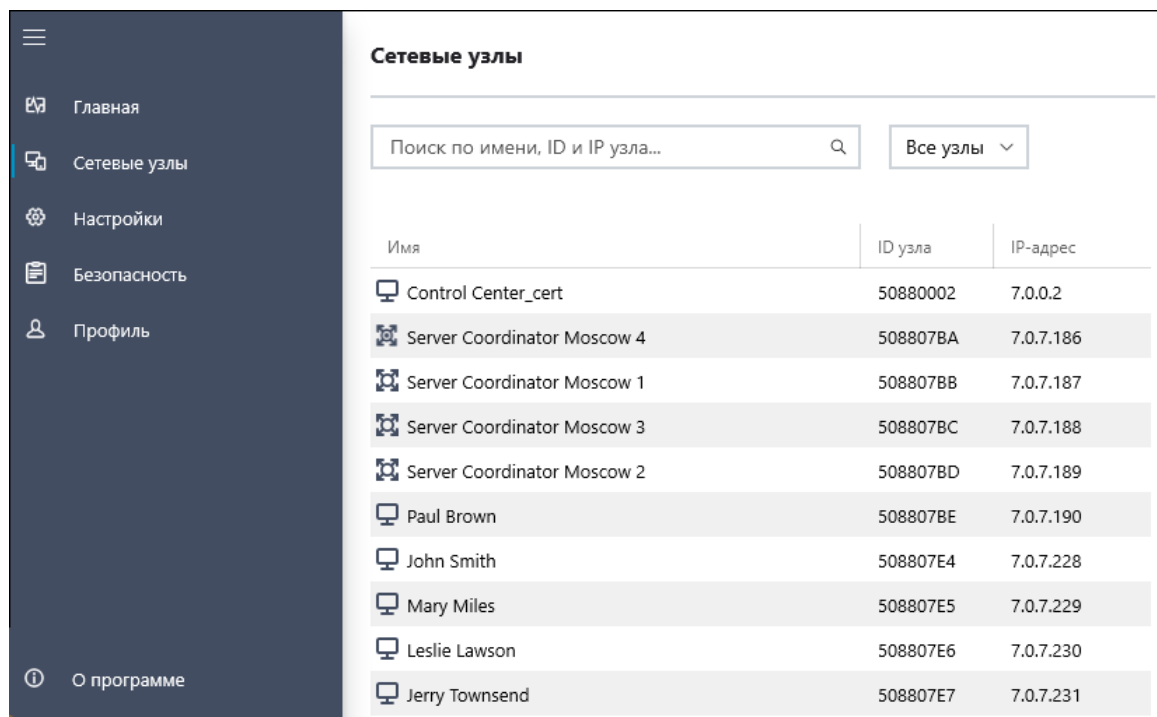


Рисунок 16. Просмотр списка защищённых узлов

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

Чтобы просмотреть подробную информацию об узле, выберите его в списке узлов. На правой панели отобразятся:

- идентификатор узла,
- IP-адрес,
- статус и время проверки соединения. Статус сбрасывается при закрытии ViPNet Client 5.

Для координатора дополнительно отобразятся IP-адреса туннелируемых узлов. Если включена виртуальная видимость туннелей, отобразятся реальные и виртуальные IP-адреса.

Если включено VPN-соединение, вы можете проверить соединение с узлом: нажмите **Проверить соединение**. После проверки для координатора дополнительно отобразятся:

- имя устройства,
- версия ОС,
- версия ПО.

Поиск узлов

Выберите  **Сетевые узлы**. В поле поиска начните вводить:

- имя узла,
- идентификатор,
- IP-адрес.

Чтобы найти координатор по его туннелю, начните вводить IP-адрес туннелируемого узла. При этом:

- Если включена виртуальная видимость туннелей, вы можете искать координатор и по реальным, и по виртуальным IP-адресам его туннелей.
- Вы можете вводить неполный IP-адрес, при поиске он преобразуется в стандартный вид из четырёх октетов.

Например, если вы введёте 11.0.13, то в результате поиска будет координатор, который туннелирует IP-адрес 11.0.0.13. Если вы введёте 11.282, то в результате поиска будет координатор, который туннелирует IP-адрес 11.0.5.2.

В результатах поиска отобразятся координаторы, которые туннелируют введённый IP-адрес. Этот адрес будет выделен в списке IP-адресов туннелей координатора.

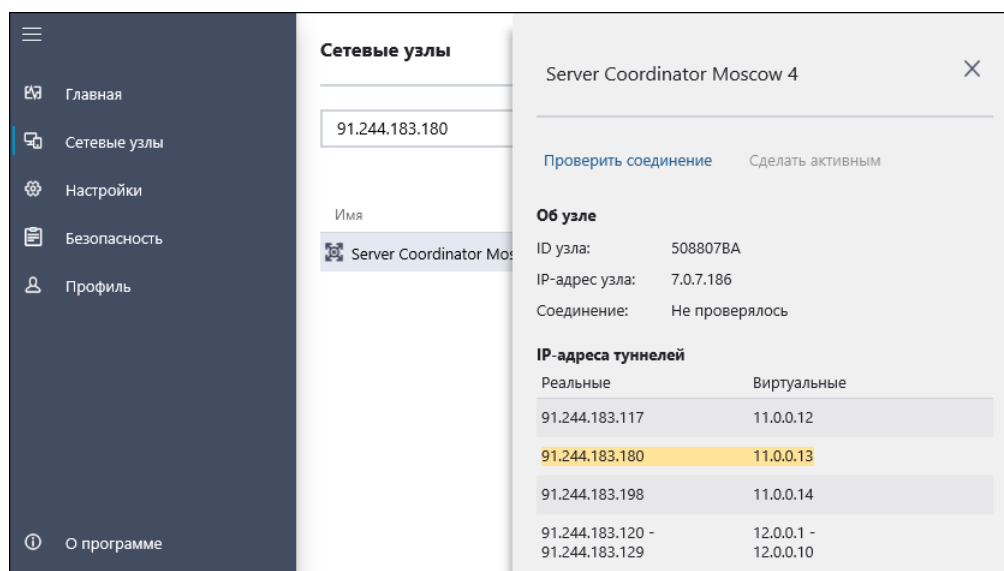


Рисунок 17. Поиск координатора по туннелю

Примечание. Обращайтесь к узлам защищённой сети 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.

Это самый надёжный способ обращения к узлам, потому что служебный адрес ViPNet не изменяется, а IP-адрес и доменное имя могут меняться.

Проверка связи с координатором

Когда клиент подключается к [защищённой сети](#), он автоматически проверяет связь с координатором — [сервером соединений](#). Этот координатор соединяет ваш компьютер с сетью ViPNet. Если он недоступен, то нет и подключения к сети.

Чтобы проверить связь с координатором вручную, на главном экране нажмите **Проверить**. Выполняйте проверку, если прервалась связь с какими-либо ресурсами защищённой сети. Если нет связи с координатором, повторите попытку через некоторое время или обратитесь к администратору.



Примечание. Если появится сообщение о разнице во времени между вашим компьютером и координатором (сервером соединений), установите часы на вашем компьютере, как рекомендуется в сообщении.

Обращение в службу поддержки

- 1 В разделе  **О программе** нажмите  **Создать отчет об ошибке**.
- 2 Опишите проблему и нажмите **Сохранить**.
Будет создан ZIP-архив с отчётом о работе и откроется папка с архивом.
- 3 Создайте электронное письмо и прикрепите к нему архив с отчётом. Опишите проблему и обстоятельства её возникновения.
- 4 Отправьте письмо на hotline@infotecs.ru.

3

Настройки ViPNet Client 5

Смена способа аутентификации в клиенте	41
Смена пароля	42
Смена сервера соединений	44
Контроль целостности и работоспособности	46
Настройка журнала событий	47
Применение настроек из конфигурационного файла	48

Смена способа аутентификации в клиенте



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами *.dst на устройствах с архитектурой процессора x86-64 и x86.

Чтобы сменить способ аутентификации по паролю на аутентификацию по персональному ключу на внешнем устройстве:

- 1 Включите VPN-соединение.
- 2 Подключите внешнее устройство к компьютеру.
- 3 Выберите **Профиль > Изменить способ аутентификации**.
- 4 Если подключено несколько внешних устройств, выберите нужное и нажмите **Далее**.

Смена способа аутентификации

Внешнее устройство
Подключите устройство и выберите его в списке

Обновить список устройств

PRO	4E46001727333932
Rutoken ECP	40f36678

Далее Отмена

Рисунок 18. Список внешних устройств

- 5 Введите PIN-код от внешнего устройства и нажмите **Далее**.
- 6 Подождите, пока персональный ключ будет записан на внешнее устройство. Если извлечь внешнее устройство до завершения операции, способ аутентификации не изменится.

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

Смена пароля

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, у клиентов с ключами *.ds5 появится напоминание о необходимости сменить пароль. Клиенты с ключами *.dst могут сменить пароль из раздела **Профиль**.

- 1 На главном экране нажмите **Сменить**.
- 2 Выберите **Сменить** и нажмите **Продолжить**.

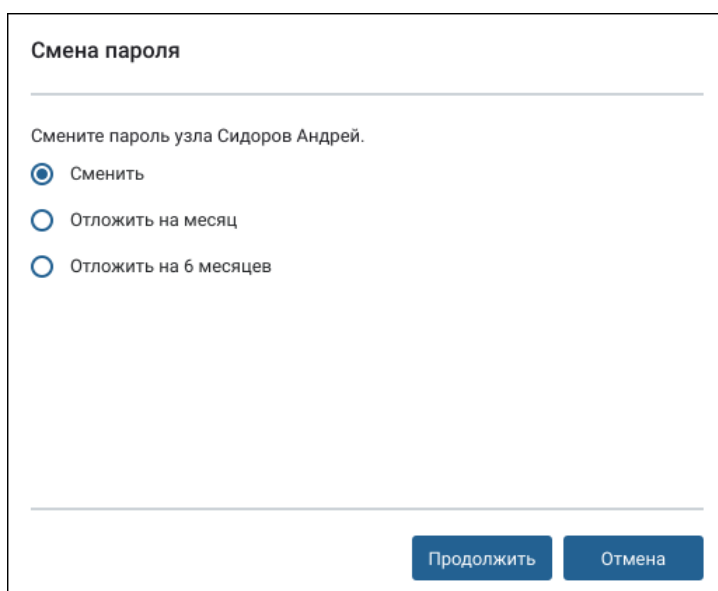


Рисунок 19. Смена пароля

- 3 Введите текущий пароль узла и нажмите **Продолжить**.
- 4 Задайте новый пароль, повторите пароль и нажмите **Сменить пароль**.

Длина пароля для клиентов с ключами *.dst должна быть от 6 до 31 символа. Для клиентов с ключами *.ds5: 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.

- 5 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, повторите пароль и нажмите **Сменить пароль**.

Длина пароля для клиентов с ключами *.dst должна быть от 6 до 31 символа. Для клиентов с ключами *.ds5: 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.

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

Просмотр срока действия пароля

Для клиентов с ключами *.ds5 срок действия пароля отображается во вкладке **Профиль** в строке **Пароль**. Для клиентов с ключами *.dst нельзя посмотреть срок действия пароля: в строке **Пароль** отображается дата создания дистрибутива ключей.

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**.

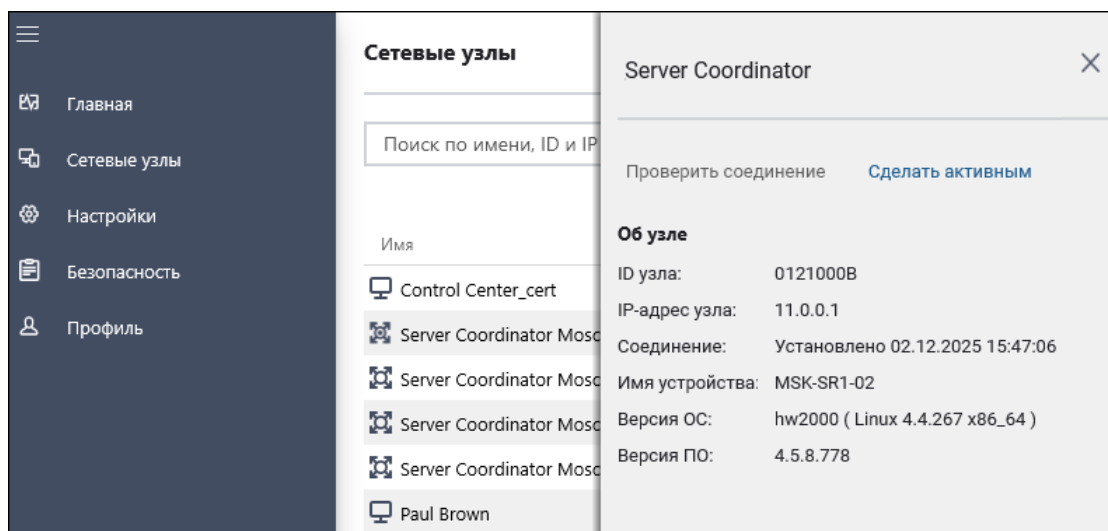


Рисунок 20. Смена сервера соединений

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 Windows, перейдите в  **Настройки**.

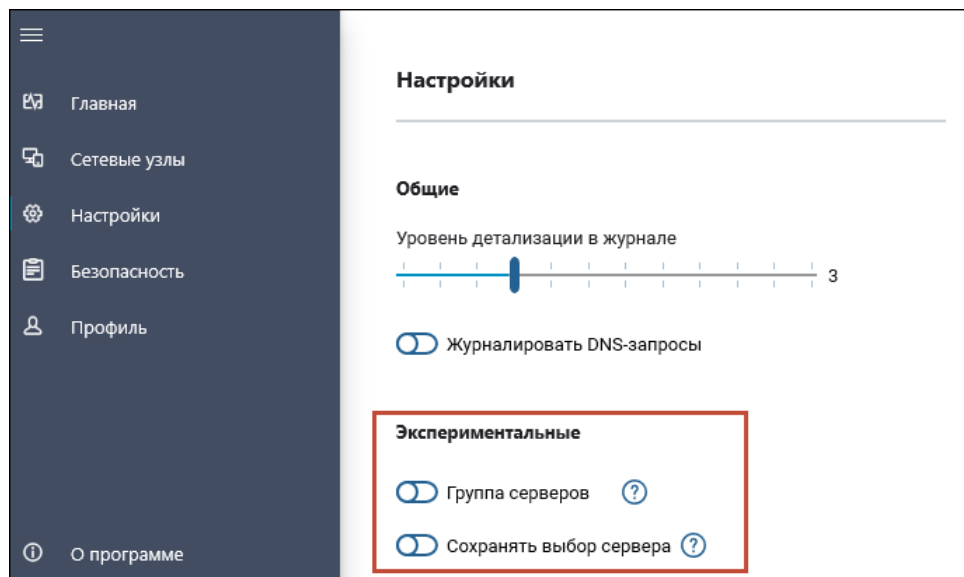


Рисунок 21. Экспериментальные настройки

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 Windows:

- 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.

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 проверки:

- 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.

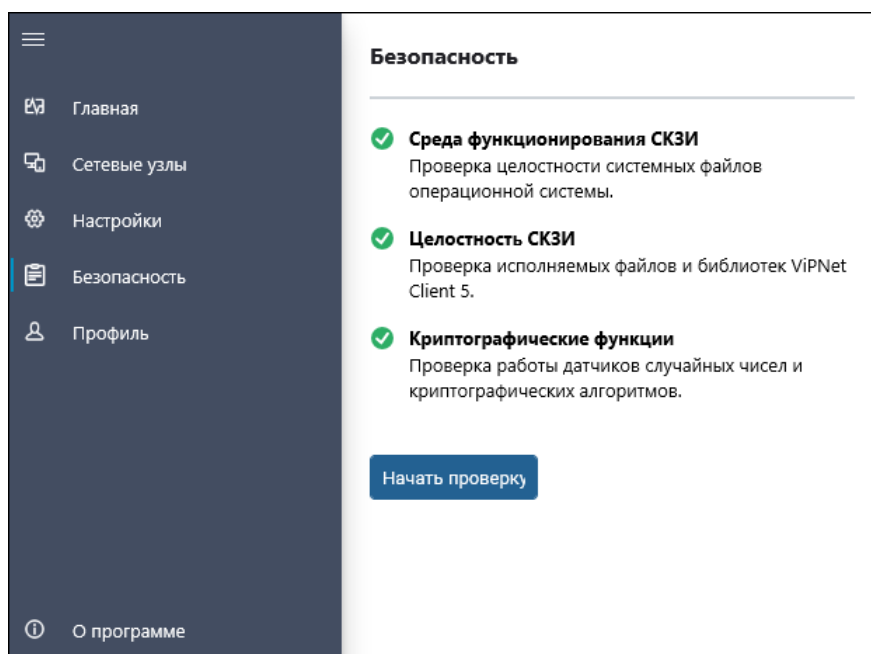


Рисунок 22. Просмотр результатов контроля целостности и работоспособности

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.

Настройка журнала событий



Внимание! Изменяйте описанные ниже настройки только по просьбе администратора или службы поддержки [ИнфоТеКС](#). При повышении уровня детализации работа в защищённой сети может быть замедлена.

Чтобы настроить уровень детализации событий о работе ViPNet Client 5 for Windows в журнале, в разделе  **Настройки** установите нужный **Уровень детализации в журнале**:

- 0 — только критичные ошибки.
- 1 — события уровня 0 и некритичные ошибки.
- 2 — события уровней 0, 1 и уведомления.
- 3 — события уровней 0, 1, 2 и информационные события.
- 4 — события уровней 0, 1, 2, 3 и события режима отладки.
- 5 и выше — события уровней 0, 1, 2, 3, 4 и детальные события работы программы.

По умолчанию используется уровень 3.

Чтобы настроить подробную детализацию DNS-запросов, включите **Журналировать DNS-запросы**.

Применение настроек из конфигурационного файла

Администратор может передать вам файл с настройками клиента *.vpnconfig, обновлением справочников или ключей — *.ctl, *.bin. Чтобы применить настройки:

- 1 Получите у администратора файл по электронной почте или другим способом.
- 2 [Выключите VPN-соединение.](#)
- 3 Дважды щёлкните файл и подтвердите установку в ViPNet Client 5.

Или в командной строке выполните:

```
vipnetclient debug --user-vpnconfig <имя_файла>.<расширение файла>
```

- 4 [Включите VPN-соединение.](#)

4

Работа в командной строке



Совет. Чтобы посмотреть список доступных команд для работы в командной строке, выполните:

```
vipnetclient --help
```

Переход с ViPNet Client 4.5	50
Установка ключей	51
Обновление ключей	53
Удаление ключей	54
Запуск и завершение работы	55
Несколько профилей на устройстве	57
Проверка VPN-соединения	60
Смена способа аутентификации	61
Смена сервера соединений	63
Просмотр информации о своём узле	64
Просмотр списка узлов	65
Смена пароля	66
Настройка параметров журнала событий	67
Обращение в службу поддержки	68

Переход с ViPNet Client 4.5

Предварительные действия

- 1 [Установите ViPNet Client 5 for Windows.](#)
- 2 Запустите ViPNet Client 4.5 от имени пользователя, которого хотите перевести в ViPNet Client 5 for Windows.
- 3 Если в ViPNet Client 4.5:
 - задан способ аутентификации по сертификату на устройстве, измените его на **Пароль** или **Персональный ключ на устройстве**.
См. руководство пользователя ViPNet Client 4.5, раздел «Изменение способа аутентификации пользователя».
 - в пароле от дистрибутива ключей есть русские буквы, измените пароль. Можно перенести только ключи, в пароле которых нет русских букв.
См. руководство пользователя ViPNet Client 4.5, раздел «Смена пароля пользователя».
- 4 Если в ViPNet Client 4.5 используется способ аутентификации **Персональный ключ на устройстве**, подключите устройство к компьютеру.

Перенос ключей

- 1 В командной строке Windows от имени администратора выполните:
`keydiskman.exe --copy --over`
- 2 При необходимости введите пароль или PIN-код от внешнего устройства.
- 3 Подождите, пока ключи будут перенесены.
После этого вы сможете включить VPN-соединение и подключаться к защищённым узлам вашей сети ViPNet.
- 4 В ViPNet Client 4.5 удалите компонент ViPNet Монитор, см. руководство пользователя ViPNet Client 4.5, раздел «Добавление, удаление и восстановление компонентов».
- 5 [Настройте доступ в ViPNet Деловая почта.](#)

Чтобы дополнительно защитить данные в корпоративной сети, установите на компьютер ViPNet EPP Агент. Он будет проверять безопасность компьютера и предотвращать сетевые угрозы.

Доступ в ViPNet Деловая почта

Чтобы продолжить пользоваться ViPNet Деловая почта, выполните:

```
keydiskman.exe --share --over
```

Установка ключей

Перед использованием клиента установите ключи ViPNet. С помощью этих ключей шифруется трафик при соединениях с другими узлами защищённой сети. Без этого работа в защищённой сети будет невозможна.

Для установки потребуются:

- **Дистрибутив ключей** *.dst или *.ds5 и пароль.
- Внешнее устройство для аутентификации и PIN-код к нему, если выбрана аутентификация по внешнему устройству.

Вы можете получить их лично или другим доверенным способом у администратора.

Установка ключей при аутентификации по паролю

1 В командной строке Windows выполните:

```
vipnetclient installkeys <путь_к_дистрибутиву_ключей> [--psw  
<пароль_от_дистрибутива_ключей>] [--no-start]
```

где:

- o psw — пароль от дистрибутива ключей (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 параметра psw и содержит спецсимволы, используйте экранирование спецсимволов. В командной строке Windows для экранирования используется символ ^. Напрямую можно экранировать следующие символы: ^, &, |, \, <, >. Знак % экранируется удвоением %, восклицательный знак ! экранируется ^^!. Например, чтобы получить пароль password^& введите password^^^&.

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

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

3 Подождите, пока ключи будут установлены.

Если появится сообщение об ошибке, обратитесь к администратору сети ViPNet.

Если вы не указывали параметр no-start, после установки ключей VPN-соединение будет включено автоматически.

Установка ключей при аутентификации по внешнему устройству

1 В командной строке Windows выполните:

```
vipnetclient installkeys <путь_к_дистрибутиву_ключей> [--pin <PIN-код>] [--psw  
<пароль_от_дистрибутива_ключей>] [--token-select <часть_названия>] [--no-start]
```

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 `psw` — пароль от дистрибутива ключей (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. Пользователям с минимальными полномочиями вводить пароль не требуется.



Примечание. Если пароль указывается с помощью параметра `psw` и содержит спецсимволы, используйте экранирование спецсимволов. В командной строке Windows для экранирования используется символ `^`. Напрямую можно экранировать следующие символы: `^`, `&`, `|`, `\`, `<`, `>`. Знак `%` экранируется удвоением `%%`, восклицательный знак `!` экранируется `^^!`. Например, чтобы получить пароль `password^&` введите `password^^^&`.

- 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 не был указан параметр `token-select` или найдено несколько внешних устройств, введите номер нужного внешнего устройства и нажмите **Enter**.
 - 3 Если PIN-код не был указан в команде, введите PIN-код от внешнего устройства и нажмите **Enter**.
 - 4 Если вы обладаете не минимальными полномочиями и пароль не указан в команде, введите его и нажмите **Enter**.
 - 5 Подождите, пока ключи будут установлены. Выполнение команды может занять некоторое время.

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

Если вы не указывали параметр `no-start`, после установки ключей VPN-соединение будет включено автоматически.

Обновление ключей

Обновление ключей необходимо, если изменилась структура защищённой сети или свойства узлов, а также в случае смены мастер-ключей. Администратор создаёт новые ключи и централизованно отправляет их на узлы, где они принимаются и устанавливаются автоматически, без участия пользователя.

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

- 1 Удалите текущие ключи.
- 2 Установите новые ключи.
- 3 Если вы используете аутентификацию по персональному ключу на внешнем устройстве и вам назначен минимальный уровень полномочий:
 - 3.1 Удалите старый персональный ключ с внешнего устройства средствами производителя.
 - 3.2 Получите от администратора внешнее устройство с новым персональным ключом.

Удаление ключей

При обновлении ключей вручную или при передаче компьютера другому пользователю:

- 1 В командной строке Windows выполните:

```
vipnetclient deletekeys [--skip-accept]
```

где:

`skip-accept` — автоматическое подтверждение удаления ключей.

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

Запуск и завершение работы

Запуск клиента и подключение к защищённой сети выполняются автоматически после установки ключей и при каждой авторизации в ОС пользователя, установившего ключи.

Подключение к защищённой сети после авторизации пользователя в ОС не происходит:

- у пользователя минимальные полномочия;
- для аутентификации используется внешнее устройство, и оно не подключено.

Чтобы запустить клиент и включить VPN-соединение вручную:

1 Если для аутентификации используется внешнее устройство:

1.1 Подключите его к компьютеру.

1.2 В командной строке Windows выполните:

```
vipnetclient start {[--pin <PIN-код>] | [--psw <пароль_от_дистрибутива_ключей>]}  
[--token-select <часть_названия>]
```

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 от дистрибутива ключей (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 параметра `psw` и содержит спецсимволы, используйте экранирование спецсимволов. В командной строке Windows для экранирования используется символ `^`. Напрямую можно экранировать следующие символы: `^`, `&`, `|`, `\`, `<`, `>`. Знак `%` экранируется удвоением `%%`, восклицательный знак `!` экранируется `^^!`. Например, чтобы получить пароль `password^&` введите `password^^^&.`

- `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.

1.3 Если не был указан параметр `token-select` либо найдено несколько внешних устройств, введите номер нужного и нажмите **Enter**.

2 Если вы обладаете минимальными полномочиями, введите пароль пользователя ViPNet или PIN-код от внешнего устройства и нажмите **Enter**.

3 Подождите, пока VPN-соединение будет включено.

Выключение VPN-соединения

Чтобы остановить клиент и выключить VPN-соединение:

```
vipnetclient stop
```

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

Несколько профилей на устройстве

Вы можете установить до десяти дистрибутивов ключей в ViPNet Client 5. 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.

1 В командной строке выполните:

```
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.

- o `psw` — пароль от дистрибутива ключей (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 параметра `psw` и содержит спецсимволы, используйте экранирование спецсимволов. В командной строке Windows для экранирования используется символ `^`. Напрямую можно экранировать следующие символы: `^`, `&`, `|`, `\`, `<`, `>`. Знак `%` экранируется удвоением `%%`, восклицательный знак `!` экранируется `^^!`. Например, чтобы получить пароль `password^&` введите `password^^^&`.

- 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 внешнее устройство не было выбрано в команде, выберите его из списка и нажмите **Enter**.
 - 4 Если пароль или PIN-код 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:

```
vipnetclient profile switch <идентификатор узла>
```

После смены профиля **включите VPN-соединение вручную**.

Удаление профиля

При удалении профиля удаляются ключи его узла.

Чтобы удалить текущий профиль:

```
vipnetclient deletekeys [--skip-accept]
```

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

Чтобы удалить другой профиль:

```
vipnetclient deletekeys --profile <идентификатор узла>
```

Если в команде не задан идентификатор узла, откроется список профилей. Введите номер профиля, который хотите удалить, и нажмите **Enter**.

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:

```
vipnetclient profile set --alias <новое имя профиля>
```

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

Чтобы вернуть имя профиля по умолчанию:

```
vipnetclient profile set --no-alias
```

Просмотр списка профилей

Выполните:

```
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`.

Проверка VPN-соединения

Когда клиент подключается к [защищённой сети](#), он автоматически проверяет связь с координатором — [сервером соединений](#). Этот координатор соединяет ваш компьютер с защищённой сетью, если он недоступен, то подключение к сети отсутствует.

Если прервалась связь с ресурсами защищённой сети, проверьте связь с координатором вручную:

```
vipnetclient debug --ping
```

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

Если появится сообщение о разнице во времени между вашим компьютером и координатором (сервером соединений), установите часы на вашем компьютере, как рекомендуется в сообщении.



Примечание. Также вы можете проверить связь с другими узлами:

```
vipnetclient debug --ping <идентификатор узла>
```

Смена способа аутентификации



Внимание! Аутентификация с помощью персонального ключа на внешнем устройстве работает только для клиентов с ключами *.dst на устройствах с архитектурой процессора x86-64 и x86.

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 23. 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.

Смена сервера соединений

В ViPNet Client 5 for Windows вы можете сменить координатор, используемый в качестве сервера соединений. Например, если текущий сервер соединений недоступен.



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

Чтобы сменить сервер соединений:

```
vipnetclient debug --active-server <идентификатор_координатора> [--insist]
```

где `--insist` — режим выбора сервера соединений при получении справочников и ключей из управляющего ПО для клиентов с ключами `*.dst`:

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

Экспериментальные 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, если ваш активный координатор недоступен, выполните:

```
vipnetclient debug --connect-server-group
```

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

- Чтобы выключить автоматический выбор сервера соединений, выполните:

```
vipnetclient debug --no-connect-server-group
```

Просмотр информации о своём узле

- Посмотреть информацию о своём узле и версии ViPNet Client 5:

```
vipnetclient info
```

Если появится сообщение о разнице во времени между вашим компьютером и координатором (сервером соединений), установите часы на вашем компьютере, как рекомендуется в сообщении.

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

Если пользовательский защищённый трафик заблокирован, отобразится строка `User traffic status Blocked`. Для разблокировки обратитесь к администратору.

- Посмотреть информацию только о версии ViPNet Client 5:

```
vipnetclient --version
```

- Посмотреть список пользователей ViPNet, с которыми связан ваш узел:

```
vipnetclient list --users
```

- Посмотреть список подключённых или настроенных устройств входа в систему:

```
vipnetclient list --tokens
```

Просмотр списка узлов

Чтобы просмотреть список защищённых узлов:

```
vipnetclient list --nodes
```

Отобразится список защищённых узлов, с которыми ваш компьютер может взаимодействовать в сети ViPNet. В этом списке типы узлов отмечены как `client` (клиент, компьютер пользователя) и `server` (координатор). Координатор, выполняющий функции сервера соединений для вашего узла, отмечен в списке символом `*`.

Поиск узлов

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

```
vipnetclient iplirdiag -s ipsettings --node-info <идентификатор узла>
```

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.

Чтобы найти координатор по его туннелю:

```
vipnetclient iplirdiag -s ipsettings --find-tunnel <реальный или виртуальный IP-адрес туннеля>
```

При этом:

- Если включена виртуальная видимость туннелей, вы можете искать координатор и по реальным, и по виртуальным IP-адресам его туннелей.
- Вы можете вводить неполный IP-адрес, при поиске он преобразуется в стандартный вид из четырёх октетов. Например, если вы введёте `10.0.3`, то в результате поиска будет координатор, который туннелирует IP-адрес `10.0.0.3`.

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

Смена пароля

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, у клиентов с ключами *.ds5 появится напоминание о необходимости сменить пароль.

1 Выполните:

```
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.

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 для клиентов с ключами *.dst должна быть от 6 до 31 символа. Для клиентов с ключами *.ds5: 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 клиентов с ключами *.ds5

Выполните: `vipnetclient info`

Срок действия пароля отобразится в строке `User password expires on`. Если требуется сменить пароль, в строке `Logon mode` отобразится статус `change required`.

Настройка параметров журнала событий



Внимание! Изменяйте описанные ниже настройки только по просьбе администратора или службы поддержки [ИнфоТеКС](#). При повышении уровня детализации работа в защищённой сети может быть замедлена.

Чтобы настроить уровень детализации событий ViPNet Client 5 for Windows, записываемых в журнал:

```
vipnetclient debug --loglevel <уровень детализации>
```

Возможные значения уровня детализации:

- 0 — только критичные ошибки.
- 1 — события уровня 0 и некритичные ошибки.
- 2 — события уровней 0, 1 и уведомления.
- 3 — события уровней 0, 1, 2 и информационные события.
- 4 — события уровней 0, 1, 2, 3 и события режима отладки.
- 5 и выше — события уровней 0, 1, 2, 3, 4 и детальные события работы программы.

По умолчанию используется уровень 3.

Чтобы настроить подробную детализацию DNS-запросов:

```
vipnetclient ipilirdiag -s dnsproxy --query-logging arg 1
```

Обращение в службу поддержки

В случае возникновения ошибок в работе клиента, создайте и передайте отчёт о работе программы в ИнфоТеКС:

- 1 Создайте отчёт о работе:

```
vipnetclient report [--output <путь к папке для сохранения отчёта>\<имя файла отчёта>]
```

где `output` — параметр для указания имени отчёта и папки, в которую будет сохранен файл отчёта. Если в команде вы не укажете папку и имя отчёта, то отчёт будет сохранён в папке, в которой была выполнена команда `vipnetclient report`, с использованием шаблона имени по умолчанию — `report_windows_<версия клиента>_<дата>_<время>.zip`.

Будет создан ZIP-архив с отчётом о работе клиента.

- 2 Создайте электронное письмо, опишите проблему и обстоятельства её возникновения, прикрепите к письму архив с отчётом.
- 3 Отправьте письмо на hotline@infotecs.ru.



Возможные неполадки и способы их устранения

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.](#)

Если нарушена целостность справочников:

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

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

- 1 Удалите ViPNet Client 5.
- 2 Установите ViPNet Client 5.
- 3 [Установите новые ключи.](#)

Пропадает удалённое подключение к узлу

Удалённое подключение к компьютеру с ViPNet Client 5 for Windows может пропадать при получении обновлений справочников и ключей из управляющего ПО. Повторите подключение вручную.

Изменился сервер соединений

При обновлении или в случае внутренних ошибок клиент может удалять информацию о взаимодействии узлов из внутренних конфигурационных файлов. Вместе с этим может сброситься выбор сервера соединений: активным снова станет координатор, заданный в управляющем ПО.

Способ устранения

Для клиентов с ключами *.dst **включите настройку Сохранять выбор сервера** или выполните:

```
vipnetclient debug --active-server <идентификатор координатора> --insist
```

Тогда после обновления клиента или сброса внутренних конфигурационных файлов сервером соединений останется координатор, выбранный вручную.



Примечание. Чтобы проверить, какой координатор используется в качестве сервера соединений, включите VPN-соединение и выполните:

```
vipnetclient info
```

Сервер соединений отобразится в строке **Active coordinator**.

В

История версий

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

Что нового в версии 5.4

- **Поддержка новых версий Windows**
 - Windows 11 LTSC 24H2,
 - Windows Server 2025.
- **Уведомления о новых письмах в ViPNet Деловая почта**

Больше не нужно отдельно настраивать уведомления о новых письмах. [Предоставьте доступ к ключам](#), и уведомления будут приходить, даже если ViPNet Деловая почта закрыта.

Что нового в версии 5.2

- **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.

- **Отправка обновлений из ViPNet ЦУС с помощью ViPNet Client 5**

Раньше для работы ViPNet ЦУС нужно было устанавливать ViPNet Client for Windows 4.5. Этот клиент использовался, чтобы отправлять обновления справочников и ключей. Теперь вы можете использовать ViPNet Client 5. Для этого на компьютер с ViPNet ЦУС версии 4.6.11 и выше установите ViPNet Client 5 без графического интерфейса с помощью файла *.msi.

- **Рассылка политик на узлы из ViPNet Policy Manager с помощью ViPNet Client 5**

Раньше для работы ViPNet Policy Manager нужно было устанавливать ViPNet Client for Windows 4.5. Этот клиент использовался, чтобы рассылать результирующие политики на узлы. Теперь вы можете использовать ViPNet Client 5. Для этого на компьютере с ViPNet Policy Manager версии 4.5.5 и выше установите ViPNet Client 5.

- **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.

- **Срок действия пароля**

Клиентам с ключами *.ds5 будет приходить напоминание о смене пароля раз в полгода, после установки ключей и после каждого обновления мастер-ключа ключей защиты обновлений. Чтобы обезопасить свои данные, нужно регулярно [менять пароль](#).

- **Журнал критически важных событий**

Чтобы повысить уровень безопасности сети, в ViPNet Client 5 ведётся журнал критически важных событий программы. В него записывается информация о действиях с ключами и межсетевым экраном, результатах проверки целостности и работоспособности, аутентификации. Журнал доступен только администратору узла.

- **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
CMC	SMS <номер телефона, на который придёт код>

- **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.

Что нового в версии 5.0

- **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.

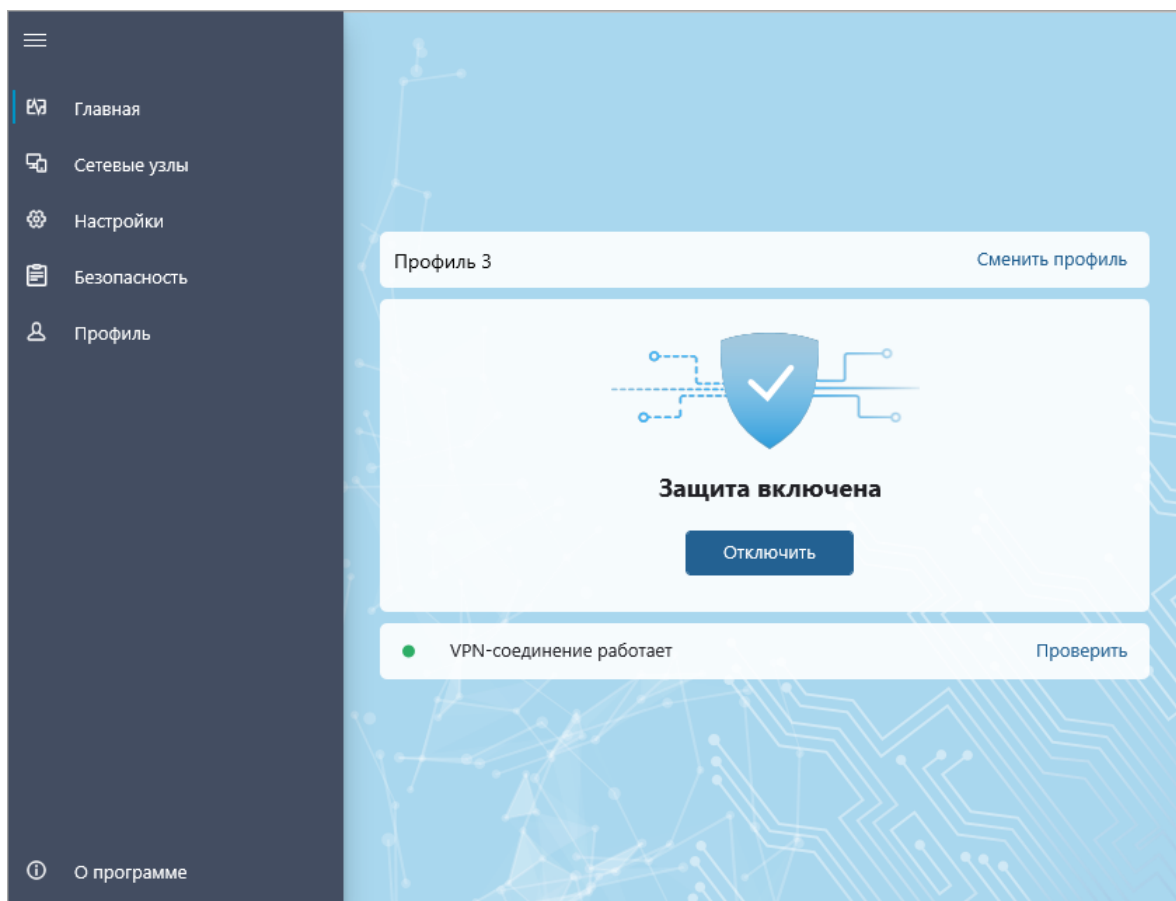


Рисунок 24. VPN-соединение включено

- **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 в защищённой сети, ViPNet Client 5 for Windows подключается к серверу соединений. Раньше, если активный сервер соединений становился недоступным, нужно было вручную назначать активным другой.

Вы можете [включить автоматический выбор активного сервера соединений](#) из группы серверов. Если ваш сервер соединений станет недоступен, ViPNet Client 5 for Windows переключится на другой.

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

- **Сохранение выбора сервера соединений**

В ViPNet Client 5 for Windows вы можете управлять режимом выбора сервера соединений. Чтобы при получении новых справочников и ключей из управляющего ПО сервером соединений оставался координатор, заданный вручную в ViPNet Client 5 for Windows, включите сохранение выбора сервера. Если настройка выключена, то при получении новых справочников и ключей сервером соединений будет выбран координатор, заданный в управляющем ПО.

- **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 устанавливаются автоматически.

- **Блокировка трафика открытой сети**

Вы можете заблокировать весь открытый IP-трафик устройства, когда включено VPN-соединение. Открытый IP-трафик, необходимый для работы Windows 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.

- **Переход с ViPNet Client 4.5**

Чтобы перейти с ViPNet Client 4.5 на ViPNet Client 5, не надо получать и устанавливать новые ключи. Просто [перенесите свои ключи](#): все связи узла сохраняются и корпоративные ресурсы будут доступны. В версии ViPNet Client 5 вы также сможете [продолжить работать с ViPNet Деловая почта](#).

- **Две версии программы: ViPNet Client 5 и ViPNet Client 5 Store Edition**

В ViPNet Client 5 Store Edition и из файла *.exe разные функции. В полной версии ViPNet Client 5 доступны функции:

- аутентификация с помощью персонального ключа на внешнем устройстве,
- запуск ViPNet Client 5 до авторизации пользователя в ОС,
- [работа в командной строке](#),
- обновление ViPNet CSS Connect через ViPNet Client 5,

- централизованное управление настройкой `authbeforeOsLogon` (отображение окна аутентификации ViPNet Client 5 до аутентификации пользователя в ОС).
- **Обновление ViPNet CSS Connect через ViPNet Client 5**

В сети под управлением ViPNet Prime у ViPNet Client 5 и ViPNet CSS Connect общий механизм обновления. Если администратор отправил вам обновление ViPNet CSS Connect, оно установится автоматически.
- **Работа в командной строке**

Вы можете работать с ViPNet Client 5 из командной строки Windows (см. [Работа в командной строке](#)). Это удобно при создании скриптов для автоматизации работы.
- **ViPNet Client 5 for Windows SDK**

Реализован набор средств разработки SDK, с помощью которого разработчики могут организовать работу с функциями ViPNet Client 5 из других программ.
- **Поддержка ViPNet Prime NVS**



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 Windows.

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 Windows 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 остаётся в пределах объёма, необходимого для достижения этих целей, и не производится в иных целях.

- **Принцип минимизации данных.**

Данные, собранные и сохранённые 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 отчётности, 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 подотчётности ответственных контролёров, оценки рисков и выявления нарушений безопасности данных.

Какие персональные данные обрабатывает ViPNet Client 5 for Windows



Примечание. ViPNet Client 5 for Windows 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 Windows

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

Данные устройства пользователя ViPNet Client 5 for Windows

Для выявления проблем в работе ViPNet Client 5 for Windows существует функция формирования отчёта, которая позволяет сформировать по инициативе пользователя ViPNet Client 5 for Windows диагностическую информацию и передать её в [службу поддержки](#). В частности, отчёт 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 развёртывания и работы ViPNet Client 5 for Windows 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 отчёта пользователь может сформировать средствами ViPNet Client 5 for Windows и передать в службу поддержки производителя.

Данные об активности устройства пользователя ViPNet-сети

ViPNet Client 5 for Windows 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 Windows 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 Windows.

Для чего используются персональные данные

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

Как долго хранятся персональные данные

ViPNet Client 5 for Windows обеспечивает автоматизированные процессы удаления данных, собираемых ViPNet Client 5 for Windows 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 Windows, за пределами продукта.

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

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 Windows можно посмотреть в интерфейсе приложения (см. [Просмотр информации о своём узле](#)).

- **Право на уточнение данных.**

Уточнение обрабатываемых ViPNet Client 5 for Windows 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 Windows не включает возможность получения согласия на операции обработки данных, осуществляемых с помощью ViPNet Client 5 for Windows. 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.

Аутентификация

Процесс односторонней или двусторонней (взаимной) проверки подлинности между клиентом (пользователем) и системой (сервером), например, с использованием учётных данных или сертификатов ключей проверки электронной подписи.

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.

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.

Открытый узел

Узел без ПО ViPNet с функцией шифрования трафика на сетевом уровне, расположенный в сети «за координатором».

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.

Токен

Устройство аутентификации, предназначенное для обеспечения информационной безопасности пользователя.

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.