



ViPNet Client 5 для ОС Аврора

Руководство пользователя

Версия продукта: 5.1.0

© АО «ИнфоТеКС», 2025

ФРКЕ.00441-01 34 01

Версия продукта 5.1.0

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 для ОС Аврора приведены в Правилах пользования, Лицензионном соглашении с конечным пользователем либо в другой эксплуатационной документации, сопровождающей ViPNet Client 5 для ОС Аврора.

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.....	4
О документе.....	4
Соглашения документа.....	4
О программе	4
Что нового в версии 5.1.0	5
Обратная связь.....	6
Подготовка к работе	7
Установка и удаление	7
Установка, обновление и удаление ключей.....	8
Для чего нужно устанавливать ключи.....	8
Установка ключей.....	8
Обновление ключей.....	10
Удаление ключей	12
Работа с ViPNet Client 5 для ОС Аврора	13
Запуск и завершение работы.....	13
Рекомендации по защите мобильного устройства.....	14
Расширенные настройки	15
Смена пароля	16
Проверка VPN-соединения.....	17
Запуск в режиме восстановления	18
Включение виртуальной видимости туннелей	18
Просмотр списка защищённых узлов и поиск узла	19
Просмотр информации о своём узле и о ViPNet Client 5	20
Регламентный контроль	21
Просмотр информации о VPN-соединении	22
Обращение в службу поддержки	23
Термины и сокращения	24

Введение

О документе

Документ поможет работать с ViPNet Client 5 для ОС Аврора (далее — ViPNet Client 5, клиент) в [защищённой сети](#) на устройствах с ОС Аврора.

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.

О программе

ViPNet Client 5 защищает IP-трафик на устройствах с ОС Аврора путём шифрования IP-пакетов.

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

Что нового в версии 5.1.0

- **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.

- **Контроль целостности среды функционирования**

В ViPNet Client 5 выполняется контроль целостности:

- при каждом запуске ViPNet Client 5,
- каждые 24 часа,
- при [регламентной проверке](#) по команде пользователя или администратора.

- **Срок действия пароля**

Клиентам с ключами в формате 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**

В целях безопасности ViPNet Client 5 записывает в системный журнал ОС Аврора критически важные события. В него записывается информация об удалении ключей, смене пароля, проверках целостности и криптографических функций. Журнал доступен только администратору устройства.

- **Установка из RuStore**

- **Поддержка ОС Аврора 5**

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](#).

Подготовка к работе

- 1 [Установите ViPNet Client 5.](#)
- 2 [Установите ключи ViPNet.](#)
- 3 [Запустите ViPNet Client 5 и подключитесь к защищённой сети.](#)

Установка и удаление

Установка



Внимание! Если на устройстве уже установлен ViPNet Client другой версии, сначала удалите его. Иначе ViPNet Client 5 не установится.

В [Аврора Маркет](#) или RuStore найдите ViPNet Client и нажмите **Установить**.

Удаление

Если в Аврора Маркет доступна витрина с ViPNet Client 5:

- 1 [Удалите ключи.](#)
- 2 Откройте **Аврора Маркет > Витрины**.
- 3 Выберите витрину с ViPNet Client 5.
- 4 Найдите ViPNet Client.
- 5 Нажмите **Удалить**.

Установка, обновление и удаление ключей

Для чего нужно устанавливать ключи

Перед использованием ViPNet Client 5 установите на устройство [ключи](#). С помощью этих ключей шифруется IP-трафик при соединениях с другими узлами защищённой сети. Без ключей работа ViPNet Client 5 в защищённой сети будет невозможна.

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

Установка ключей

- 1 Получите у администратора дистрибутив ключей.
- 2 Передайте дистрибутив ключей на устройство.
- 3 В настройках устройства выберите **Управление соединениями > VPN**.

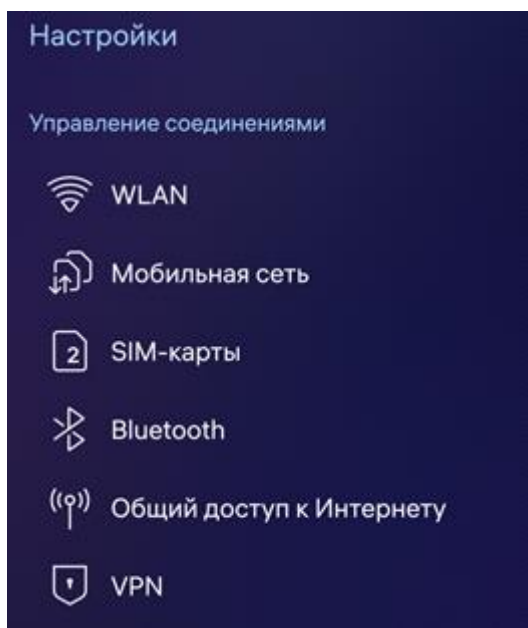


Рисунок 1. Настройки устройства

- 4 На открывшемся экране нажмите **Добавить VPN**.

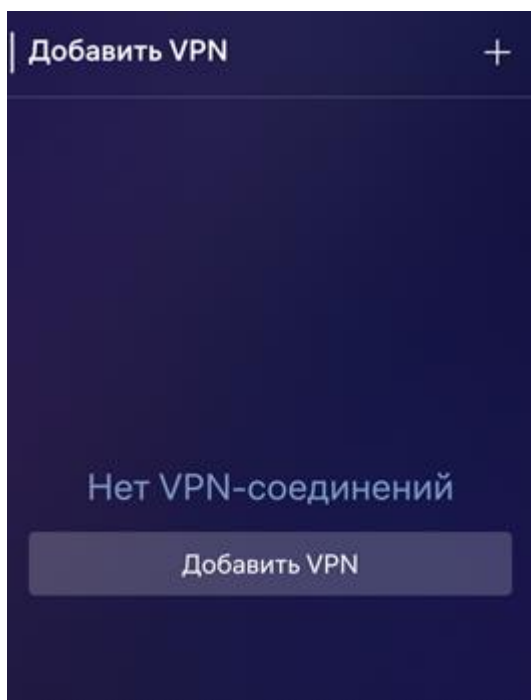


Рисунок 2. Добавление VPN-соединения

- 5 На экране **Выберите тип VPN** нажмите **ViPNet**.

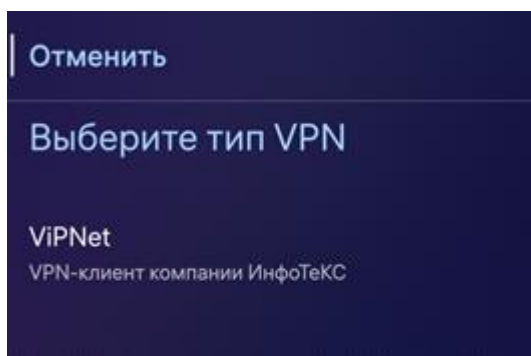


Рисунок 3. Выбор типа VPN-соединения

- 6 На экране **Новое VPN-соединение:**

6.1 Задайте имя VPN.

6.2 Введите любые символы в поле **Адрес сервера** (например, 192.168.1.1).

Поле **Адрес сервера** не влияет на настройку VPN. Если вы используете несколько VPN-соединений, указывайте для них разные значения в этом поле.

6.3 Нажмите  и выберите файл *.dst или *.ds5.

6.4 Подтвердите добавление соединения в список VPN-подключений устройства.

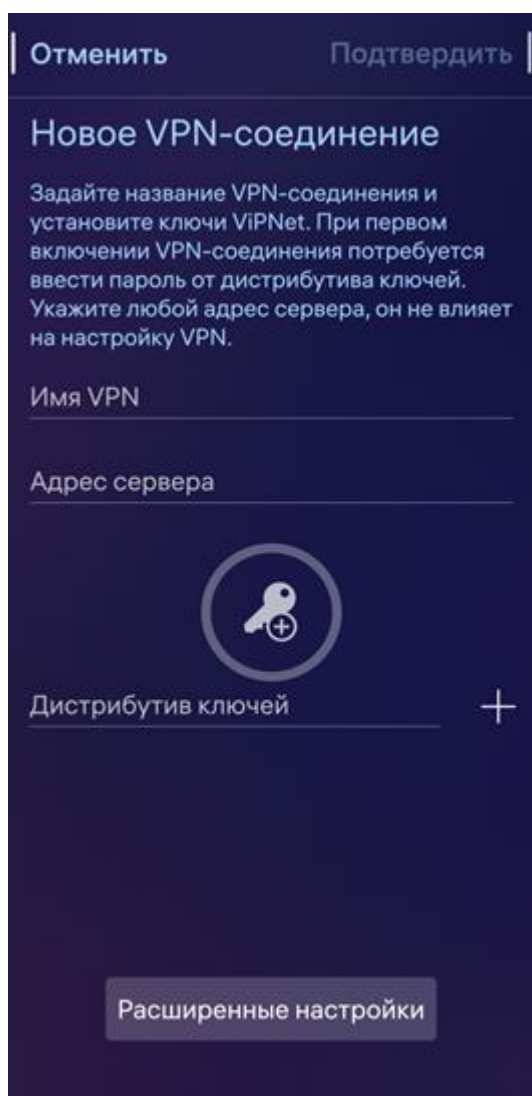


Рисунок 4. Настройка подключения к сети ViPNet

7 Подключитесь к сети ViPNet.

Обновление ключей

Обновление ключей на узле 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 новые ключи, установите их вручную:

- 1 На экране настроек устройства выберите **Управление соединениями > VPN**.
- 2 Нажмите и удерживайте имя VPN.

- 3 Нажмите **Редактировать**.

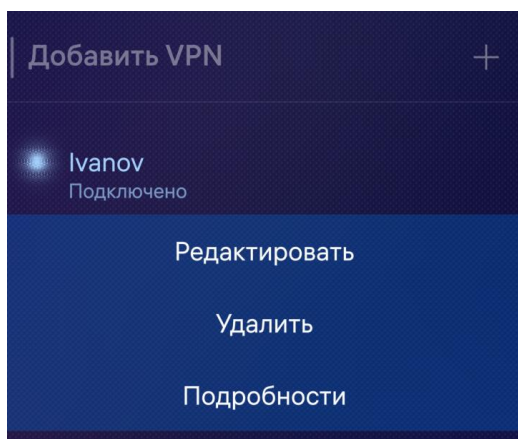


Рисунок 5. Редактирование подключения к сети ViPNet

- 4 На экране **Изменить настройки VPN** нажмите **Обновить ключи** и выберите новый файл *.dst или *.ds5.

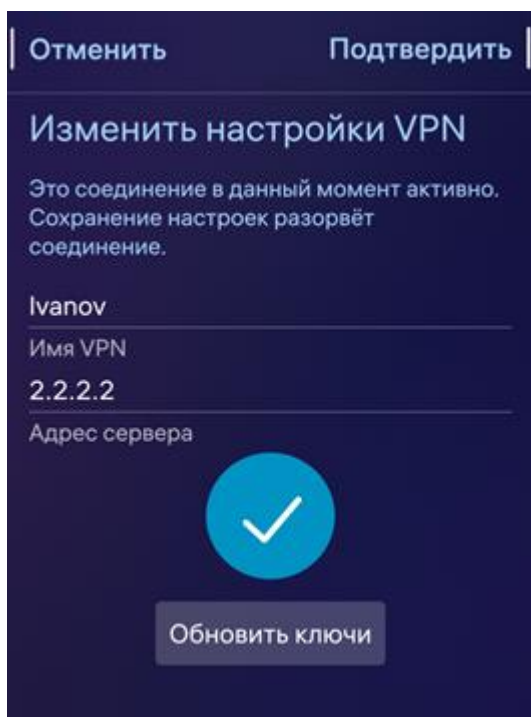


Рисунок 6. Обновление ключей вручную

- 5 Подтвердите обновление ключей и [перезапустите VPN](#).

Удаление ключей

Если вы перестаёте пользоваться ПО ViPNet, передаёте устройство другому пользователю или ключи скомпрометированы, удалите ключи:

- 1 На экране настроек устройства выберите **Управление соединениями > VPN**.
- 2 Выключите VPN-соединение: нажмите на имя VPN.
- 3 Нажмите и удерживайте имя VPN.
- 4 В появившемся меню нажмите **Удалить**.

Работа с ViPNet Client 5

Запуск и завершение работы



Внимание! Если при создании VPN-соединения вы указали ошибочные параметры, удалите его, как описано в разделе [Удаление ключей](#).

- 1 В настройках устройства выберите **Управление соединениями** > **VPN**.
- 2 Нажмите на имя VPN.

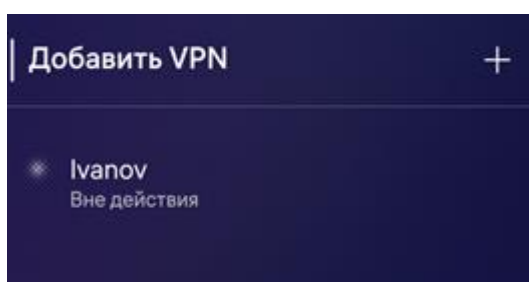


Рисунок 7. Просмотр списка VPN-подключений

- 3 Если вам назначены минимальные полномочия, и вы перезагружали устройство:
 - 3.1 В поле **DST:Password** введите пароль от дистрибутива ключей.
 - 3.2 Нажмите **Подключиться**.

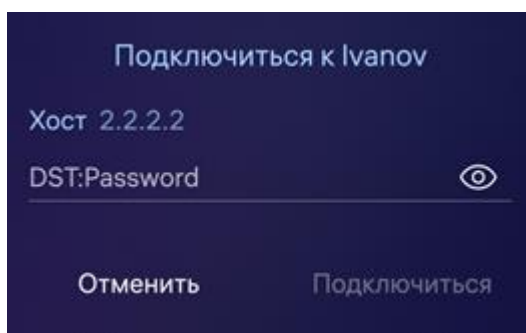


Рисунок 8. Ввод пароля для подключения к сети ViPNet

Чтобы выключить VPN-соединение, повторно нажмите на имя VPN.

Рекомендации по защите мобильного устройства

Недостаточная защита мобильного устройства, которое используется для доступа в корпоративную сеть, ставит под угрозу не только личные данные пользователя этого устройства, но и коммерческие сведения компании.

Чтобы защитить данные, хранящиеся на устройстве с ViPNet Client 5, и параметры доступа в корпоративную сеть:

- Запускайте ViPNet Client 5 только для выполнения задач, требующих доступ в защищённую сеть. Завершайте работу ViPNet Client 5, когда все задачи в защищённой сети выполнены.
- Не оставляйте без присмотра устройство с включённым VPN-соединением.
- Средствами ОС Аврора настройте блокировку экрана устройства с использованием кода безопасности, состоящего не менее чем из шести символов.

Расширенные настройки

- 1 В настройках устройства в разделе **Управление соединениями** выберите **VPN**.
- 2 Нажмите и удерживайте имя VPN.
- 3 В появившемся меню выберите **Редактировать**.
- 4 На экране **Изменить настройки VPN** нажмите **Расширенные настройки**.

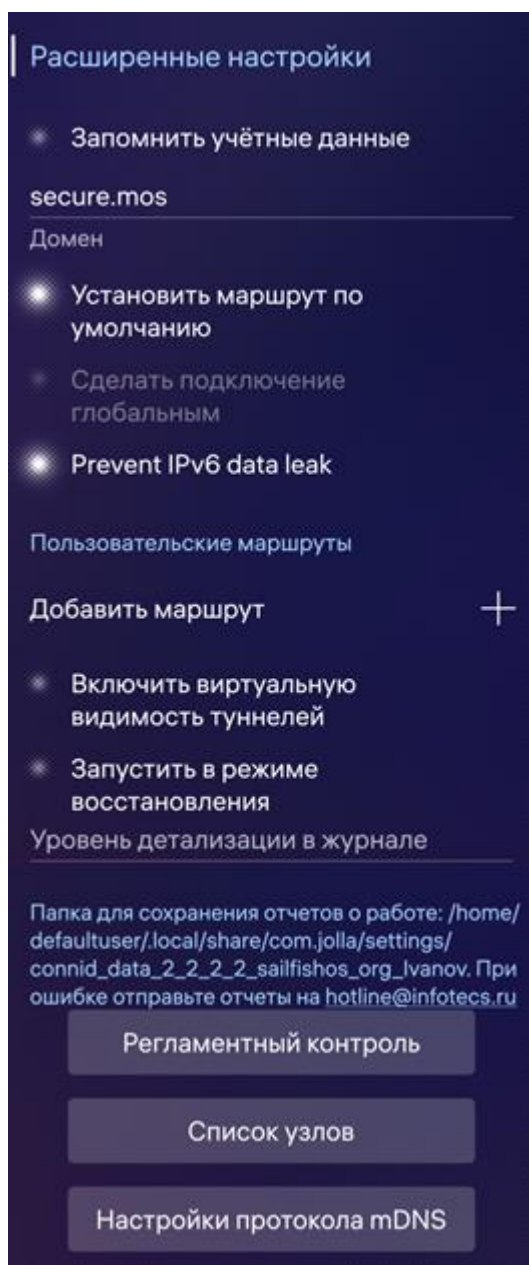


Рисунок 9. Расширенные настройки ViPNet Client 5

Смена пароля

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

- 1 [Перейдите в расширенные настройки.](#)
- 2 Нажмите **Сменить пароль**.

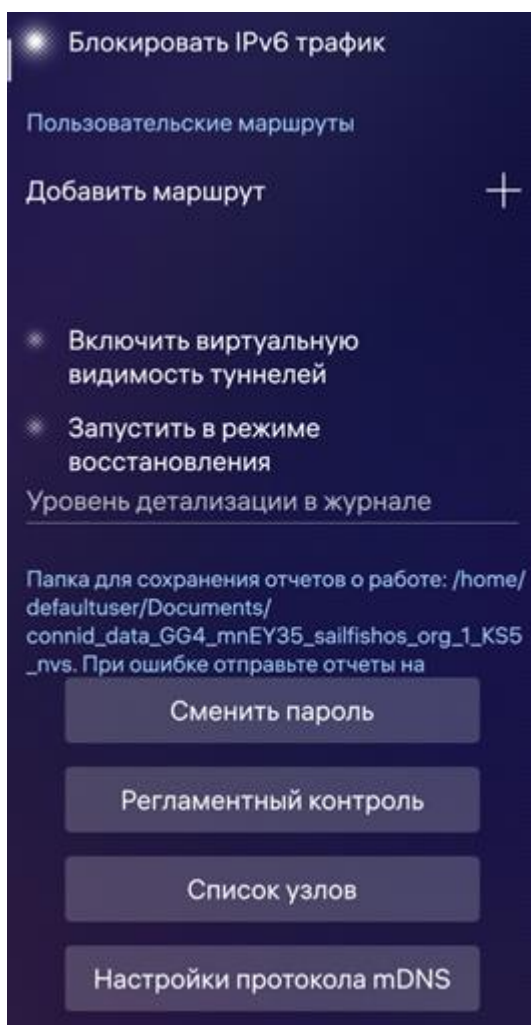


Рисунок 10. Смена пароля

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

Новый пароль должен отличаться от текущего пароля. Длина пароля латинскими буквами должна быть 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**.

Проверка VPN-соединения

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

Если прервалась связь с ресурсами защищённой сети, вы можете проверить связь с координатором вручную:

- 1 **Перейдите в расширенные настройки.**
- 2 Выберите **Список узлов**.
- 3 Нажмите  и дождитесь установления соединения с координатором. Если связь с координатором отсутствует, повторите попытку через некоторое время.

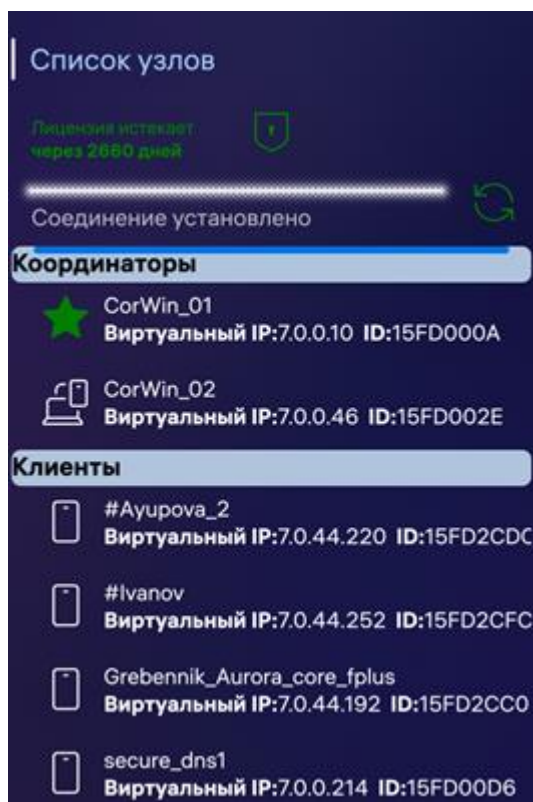


Рисунок 11. Проверка связи с координатором

Запуск в режиме восстановления

При сбое ОС, ошибках обновления справочников и ключей и в других нештатных ситуациях могут повредиться внутренние конфигурационные файлы приложения. ViPNet Client 5 автоматически их восстанавливает и поддерживает работоспособность VPN-соединения.

Если не удалось восстановить конфигурационные файлы автоматически и VPN-соединение не работает:

- 1 [Перейдите в расширенные настройки.](#)
- 2 Нажмите **Запустить в режиме восстановления.**
- 3 Вернитесь на предыдущий экран.
- 4 Нажмите **Подтвердить.**
- 5 [Включите VPN-соединение.](#)

Приложение найдёт и восстановит повреждённые конфигурационные файлы.

Включение виртуальной видимости туннелей

Часть туннелируемых ресурсов защищённой сети может быть недоступна, если их реальные IP-адреса пересекаются с адресами локальной сети устройства. Чтобы сделать ресурсы доступными, включите их видимость по виртуальным IP-адресам:

- 1 [Перейдите в расширенные настройки.](#)
- 2 Нажмите **Включить виртуальную видимость туннелей.**
- 3 Вернитесь на предыдущий экран.
- 4 Нажмите **Подтвердить.**
- 5 [Перезапустите VPN-соединение.](#)

Просмотр списка защищённых узлов и поиск узла

1 Перейдите в расширенные настройки.

2 Нажмите **Список узлов**.

Появится список защищённых узлов, с которыми вы можете взаимодействовать.

3 Чтобы найти узел, введите его имя в поле поиска внизу экрана.

4 Чтобы просмотреть подробную информацию об узле, удерживайте строку с его именем и нажмите **Об узле**.

Отобразится информация об узле. Для координаторов также отображаются туннелируемые ими IP-адреса открытых узлов.

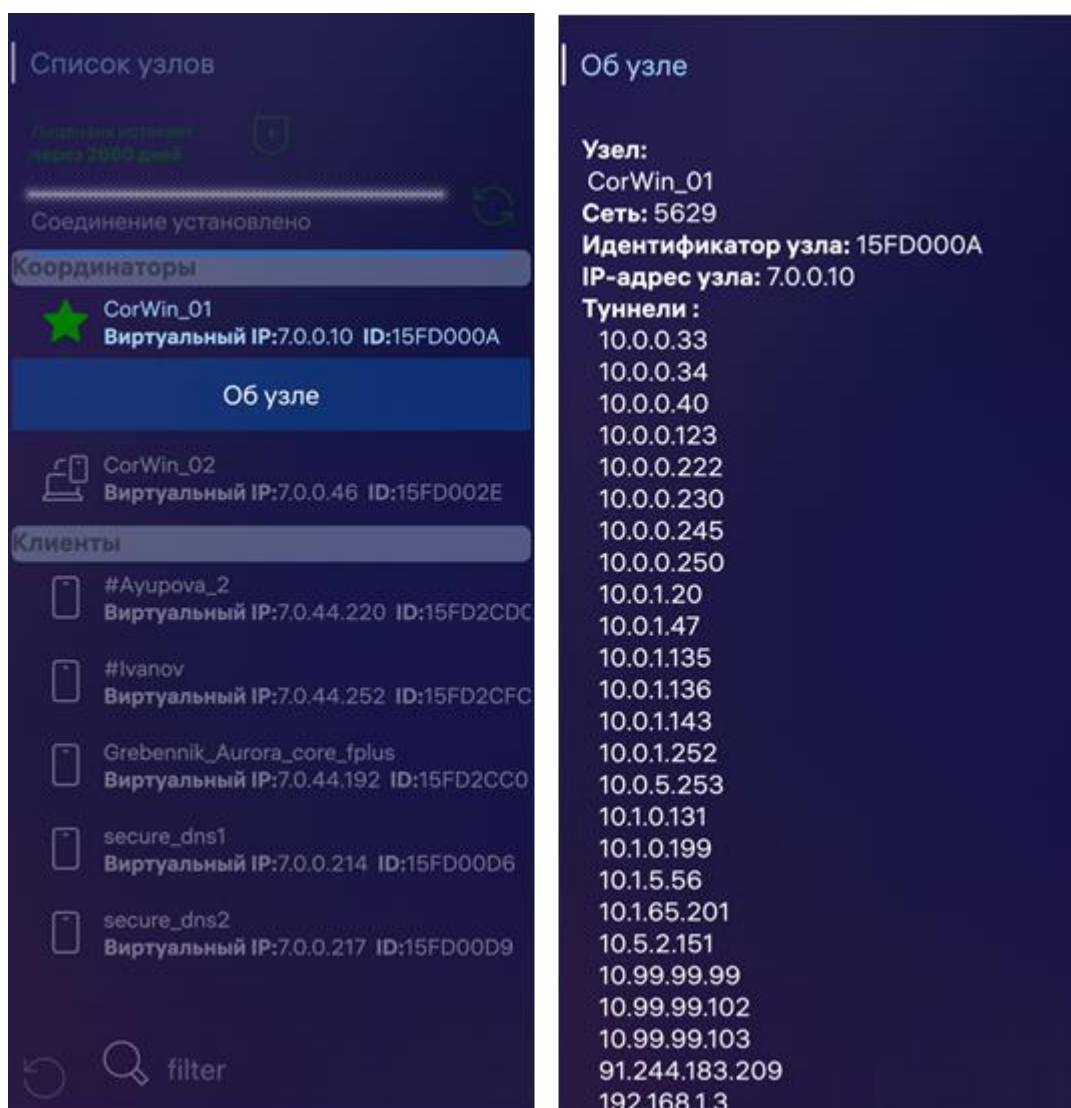


Рисунок 12. Просмотр информации о координаторе

5 Чтобы проверить доступность узла в защищённой сети, в списке узлов нажмите на его иконку.

Если узел доступен, иконка станет зелёной, если недоступен — красной.

Просмотр информации о своём узле и о ViPNet Client 5

1 Перейдите в расширенные настройки.

2 Нажмите **Регламентный контроль** > **Об узле**.

Отобразится информация:

- версия ViPNet Client 5,
- количество ключей,
- имя и идентификатор узла,
- имя и номер сети,
- даты выдачи и истечения лицензии,
- уровень полномочий:
 - 0 — минимальные,
 - 1 — средние,
 - 2 — максимальные,
- роли узла (описание ролей см. в руководстве администратора управляющего ПО).

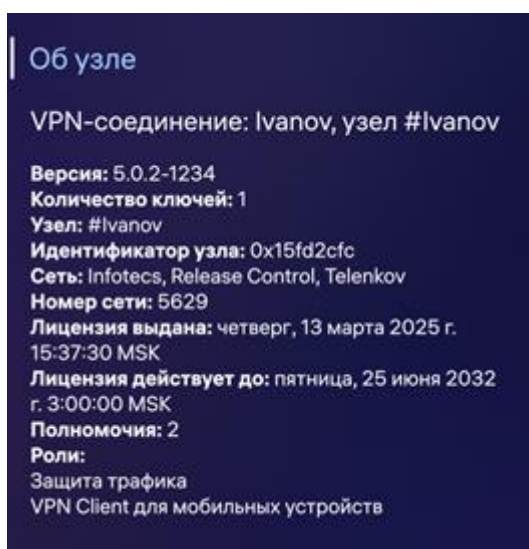


Рисунок 13. Просмотр информации о своём узле и о ViPNet Client 5

Регламентный контроль

Контроль целостности ViPNet Client 5 выполняется:

- При каждом запуске ViPNet Client 5.

При нарушении целостности сохранится запись в журнал, а подключение к сети ViPNet будет недоступно.

- Каждые 24 часа.

При нарушении целостности появится сохранится запись в журнал.

- При регламентной проверке по команде пользователя или администратора.

При нарушении целостности появится уведомление об этом, сохранится запись в журнал, а подключение к сети ViPNet будет недоступно.

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,
- криптографических функций,
- целостности.

Для этого:

- 1 [Перейдите в расширенные настройки.](#)
- 2 Нажмите **Регламентный контроль**.
- 3 На экране регламентного контроля выберите виды проверок, которые требуется выполнить, и нажмите **Начать проверку**.

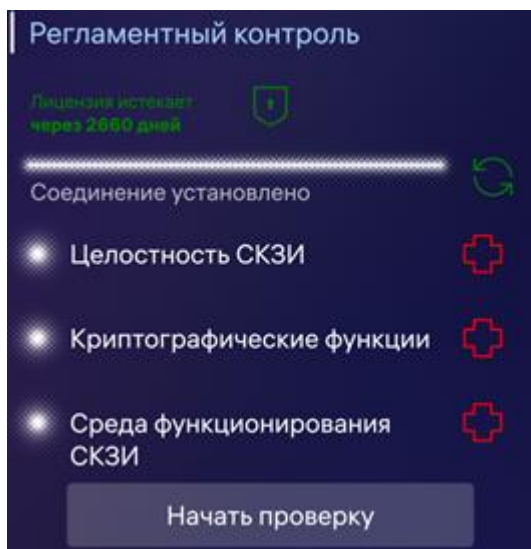


Рисунок 14. Запуск проверки целостности и работоспособности

Дождитесь завершения проверки. Результат отобразится на экране.

Просмотр информации о VPN-соединении

- 1 В настройках устройства в разделе **Управление соединениями** выберите **VPN**.
- 2 Нажмите и удерживайте имя VPN.
- 3 Выберите **Подробности**.

Откроется экран **Детали соединения**. На нём вы можете просмотреть информацию о состоянии подключения к защищённой сети, параметрах подключения и расположении ключей.

Детали соединения ViPNet	192.168.1.10/255.255.255.2557.0.44.252
Имя Ivanov	Маршрут сервера
Адрес сервера 2.2.2.2	10.0.1.252/255.255.255.2557.0.44.252
Домен secure.mos	Маршрут сервера
Состояние соединения	10.0.0.40/255.255.255.2557.0.44.252
Состояние Подключено	Маршрут сервера
Восстанавливать подключение автоматически Да	192.168.90.110/255.255.255.2547.0.44.252
Запомнить учётные данные Нет	Маршрут сервера
DNS-серверы	192.168.1.114/255.255.255.2557.0.44.252
10.0.0.40,7.0.0.214,7.0.0.217,192.168.2.2	Маршрут сервера
Адрес 7.0.44.252	10.5.2.151/255.255.255.2557.0.44.252
Маска сети 255.255.255.255	Маршрут сервера
Шлюз 91.244.183.134	10.0.1.20/255.255.255.2557.0.44.252
Другая сторона соединения 7.0.44.252	Состояние поставщика
Маршрут сервера	ViPNet.DstFile
192.168.3.108/255.255.255.2547.0.44.252	/home/defaultuser/Documents/Ivanov.dst
Маршрут сервера	ViPNet.DstPath
192.168.1.34/255.255.255.2557.0.44.252	/home/defaultuser/.local/share/system/vpn-data/data_2_2_2_2_sailfishos_org
Маршрут сервера	ViPNet.ReportBasePath
10.0.5.253/255.255.255.2557.0.44.252	/home/defaultuser/.local/share/com.jolla/settings
	ViPNet.UnmergeNewDst no
	ViPNet.vpnName Ivanov

Рисунок 15. Информация о VPN-соединении

Обращение в службу поддержки

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

- 1 Включите VPN-соединение.
- 2 Перейдите в расширенные настройки.
- 3 Нажмите **Список узлов**.
- 4 На открывшемся экране в списке проведите сверху вниз и нажмите **Создать отчет об ошибке**.
Будет создан ZIP-архив с отчётом о работе клиента. Папка с отчётами указана в расширенных настройках в строке **Папка для сохранения отчетов о работе**.
- 5 Скопируйте архив с отчётом на компьютер.
- 6 Создайте электронное письмо, опишите проблему и обстоятельства её возникновения, прикрепите к письму архив с отчётом.
- 7 Отправьте письмо на hotline@infotecs.ru.

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.

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для формирования и обновления ключей сетевых узлов ViPNet, а также для управления сертификатами и списками аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для Удостоверяющего и ключевого центра;
- задание полномочий пользователей сетевых узлов ViPNet.

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.

Мастер-ключ

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

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

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

Роль

Функциональность сетевого узла, которая решает целевые и служебные задачи сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

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

Сервер соединений

Функциональность координатора, обеспечивающая соединение клиентов друг с другом в случае, если они находятся в разных подсетях и не могут соединиться напрямую. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервер соединений для клиента также является сервером IP-адресов.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в управляющем ПО.

Сеть ViPNet

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

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.

Шлюз

Устройство, предназначенное для соединения двух сетей с разными канальными протоколами. Перед передачей данных из одной сети в другую шлюз их преобразует, обеспечивая совместимость протоколов.