ООО «АМИКОН»

УТВЕРЖДЕН

РОФ.ПЕРС.00121-01 32-ЛУ

Амиконнект для Linux

Руководство администратора

РОФ.ПЕРС.00121-01 32

Листов 30

2026

Аннотация

Настоящее руководство предназначено для администраторов систем защищенного удаленного доступа к корпоративной сети на основе «Амиконнекта» и ФПСУ, работающих на ПЭВМ в операционных системах Linux (на примерах SberOS и Debian). Руководство является документом, в соответствии с которым должны производиться установка, удаление и использование программы.

Если у вас возникнут какие-либо вопросы или предложения, вы можете обратиться непосредственно в ООО «АМИКОН». Вам всегда будут представлены подробные консультации по телефону или электронной почте.

Отзывы и предложения по документации просьба высылать на электронную почту.

Контакты:

Наш адрес: ООО «АМИКОН», Варшавское шоссе, д. 125 (секция 1, цокольный этаж), г. Москва, 117587.

Телефон: +7 495 797-64-12, +7 495 797-64-13.

Сайт: https://amicon.ru/

On-line документация по продукции ООО «АМИКОН»: https://wiki.amicon.ru/

Электронная почта: support@amicon.ru

© 2026 ООО «АМИКОН», 1994-2026. Все права защищены.
Все авторские права на эксплуатационную документацию защищены.
Документ входит в комплект поставки изделия.
Без специального письменного разрешения ООО «АМИКОН» настоящий документ или его часть в печатном или электронном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.
Информация, содержащаяся в настоящем документе, может быть изменена разработчиком

Содержание

1. Список определений и сокращений 4

2. Общие сведения 6

3. Установка «Амиконнекта» 9

3.1. Процесс установки 9

4. Установка сертификатов 12

4.1. Установка корневого сертификата 12
4.2. Установка пользовательского сертификата 13

5. Настройки VPN-профиля 15

5.1. Адрес сервера 17
5.2. Имя туннельной группы 18
5.3. Способ двухфакторной аутентификации 20
5.4. Переключение языка 21

6. Запуск «Амиконнекта» 22

6.1. Папки и системные компоненты, затрагиваемые установкой 23

7. Установка VPN-соединения с ФПСУ 26

7.1. Соединение через значок приложения 26
7.2. Соединение через окно подключения 26

8. Удаление «Амиконнекта» 28

9. Дополнительные способы настройки 29

9.1. Получение информации о сертификате пользователя 29
9.2. Экспорт логов 30

1. Список определений и сокращений

«Амиконнект» (клиент PKI)	программный клиент на устройстве пользователя. Обеспечивает инициацию защищенного VPN-соединения, передачу данных уровней L3–L7 модели OSI и взаимодействие с ФПСУ-IP для аутентификации и авторизации
ОС	операционная система
ПО	программное обеспечение
Сертификат	электронный документ, который связывает открытый ключ с определённой сущностью, такой как человек, организация или устройство. При работе с «Амиконнектом» используются корневые и личные сертификаты.
УЦ	удостоверяющий центр — доверенная третья сторона, ответственная за выдачу и отзыв сертификатов, издает сертификат открытого ключа пользователя на определённый срок и подтверждает, что конкретному пользователю принадлежит открытый ключ и соответствующий ему закрытый ключ
ФПСУ	криптомаршрутизатор и межсетевой экран ФПСУ, программный комплекс
Хост	узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую

BETA-версия «Амиконнект»	версия ПО с полным доступом к функциям на ограниченный срок
OCSP	Online Certificate Status Protocol, протокол состояния сетевого сертификата
PKI	Public Key Infrastructure, инфраструктура открытых ключей
VPN	Virtual Private Network, виртуальная частная сеть

2. Общие сведения

«Амиконнект» (клиент PKI) предназначен для защиты доступа отдельной рабочей станции к ресурсам сети передачи данных. Доступ организуется с использованием инфраструктуры открытых ключей (Public Key Infrastructure, PKI).

Между ФПСУ-IP и «Амиконнектом» поэтапно организуется защищенное VPN-соединение, через которое могут передаваться данные уровней L3–L7 модели OSI.

Взаимная двухсторонняя аутентификация клиентов PKI и ФПСУ-IP производится с использованием сертификата открытого ключа пользователя и собственного сертификата ФПСУ-IP. Пользователь Амиконнект идентифицируется реквизитами своего сертификата. На ФПСУ-IP реализованы PKI-алгоритмы RSA и ГОСТ.

VPN-протокол нечувствителен к задержкам и плохим каналам связи и способен функционировать на каналах связи с задержками до 300 мс. Клиент PKI поддерживает работу на каналах связи с задержками более 300 мс.

Организация VPN-соединения между клиентом PKI и ФПСУ-IP для доступа к информационным ресурсам реализована с применением технологий, облегчающих конфигурирование и управление сетевыми настройками клиентов, на ФПСУ-IP устанавливаются минимальные настройки клиентов PKI. Дополнительное (после первоначальной аутентификации на ФПСУ-IP) решение по доступу клиента PKI к защищаемой сети может быть принято с помощью внешних по отношению к ФПСУ-IP сервисов RADIUS, DHCP, OCSP, compliance (интеграция с комплексом информационной безопасности «САКУРА», разработанным компанией «ИТ-Экспертиза»).

Система использует клиент-серверную архитектуру, предусматривающую наличие следующих компонентов:

- VPN-клиент;
- VPN-сервер;
- compliance-клиент;
- compliance-сервер.

Данное решение может быть внедрено в действующую IT-инфраструктуру предприятия, включающую инфраструктуру PKI, либо использовано при развёртывании новой IT-инфраструктуры.

Схема взаимодействия клиента PKI и ФПСУ определяет, что пользователь клиента PKI получает от удостоверяющего центра сертификации (далее - УЦ) закрытый ключ и сертификат открытого ключа и устанавливает их на рабочую станцию клиента PKI. На ФПСУ-IP должны быть загружены ключевая пара — закрытый ключ и собственный сертификат самого ФПСУ-IP, а также сертификаты удостоверяющих центров, выдавших клиентские сертификаты клиентам PKI. При подключении клиента PKI к защищенной сети ФПСУ-IP проверяет сертификат, предъявленный клиентом PKI, и отправляет на сервер OCSP-запрос о статусе сертификата. Ответчик OCSP возвращает ответ со статусом сертификата. При действующем сертификате клиент PKI авторизуется в защищённой сети.

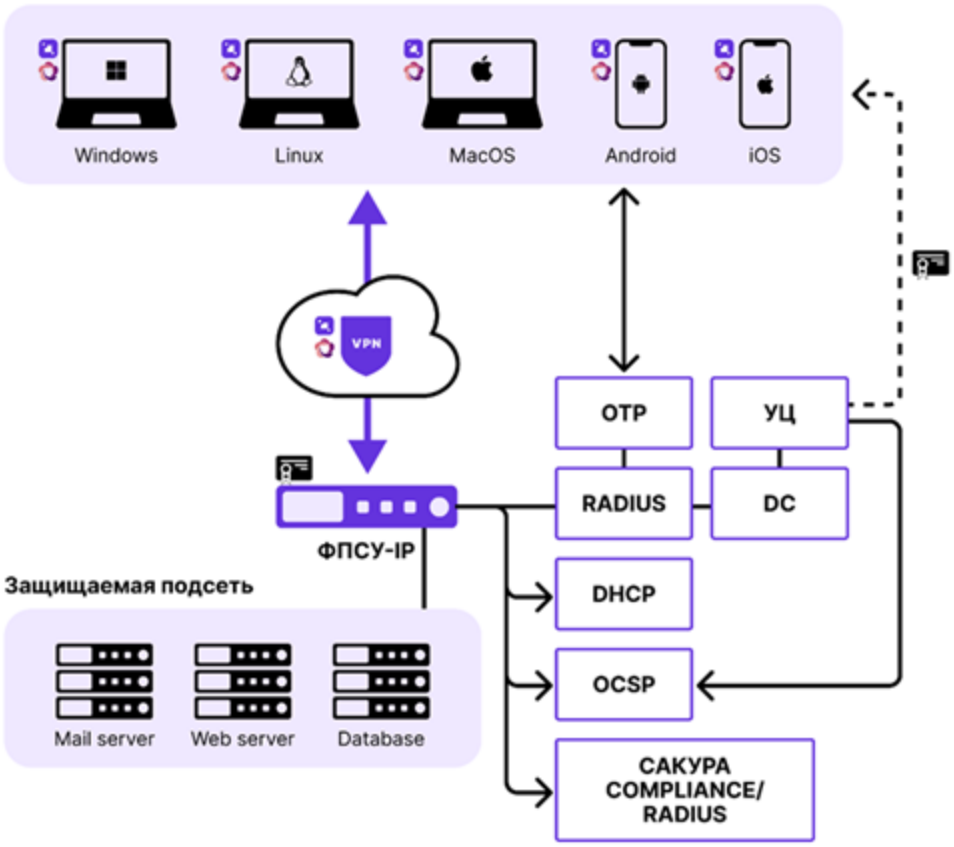


Рисунок 1 — Схема взаимодействия компонентов системы удаленного доступа

Примечание: все BETA-версии «Амиконнекта» имеют ограниченный срок действия — 90 дней с момента первого запуска.

3. Установка «Амиконнекта»

Установка и удаление клиентского приложения производится только пользователем с правами локального администратора.

Для установки программного обеспечения Амиконнект компьютер должен отвечать следующим программным и аппаратным требованиям:

- операционная система Debian 11 и выше, а также SberOS версия 3 и выше;

- аппаратные требования: в соответствии с требованиями операционной системы.

При возникновении ошибок при установке необходимо следовать инструкциям терминала, которые укажут на пакет настроек, необходимый для установки. Инструкция не описывает эти шаги, так как настройки системы в каждом конкретном случае разные.

3. 1. Процесс установки

Необходимо выполнить следующие действия:

1. Запустить терминал.

2. Установить набор компиляторов GCC 12, введя команду:

sudo apt update && sudo apt install gcc-12

На экран терминала будет выведено сообщение:

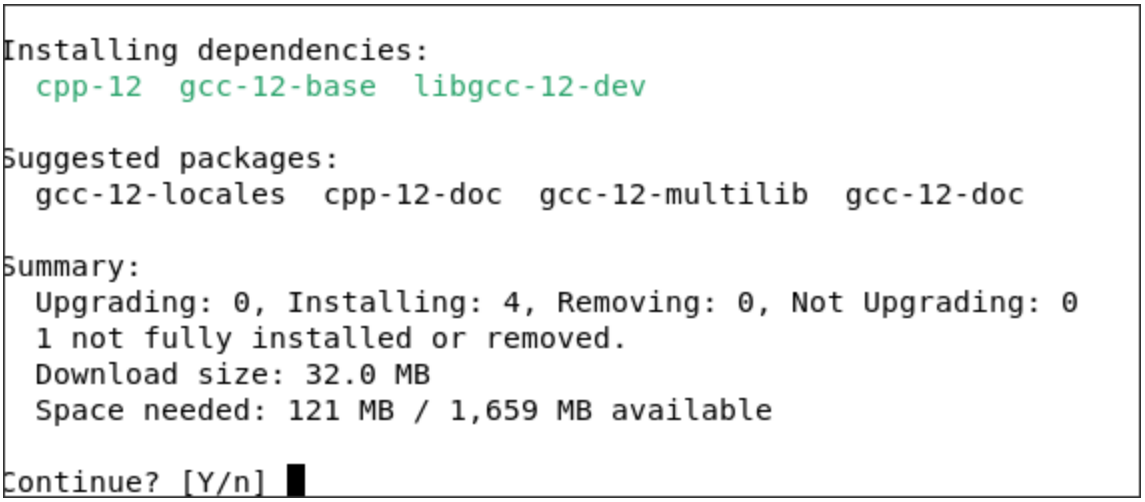


Рисунок 2 - Сообщение о загрузке набора компиляторов

Примечание: для скачивания набора компиляторов потребуется доступ в интернет. Без этого набора распаковка и установка amiconnect.service невозможна.

3. Перейти в папку, в которой находится Debian-пакет – это архив, содержащий программу, указанные зависимости, скрипты установки и инструкции для системы:

cd /path/to/dir/

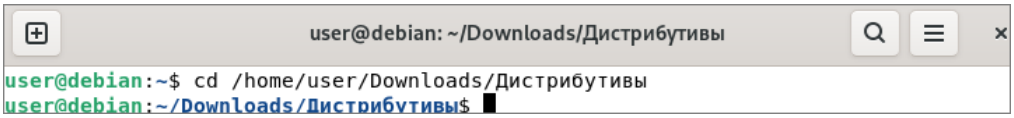


Рисунок 3 - Сообщение об изменении директории

4. Установить файл командой

sudo dpkg -i ./имя_файла

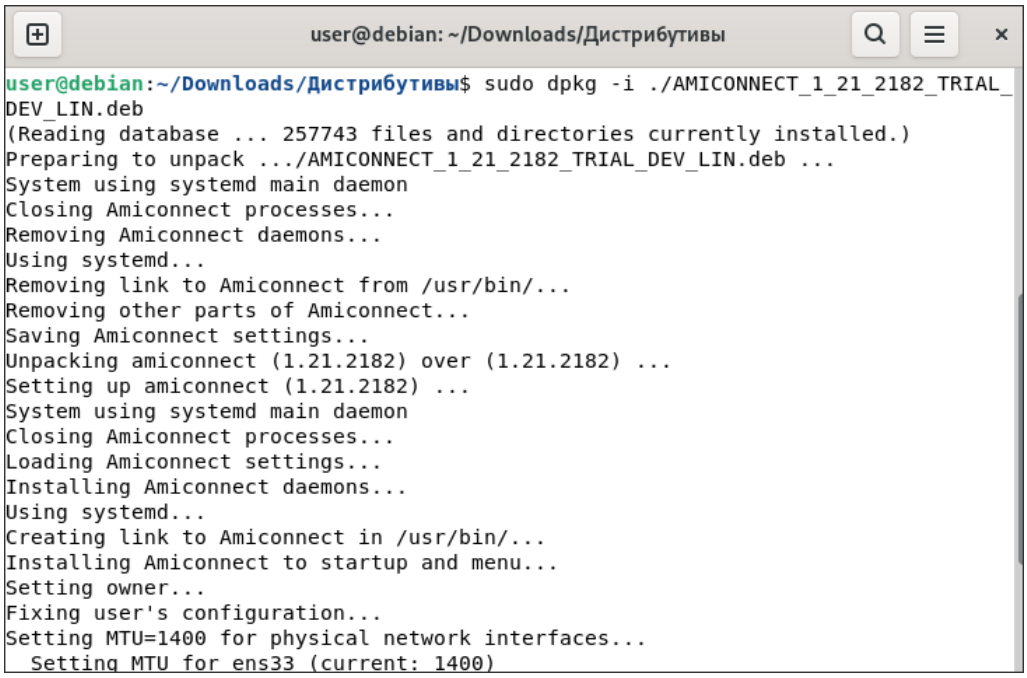


Рисунок 4 - Отображение информации об установке Амиконнект

После этих действий установка будет выполнена.

После установки приложения требуется в обязательном порядке перезагрузить систему.

4. Установка сертификатов

Даже если не требуется устанавливать сертификаты, всё равно необходимо убедиться, что корневой и пользовательский сертификаты были успешно установлены в соответствующие хранилища сертификатов и доступны для использования. Корневой и пользовательский сертификаты доступны в форматах .cer, .crt или .pfx.

Проверка осуществляется вводом в терминал команды:

certutil -d /$HOME/.pki/nssdb/ -A -t “TC,,” -n “CA” -i “расположение_сертификата/имя_сертификата"

Перед тем, как устанавливать сертификаты в систему, необходимо скачать и установить утилиты. Для системы SberOS важно помнить, что обновление пакета можно сделать только один раз.

Команды для скачивания и установки:

- *apt update*

- *apt install libc6 gcc make libopengl0 libnss3 libnss3-tools*

4. 1. Установка корневого сертификата

Для установки корневого сертификата необходимо:

- Вести в терминале команду для копирования сертификата:

certutil -d /$HOME/.pki/nssdb/ -A -t “TC,,” -n “CA” -i “расположение_сертификата/имя_сертификата”.

- Нажать Enter.

Сертификат будет скопирован.

4. 2. Установка пользовательского сертификата

Для установки корневого сертификата необходимо:

- Ввести команду для копирования сертификата в одну строку:

sudo pk12util i расположение_сертификата/имя_сертификата.pfx -W пароль -d ~/.pki/nssdb/

- Далее следует нажать Enter.

Сертификат будет скопирован.

Для проверки установки пользовательского сертификата следует убедиться в том, что сертификат отображается в списке сертификатов и проверить такие его данные как:

- Срок действия сертификата.
- Наличие закрытого ключа (если применимо).
- Соответствие имени и отпечатка сертификата.

Проверка установленного сертификата и просмотр его свойств осуществляется утилитами certutil, openssl.

После установки сертификатов необходимо убедиться, что все они отображаются в приложении Амиконнект. Запустив приложение, их можно найти в разделе настроек, связанном с сертификатами: «Профиль и адреса». Там же, на основе установленного пользовательского сертификата, отобразится профиль пользователя. В примере на изображении это

«Пользователь 1» и «Пользователь 2».

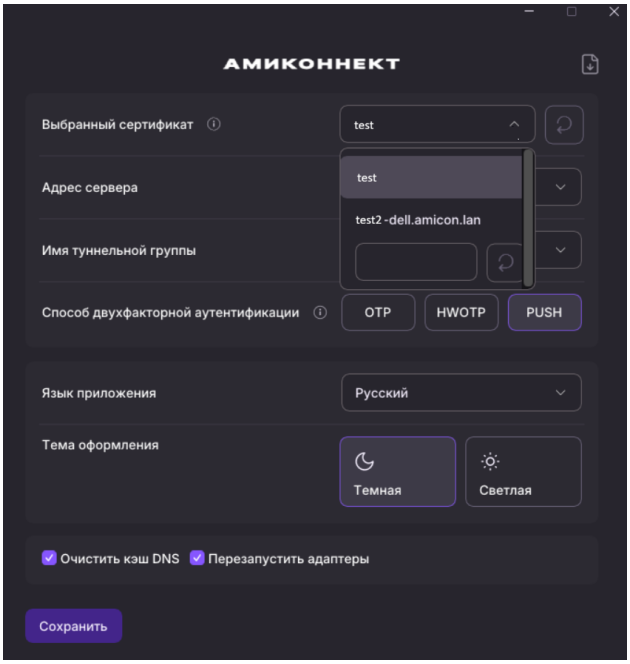


Рисунок 5 -- Профиль и адреса

5. Настройки VPN-профиля

Для настроек соединения Амиконнект и ФПСУ необходимо в выпадающем меню выбрать пункт «Открыть». Далее следует выбрать профиль и перейти в настройку его данных. Профили отображаются в интерфейсе Амиконнект исходя из найденных в локальном хранилище операционной системы пользовательских сертификатов. Разные профили могут понадобиться в том случае, если сотруднику необходимо иметь доступ к разным защищённым средам, находящимся за разными ФПСУ, и эти среды требуют наличия разных сертификатов для аутентификации пользователя.

Для настроек выбранного профиля необходимо два раза нажать левой кнопкой мыши на иконке Амиконнект в статус-баре, после чего нажать на знак настроек в правом верхнем углу открывшегося окна:

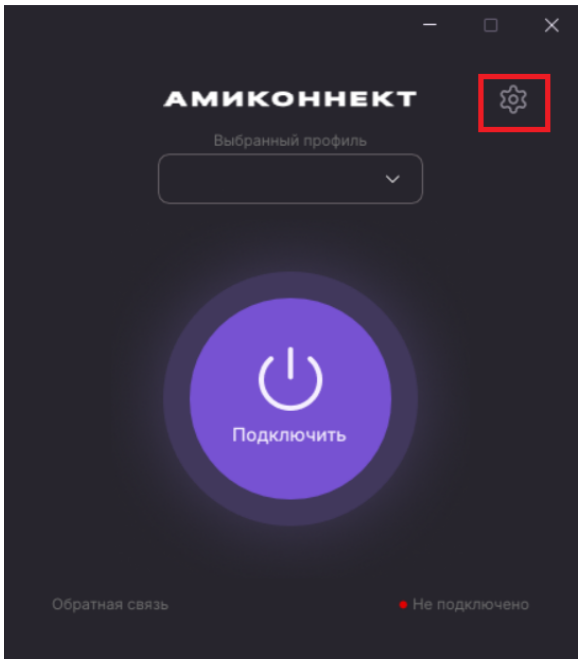


Рисунок 6 – Значок настроек

В открывшемся окне для выбранного профиля настраиваются такие параметры, как «Адрес сервера», «Имя туннельной группы», «Способ двухфакторной аутентификации». Также имеется возможность выбрать язык интерфейса и цвет темы: светлую или тёмную.

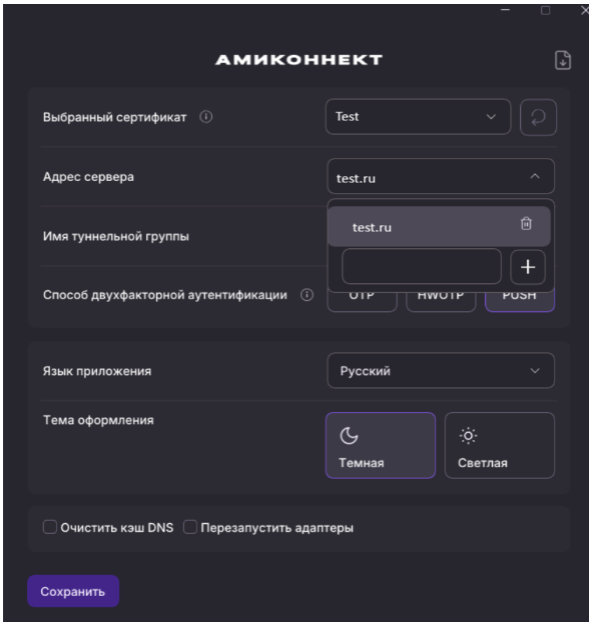


Рисунок 7 – Настройки Амиконнект

5. 1. Адрес сервера

Для настроек выбранного профиля необходимо два раза нажать левой кнопкой мыши на иконке Амиконнект в статус-баре, после чего нажать на знак настроек в правом верхнем углу открывшегося окна:

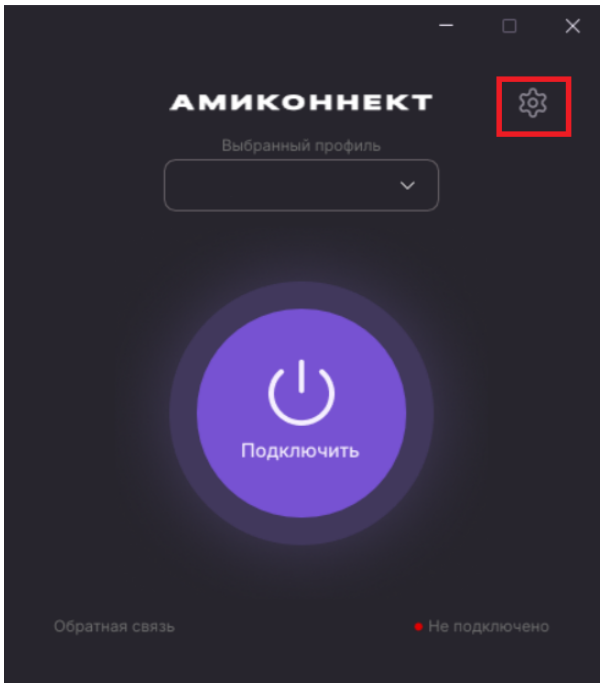


Рисунок 8 – Значок настроек

В открывшемся окне в поле «Используемый адрес» предоставляется возможность ввести IP-адрес ФПСУ-IP, через который будет осуществляться доступ Амиконнект к защищенным хостам, и нажать кнопку «+» для добавления адреса в настройки профиля.

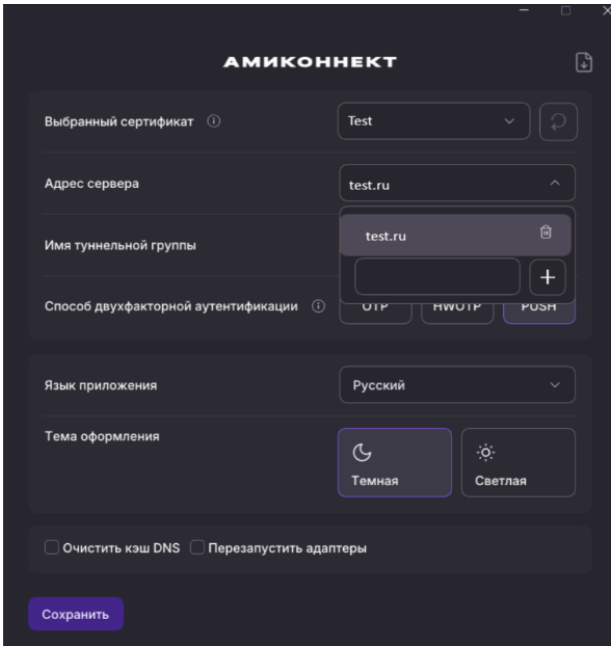


Рисунок 9 – Настройки Амиконнект

Удаление адреса возможно по кнопке удаления .

5. 2. Имя туннельной группы

Туннельные группы формируются на основе информации об издателе сертификата. При этом вводится символьное имя туннельной группы, присвоенной пользователю. Предварительно необходимо обратиться к администратору ФПСУ для уточнения имени туннельной группы и необходимости заполнения параметра

Для ввода имени туннельной группы необходимо два раза нажать левой кнопкой мыши на иконке Амиконнект в статус-баре, после чего нажать на

знак настроек в правом верхнем углу. открывшегося окна:

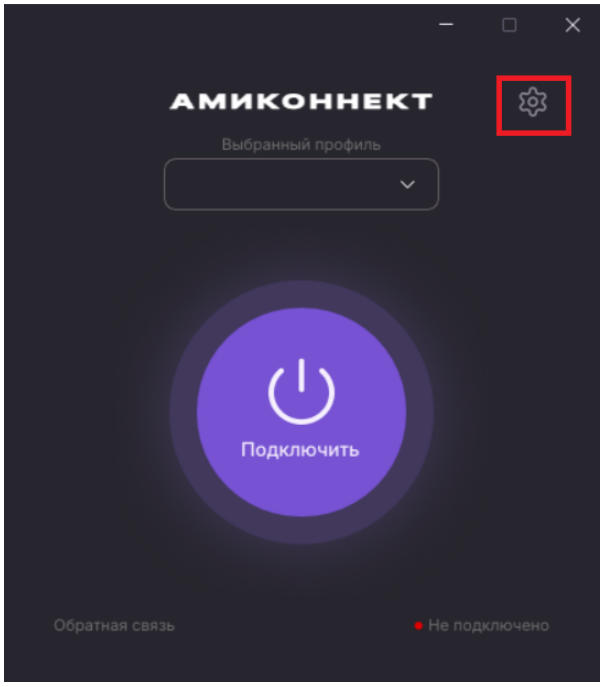


Рисунок 10 – Значок настроек

В открывшемся окне в поле «Имя туннельной группы» предоставляется возможность ввести имя туннельной группы, для разделения пользователей по разным туннельным группам и нажать кнопку «+» для добавления названия группы в настройки профиля.

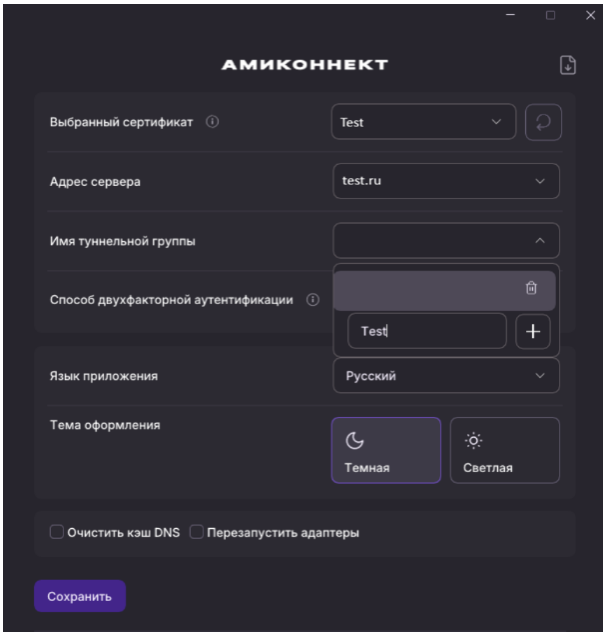


Рисунок 11 – Настройки Амиконнект

Удаление адреса возможно по кнопке удаления .

5. 3. Способ двухфакторной аутентификации

В строке выбора способа двухфакторной аутентификации есть возможность выбрать один из трех доступных и настроенных системой способов: OTP, HWOTP и PUSH:

- **OTP** – одноразовый пароль;
- **HWOTP** – пароль с внешнего носителя;
- **PUSH** – подтверждение через **SberOTP.**

То, какой именно способ необходим конкретному пользователю или группе пользователей, определяется специальным подразделением, ответственным за настройку уровней доступа интеграции **ПАК ФПСУ**. До пользователей доводится эта информация и каждый из них самостоятельно выбирает в настройке подходящий ему способ аутентификации.

5. 4. Переключение языка

Для выбора языка интерфейса необходимо перейти к пункту «Язык приложения» и выбрать «Русский» для отображения интерфейса Амиконнект на русском языке, или «English» для отображения интерфейса Амиконнект на английском языке.

6. Запуск «Амиконнекта»

Программное обеспечение Амиконнект загружается автоматически, при старте операционной системы (до регистрации пользователя в операционной системе).

После авторизации пользователя в операционной системе, в области уведомлений на панели задач отображается значок Амиконнект: .

Перед использованием Амиконнект необходимо выполнить предварительную настройку:

- добавить корневой сертификат сервера подключения;

- добавить личный сертификат пользователя;

- настроить используемый VPN-профиль.

Для вызова меню необходимо нажать левой или правой клавишей мыши на значке программы. На экран будет выдано меню Амиконнект, содержащее следующие команды:

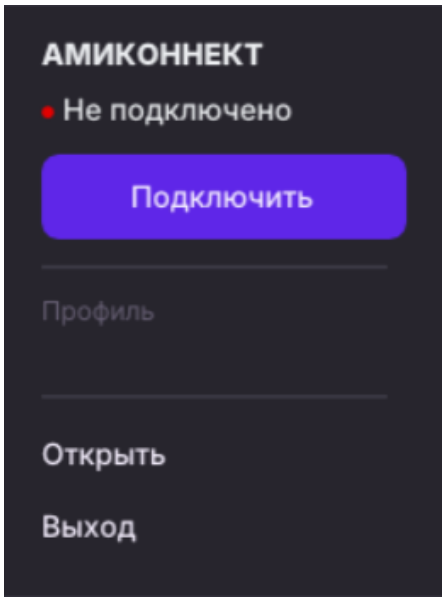


Рисунок 12 – Амиконнект

Перед использованием Амиконнект необходимо выполнить предварительную настройку:

- добавить корневой сертификат сервера подключения;

- добавить личный сертификат пользователя;

- настроить используемый VPN-профиль.

6. 1. Папки и системные компоненты, затрагиваемые установкой

Администраторам установки важно знать, какие файлы и каталоги создаются или изменяются в процессе установки приложения Амиконнект. Эта информация необходима для:

- Контроля корректности установки.
- Поиска и устранения возможных проблем.
- Резервного копирования или переноса данных.
- Обеспечения безопасности и контроля доступа к файлам.

Каталог установки:

- Папка установки клиента по умолчанию: /lib/Amiconnect
- Папка настроек пользователя: ~/amiconnect
- Имя демона amiconnectd, расположен: /lib/Amiconnect/amiconnectd
- Файл настройки автоматического запуска фонового процесса: /etc/systemd/system/amiconnect.service
- Скрипт amiconnectstartup, непосредственно запускающий фоновый процесс, находится в папке установки клиента. В качестве драйвера-фильтра используется модуль AmiNFFilterPKI, собирается в папке /lib/Amiconnect/Drivers

Файл настроек пользователя **cfg.ini** (права на запись чтение имеет пользователь) располагается в папке настроек пользователя.

Логи каждого пользователя находятся в папке настроек пользователя в подпапке log\ClientLog.csv

Логи сервиса в папке установки в подпапке log\SrvLog.csv

Файл status.json, расположенный в папке установке необходим для взаимодействия с Сакурой (права на запись чтение имеет пользователь).

Фоновый процесс обладает правами root, без чего его работа невозможна.

GUI - обладает правами пользователя.

GUI приложение Amiconnect обладает правами пользователя, посылает команды сервису для взаимодействия с драйвером и подключения к серверу ФПСУ.

7. Установка VPN-соединения с ФПСУ

7. 1. Соединение через значок приложения

Подключение к ФПСУ можно осуществить, вызвав меню нажатием курсором мыши на значок в трее или использовать специальное окно соединения. Для установки соединения пользователю необходимо выполнить несколько простых действий.

Чтобы подключиться через значок в панели задач необходимо вызвать меню нажатием курсором на значке приложения. В появившемся меню выбрать пункт «Подключить». Пользователю будет предложено пройти аутентификацию одним из трех способов аутентификации. После прохождения проверки подключение будет установлено.

При выполненном подключении значок приложения Амиконнект в панели задач изменит свой цвет на фиолетовый. Также в меню значка в панели задач, в первой строке появится надпись подключено с индикатором зелёного цвета.

Разрыв соединения можно осуществить путём нажатия на кнопку «Отключить» в меню значка приложения в панели задач.

ВАЖНО: В случае незапланированного разрыва соединения значок приложения в панели задач изменит цвет на красный. Пользователь получит уведомление о вероятных причинах разрыва соединения.

7. 2. Соединение через окно подключения

Соединение с ФПСУ также можно осуществить через специальное окно подключения (см. изображение ниже). Чтобы вызвать окно подключения необходимо дважды щелкнуть по значку приложения Амиконнект левой кнопкой мыши.

В появившемся окне подключения можно увидеть круглую кнопку с надписью «Подключить». Нажав на кнопку, можно инициировать соединение приложения с ФПСУ. При корректных настройках пользователю будет предложено пройти аутентификацию одним из трех способов аутентификации. После прохождения проверки подключение будет установлено. Цвет обводки кнопки подключения изменится (см. изображение ниже). В правой части окна подключение появится надпись «Подключено», а индикатор рядом с надписью будет окрашен в зелёный цвет.

8. Удаление «Амиконнекта»

Амиконнект полностью удаляется с устройства, включая все связанные файлы, настройки и записи в реестре. Удаление можно осуществить через терминал, для чего необходимо:

- Открыть терминал.

- Ввести команду:

```
sudo apt remove amiconnect.
```

- Нажать Enter.

После выполнения всех описанных шагов необходимо убедиться, что приложение Амиконнект, а также связанные с ним сертификаты и настройки полностью удалены с вашей рабочей станции. Это обеспечит чистоту системы и предотвратит возможные конфликты при повторной установке или использовании других программ.

9. Дополнительные способы настройки

9. 1. Получение информации о сертификате пользователя

В приложении Амиконнект реализована возможность получения информации об имени сертификата и сроке его действия прямо из приложения.

Для получения этой информации достаточно навести курсор на значок «i» (см. изображение ниже). Информация о сертификате активного профиля появится в небольшом информационном окне.

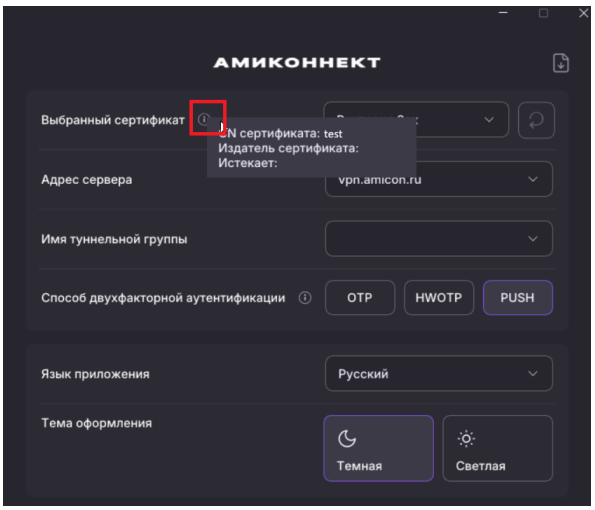


Рисунок 13 – Выбранный сертификат

9. 2. Экспорт логов

В приложении Амиконнект имеется функция выгрузки логов. Для формирования файла с записями необходимо нажать на соответствующую кнопку (см. изображение ниже). После нажатия откроется системная папка, в которой можно будет увидеть архив с записями.

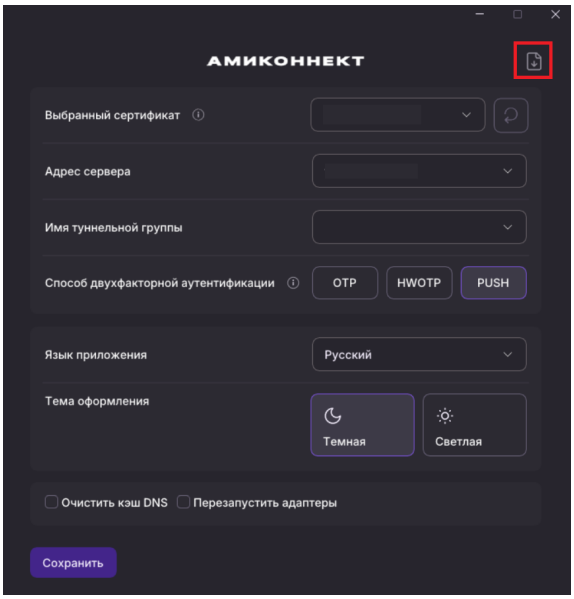


Рисунок 14 – Кнопка выгрузки логов