ООО «АМИКОН»

УТВЕРЖДЕН

РОФ.ПЕРС.00124-01 32-ЛУ

АМИКОННЕКТ
(для iOS)

Руководство администратора

РОФ.ПЕРС.00124-01 32

Листов 35

2026

Аннотация

Настоящее руководство предназначено для администраторов систем защищенного удаленного доступа к корпоративной сети на основе АМИКОННЕКТ и ФПСУ, работающих на мобильных устройствах под управлением операционных систем iOS. 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 и факс: +7-(495)797-64-12, +7-(495)797-64-13.

Сайт: https://www.amicon.ru/

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

Электронная почта: support@amicon.ru

Содержание

1. Список определений и сокращений

НСД	несанкционированный доступ к информации;
ОС	операционная система;
ПО	программное обеспечение;
ПЭВМ	персональная электронная вычислительная машина;
ФПСУ	криптомаршрутизатор и межсетевой экран ФПСУ, программный или программно-аппаратный комплекс
OCSP	«Online Certificate Status Protocol», протокол состояния сетевого сертификата
PKI	«Public Key Infrastructure», инфраструктура открытых ключей
UDP	«User Datagram Protocol», протокол транспортного уровня, не требующий подтверждения доставки дейтаграмм
VPN	«Virtual Private Network», виртуальная частная сеть
АМИКОННЕКТ (Клиент PKI)	программный клиент на устройстве пользователя. Обеспечивает инициацию защищённого VPN-соединения, передачу данных уровней L3–L7 модели OSI и взаимодействие с ФПСУ-IP для аутентификации и авторизации

МЭ	межсетевой экран
УЦ	удостоверяющий центр – доверенная третья сторона, ответственная за выдачу и отзыв сертификатов, издает сертификат открытого ключа пользователя на определенный срок и подтверждает, что конкретному пользователю принадлежит открытый ключ и соответствующий ему закрытый ключ
Хост	узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую
Сертификат	сертификат открытого ключа – электронный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу

2. Общие сведения

АМИКОННЕКТ (Клиент PKI) является средством защиты информационных обменов отдельных рабочих станций от несанкционированного доступа. Клиент АМИКОННЕКТ предназначен для построения защищенных каналов связи между рабочей станцией и ФПСУ.

Механизм защиты канала связи заключается в том, что поверх существующей общедоступной или частной сети передачи данных создается межсетевой VPN-туннель между Клиентом АМИКОННЕКТ и ФПСУ, по которому IP-пакеты передаются в зашифрованном виде, что обеспечивает целостность и конфиденциальность передаваемой информации. В VPN-туннеле производятся обязательные взаимные процедуры идентификации и аутентификации Клиента АМИКОННЕКТ и ФПСУ, как при установлении защищенного соединения, так и в процессе передачи данных через VPN-туннель.

Аутентификация взаимодействующих Клиента АМИКОННЕКТ и ФПСУ, а также шифрование передаваемой в VPN-туннеле информации производятся с использованием PKI-сертификатов, установленных на приложении и центральный компонент ПАК ФПСУ.

В памяти мобильного устройства хранятся VPN-профили пользователей, содержащие информацию о IP-адресе ФПСУ, с которым Клиент АМИКОННЕКТ устанавливает защищенный межсетевой VPN-туннель, IP-адресах находящихся за ФПСУ рабочих станций, к которым пользователь Клиента сможет получить защищенный доступ; уникальных системных номерах и имени, закрепленных за данным пользователем Клиента АМИКОННЕКТ администратором.

Во время активного VPN-соединения с ФПСУ, Клиент АМИКОННЕКТ осуществляет автоматический сбор регистрационной информации о приеме и передаче пакетов на мобильное устройство пользователя.

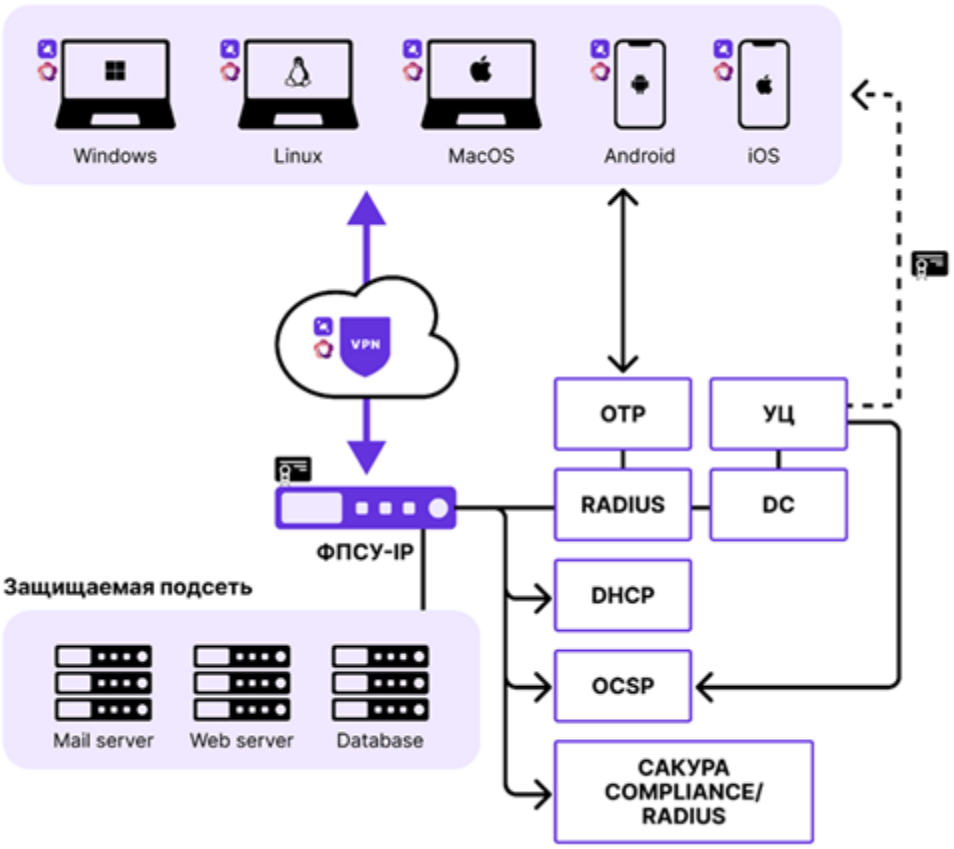

Рисунок 1 - Общая схема применения

3. Инсталляция АМИКОННЕКТ

Клиент устанавливается на мобильное устройство под управлением ОС iOS, подключенное к IP-сети передачи данных, которая обеспечивает доставку пакетов до ФПСУ с установленной подсистемой работы с АМИКОННЕКТ.

Для установки актуальной версии приложения АМИКОННЕКТ необходимо зайти с мобильного телефона, подключенного к интернет-сети в магазин приложений App Store и в поисковой строке написать название приложения АМИКОННЕКТ. В результатах поиска появится приложение.

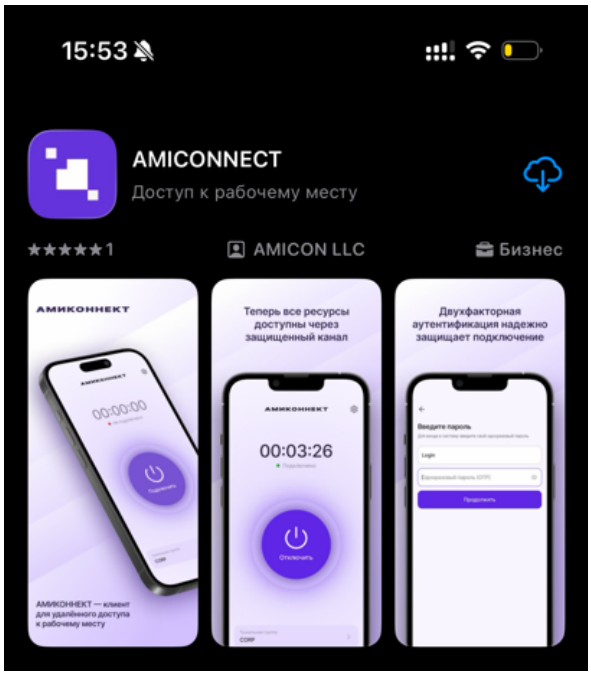

Рисунок 2 – Приложение АМИКОННЕТ в магазине приложений App Store

Далее необходимо выполнить следующие действия:

- пройти на страницу мобильного приложения;
- убедиться, что издателем является компания «АМИКОН» и

инициировать установку приложения на мобильный телефон:

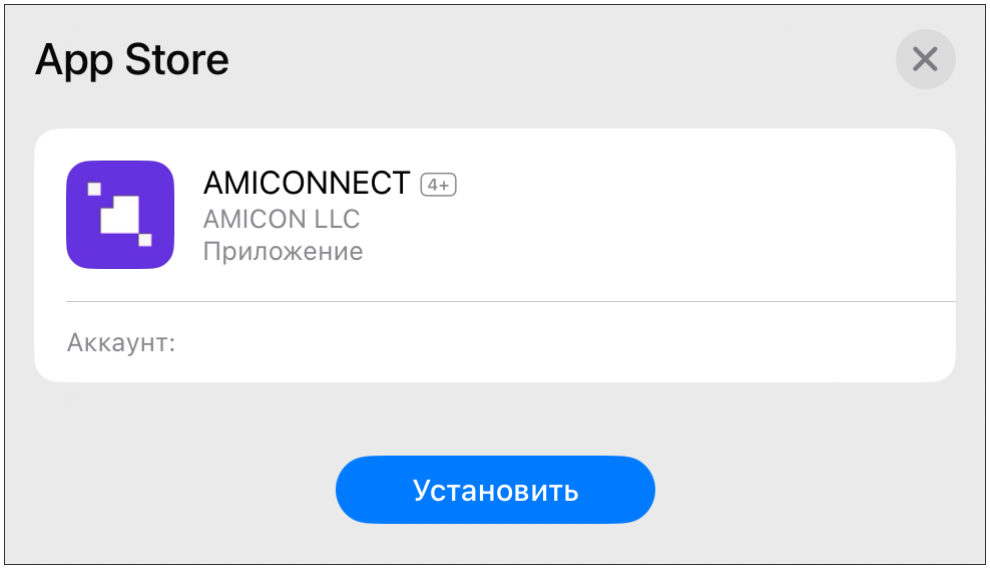

Рисунок 3 – Сообщение об издателе

4. Запуск, настройка и удаление АМИКОННЕКТ

Перед использованием АМИКОННЕКТ необходимо выполнить предварительную настройку:

- добавить корневой сертификат сервера подключения;

- добавить личный сертификат пользователя;

- настроить используемый VPN-профиль.

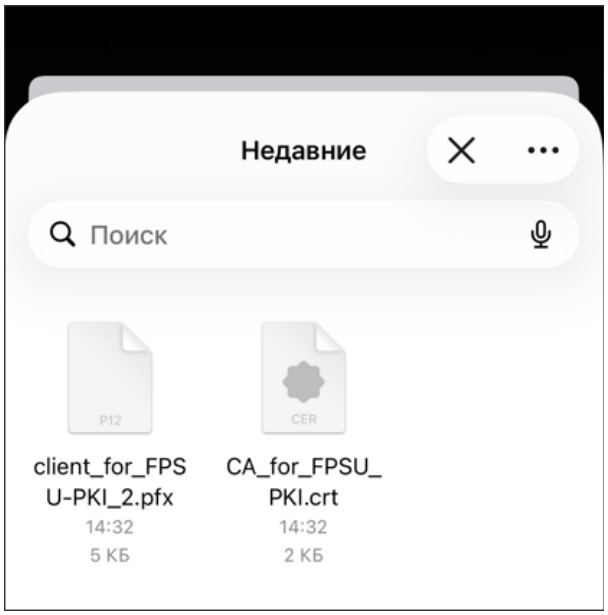

Рисунок 4 – Окно хранилища файлов

4. 1. Работа с VPN-профилем

Для инициации соединения необходимо создать профиль. Существует два способа настройки профилей пользователя и загрузки сертивикатов:

1. Через каталог настроек: загрузку каталога, в который входят сертификаты и адреса подключения.

2. Сертификаты загружаются вручную, адрес подключения вписывается отдельно. При запуске приложения пользователю будет предложено загрузить каталог настроек, что соответствует первому способу настройки.

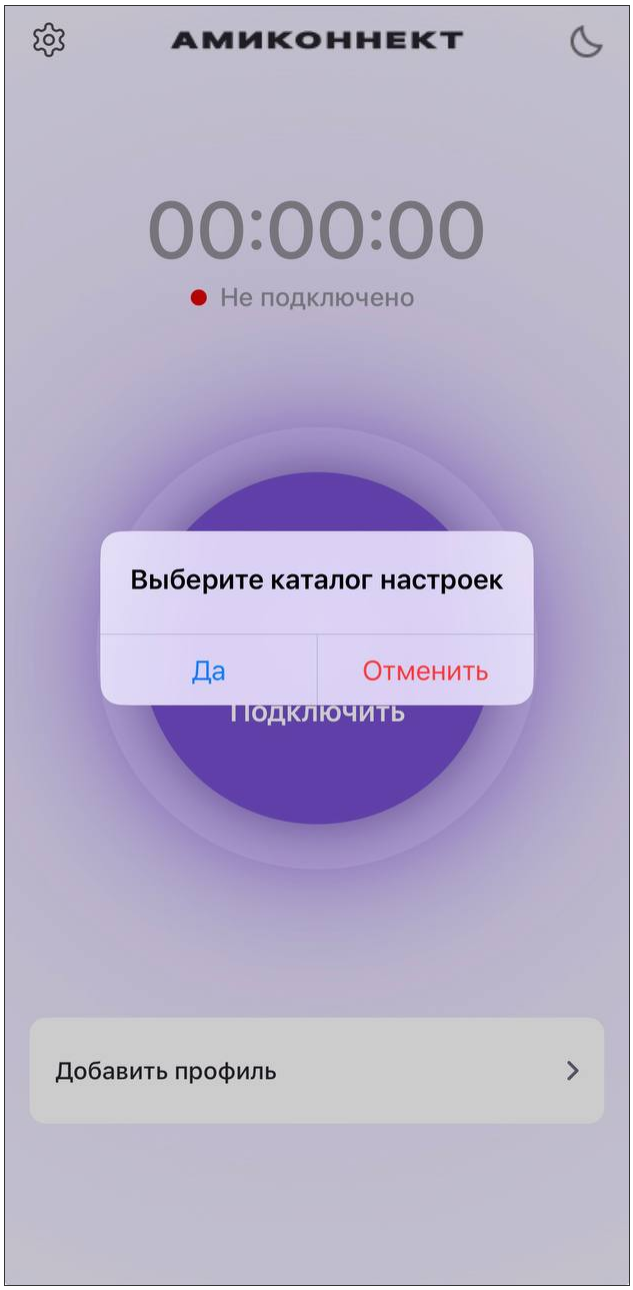

Рисунок 5 – Выбор каталога настроек

Нажав на уведомлении «Да» пользователь попадёт в хранилище файлов. В хранилище необходимо выбрать заранее помещенный туда каталог. При загрузке каталога все настройки профиля установятся автоматически. Останется только их проверить в пункте настроек и выполнить тестовое подключение. Шаги для выполнения тестового

подключения к ФПСУ описаны в соответствующей части инструкции.

Для ручной настройки (второй способ) необходимо при появлении уведомления, предлагающего загрузить каталог настроек, нажать «Отменить», пройти в настройки нажав на значок шестерёнки и в открывшемся окне настроек выполнить загрузку корневого и личного сертификатов. Это необходимо для установки будущего соединения с ФПСУ.

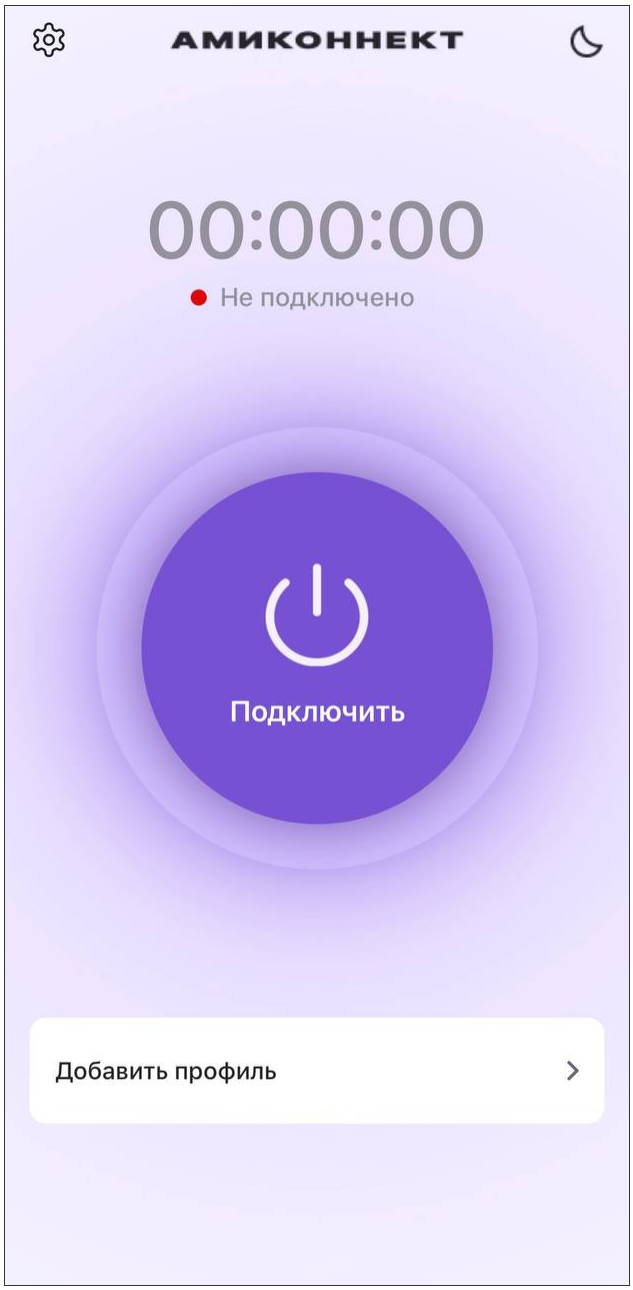

Рисунок 6 – Главное окно

Кроме того предоставляется возможность выйти на главный экран и внизу окна нажать на кнопку «Добавить профиль». В открывшемся окне «Профили» необходимо нажать на «+» и пройти в окно «Сертификат .pfx». Здесь требуется нажать на кнопку «+ Добавить сертификат». Приложение откроет хранилище файлов, в котором необходимо найти личный сертификат и добавить

его нажатием на него. Сертификат будет добавлен в профиль. Имя профиля будет отображаться в списке «Профили». Теперь можно вернуться на главный экран нажав на кнопку «Стрелка назад» в верхнем левом углу.

4. 1. 1. Установка сертификатов

На главном экране приложения необходимо найти значок Настройки (шестерёнка в верхнем правом углу), нажав на значок, вы окажетесь в окне настроек.

В открывшемся меню настроек необходимо выбрать пункт «Сертификат».

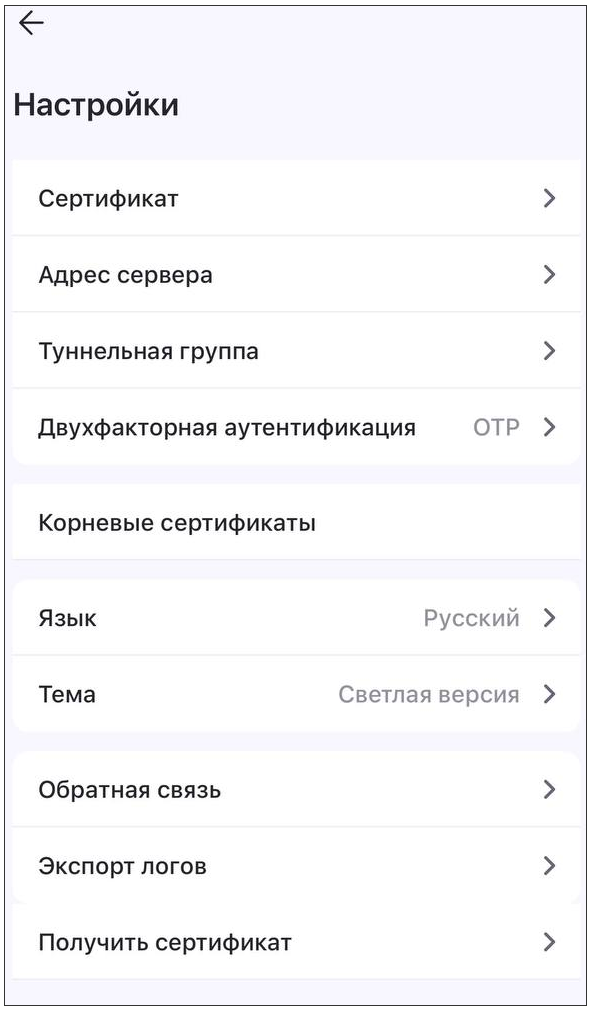

Рисунок 7 – Окно настроек

Далее открывается окно добавления сертификатов. Необходимо нажать на пункт «+ Добавить сертификат».

Рисунок 8 – Окно добавления корневого сертификата

После нажатия на пункт «+ Добавить сертификат» откроется хранилище файлов, в которое заранее должны быть помещены сертификаты (корневой и личный). Для установки сертификатов необходимо найти их среди файлов и поочерёдно загрузить в приложение.

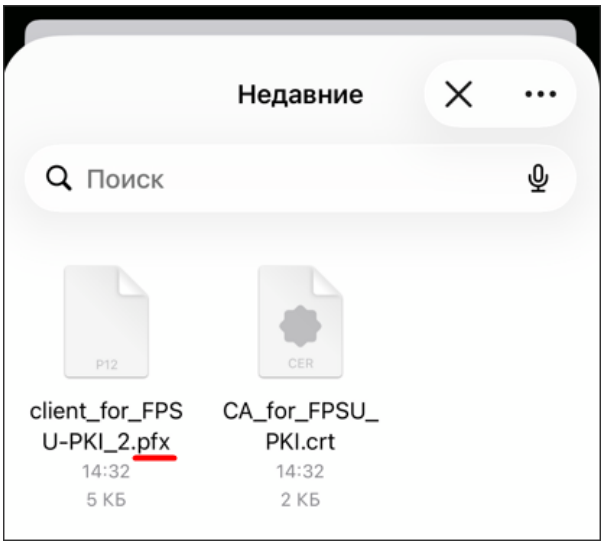

Рисунок 9 – Окно хранилища файлов

Личный сертификат должен быть загружен в формате .pfx и для его установки потребуется ввести пароль, установленный при генерации сертификата.

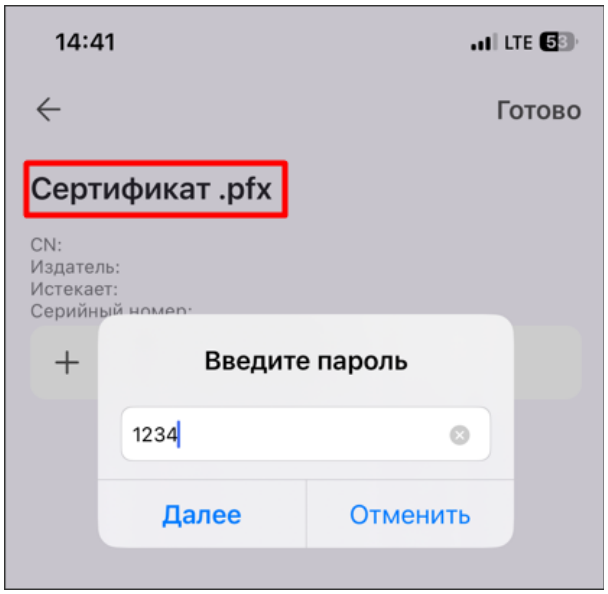

Рисунок 10 – Окно для ввода пароля при добавлении личного сертификата

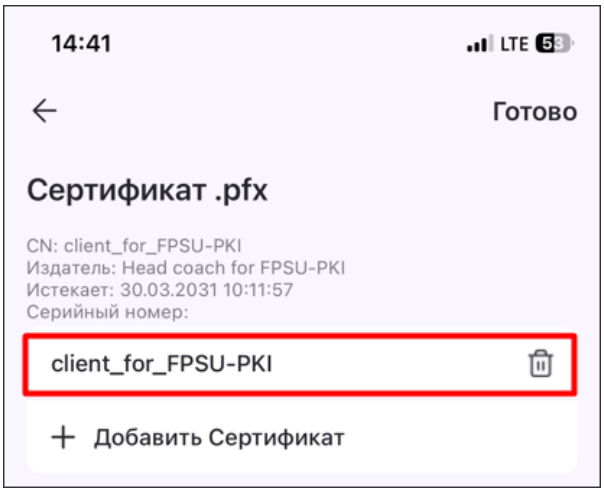

Рисунок 11 – Окно с добавленным личным сертификатом

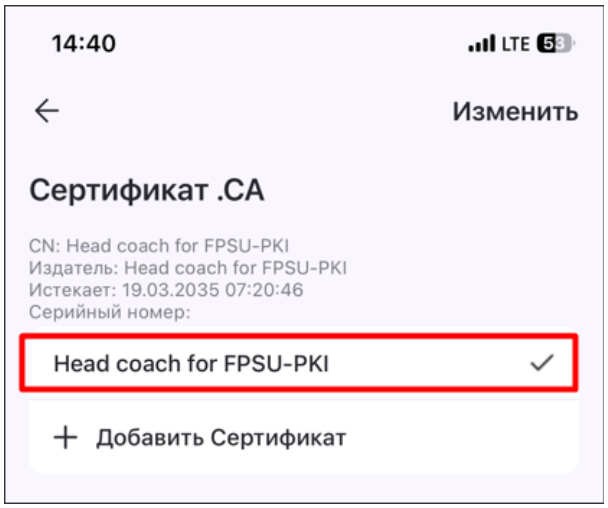

Рисунок 12 – Окно с добавленным корневым сертификатом

4. 1. 2. Добавление адреса подключения

После загрузки сертификатов необходимо вписать адрес подключения. Для этого в окне настроек необходимо выбрать пункт «Адрес ФПСУ» — это адрес, с которым будет инициироваться подключение приложения для создания защищенного соединения.

На экране мобильного устройства откроется окно «Адрес сервера».

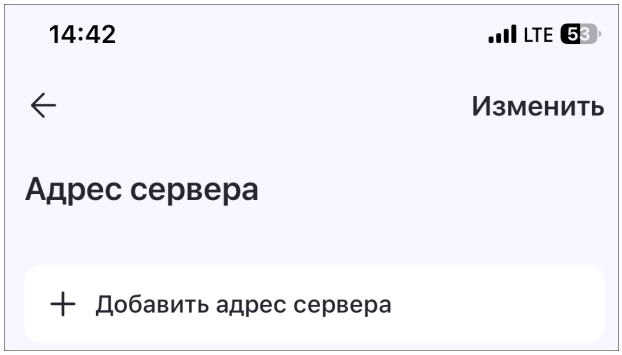

Рисунок 13 – Окно для добавления адреса сервера

Далее необходимо нажать «+ Добавить адрес сервера», после чего на экране откроется окно для ввода адреса сервера.

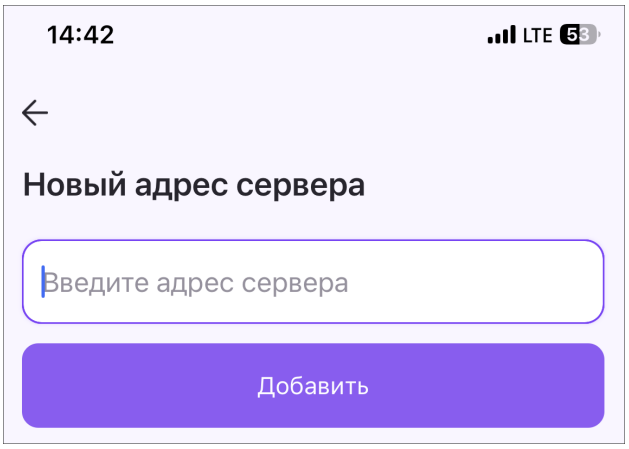

Рисунок 14 – Окно для ввода адреса сервера

После ввода ip-адреса или наименования сервера необходимо нажать кнопку «Добавить».

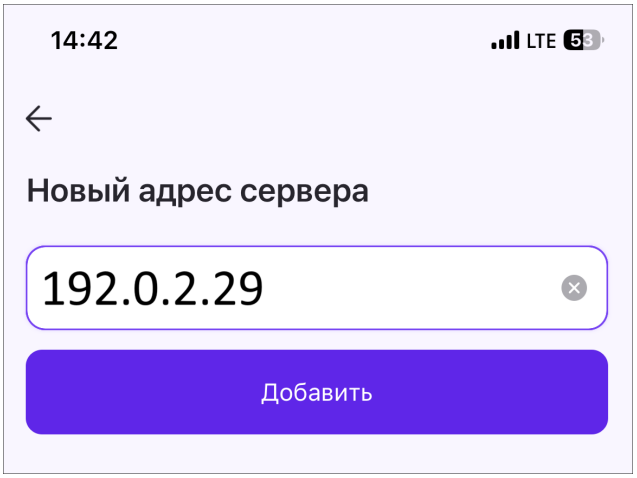

Рисунок 15 – Окно с добавленным адресом сервера

После добавления адреса сервера необходимо нажать кнопку возврата в меню настроек («□ ») - адрес будет отображен в окне настроек.

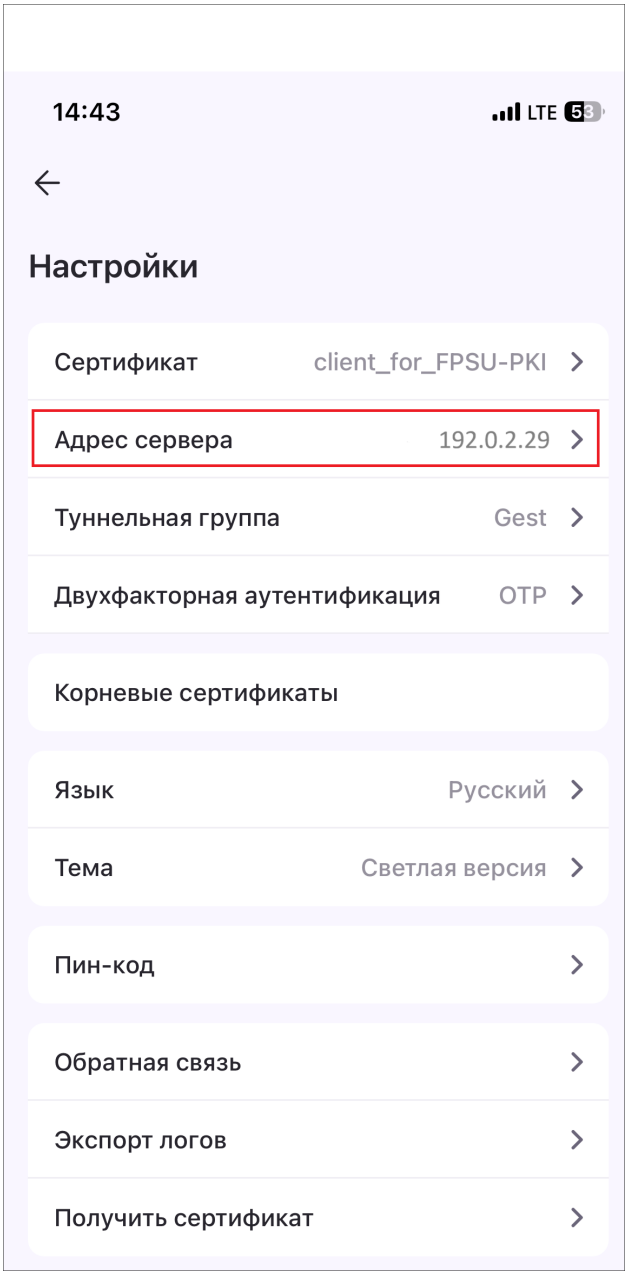

Рисунок 16 – Окно настроек с введенным адресом

4. 1. 3. 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.

На главном экране приложения необходимо найти значок Настройки (шестерёнка в верхнем правом углу), нажав на значок, вы окажетесь в окне настроек.

В открывшемся меню настроек необходимо выбрать пункт «Тунельная группа».

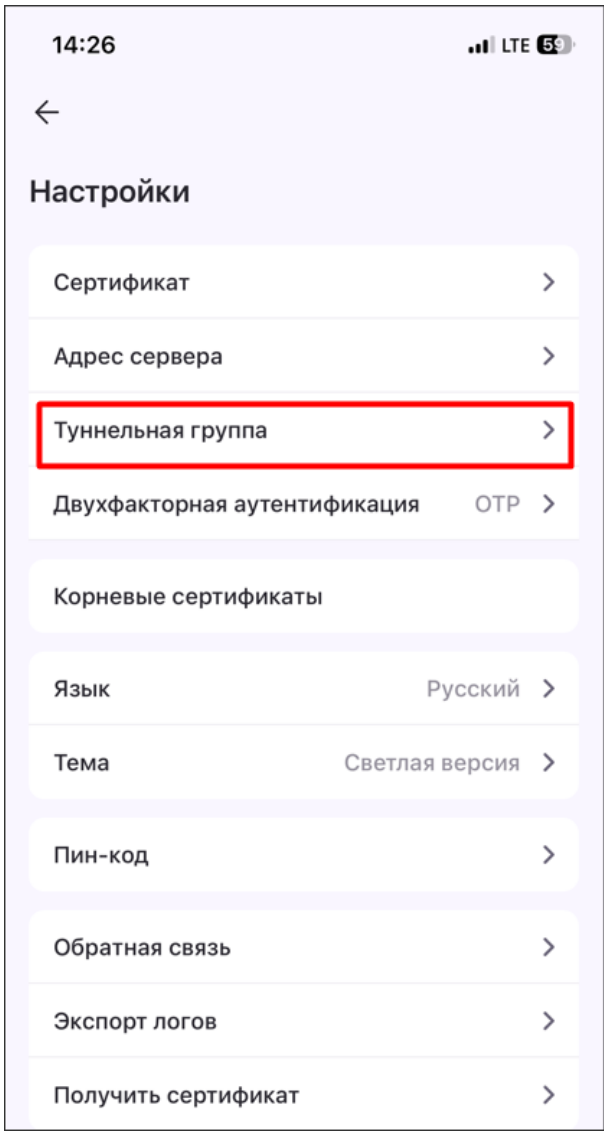

Рисунок 17 – Окно настроек

Далее необходимо нажать «+ Добавить туннельную группу», после чего на экране откроется окно для ввода имени туннельной группы.

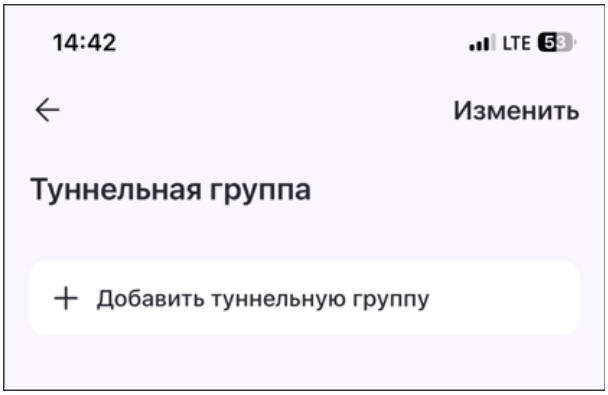

Рисунок 18 – Окно для добавления туннельной группы

После ввода имени туннельно группы необходимо нажать кнопку «Добавить».

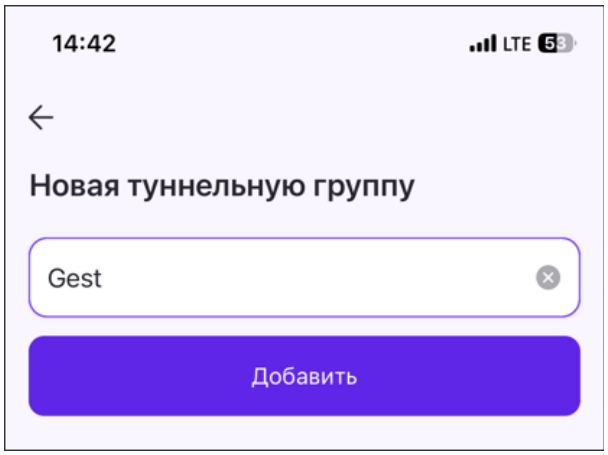

Рисунок 19 – Окно для ввода имени туннельной группы

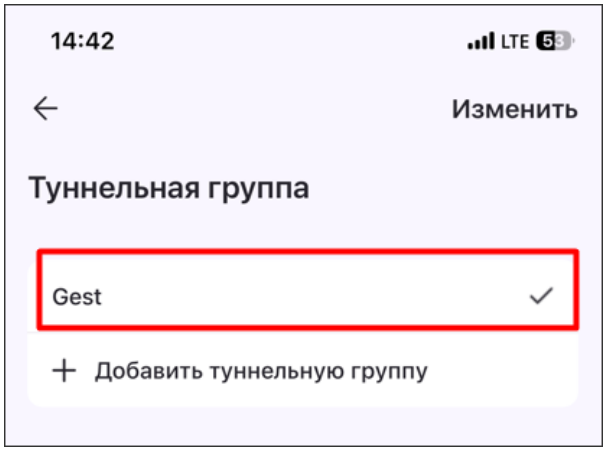

Рисунок 20 – Окно с дабавленным именем туннельной группы

После добавления имени туннельной группы, необходимо нажать кнопку возврата в меню настроек («□ ») - адрес будет отображен в окне настроек.

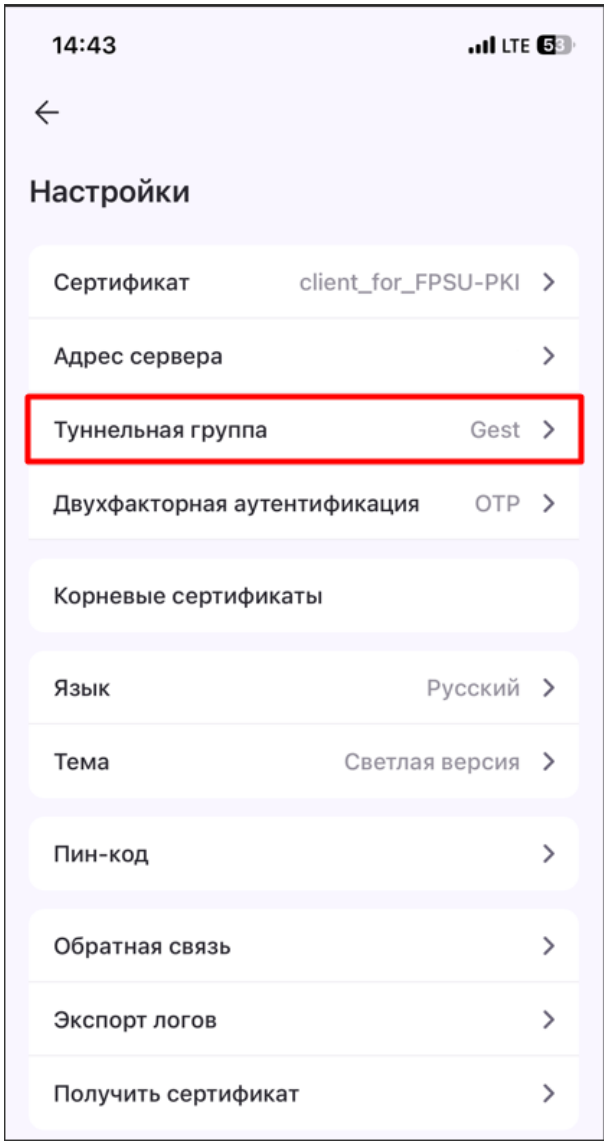

Рисунок 21 – Окно настроек с добавленным именем ткннельной группы

4. 1. 4. 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.**

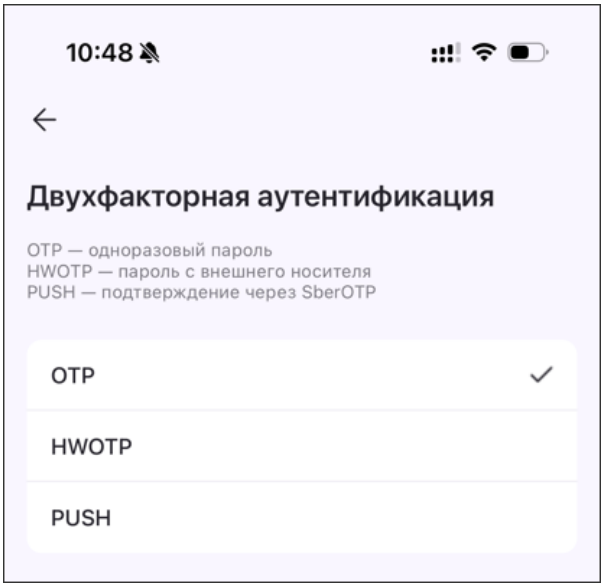

Рисунок 22 – Окно с выбранной аутефикацией OTP

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.

4. 2. Удаление VPN-профиля

При необходимости VPN-профиль (профиль пользователя) может быть удален. Для того, чтобы удалить VPN-профиль, необходимо выбрать VPN-профиль из списка, открыть вкладку «Профили» на главном экране приложения, и перейти в хранилище профилей. Проведя пальцем влево по профилю, вы вызовете появление кнопки «Удалить». При нажатии на кнопку можно увидеть появившееся уведомление подтверждающее удаление профиля.

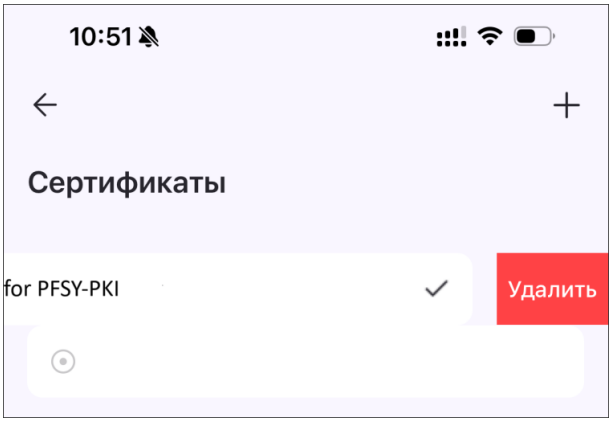

Рисунок 23 – Окно удаления VPN-профиля

После подтверждения действия профиль будет удален.

4. 3. Удаление приложения АМИКОННЕКТ

Удаление приложения АМИКОННЕКТ производится обычным способом. Удалить его можно путём недолгого удерживания иконки приложения до появления дрожания приложений на экране телефона и крестика в углу приложения.

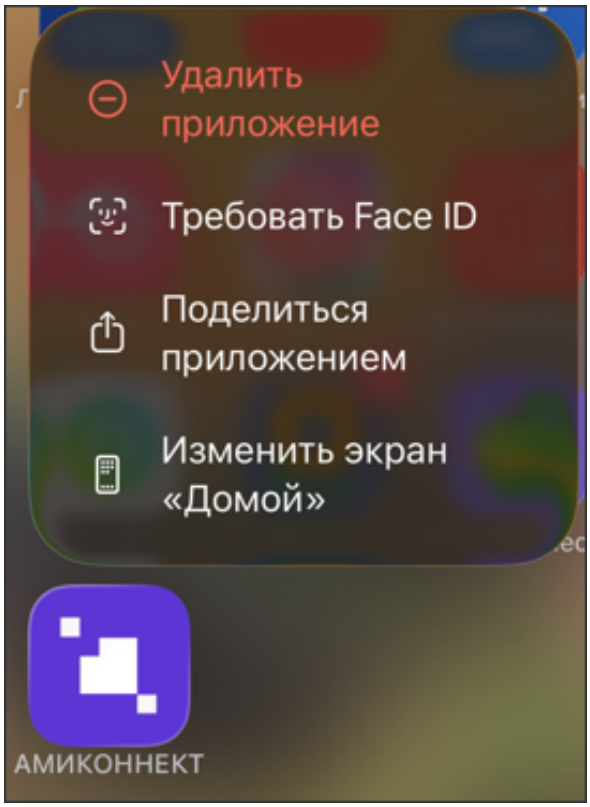

Рисунок 24 – Удаление приложения с экрана телефона

Также есть возможность удалить приложение через настройки: Настройки – Основные – Хранилище iPhone. Далее в списке приложений необходимо найти приложение Клиент АМИКОННЕКТ, пройти в настройки приложения и нажать на кнопку «Удалить приложение». Приложение будет удалено.

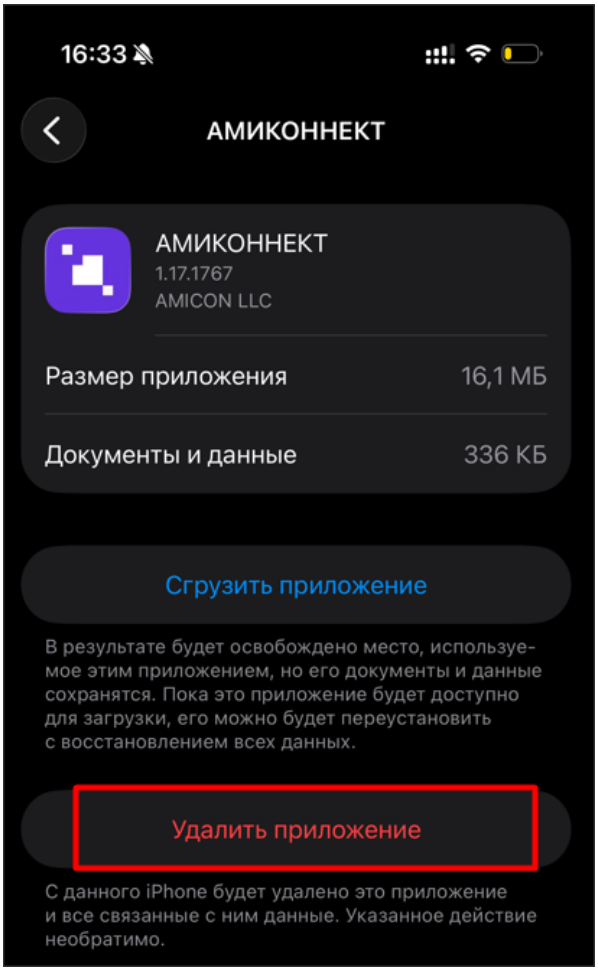

Рисунок 25 – Удаление приложения через меню настроек телефона

При удалении приложения, из папки «Документы» также будет удалена системная папка программы со всем её содержимым. Если сертификаты хранились не в ней, то их необходимо удалить вручную. После удаления сертификатов процесс деинсталляции программы и её компонентов можно считать завершенным.

5. Установка VPN-соединения с ФПСУ

При использовании мобильного приложения «АМИКОННЕКТ» аутентификация производится с применением VPN-профиля (профиля пользователя). Для создания VPN-профиля пользователя используется ключевая информация на основе сертификатов PKI.

VPN-профили, добавленные на мобильное устройство (смартфон или планшет), позволяют подключаться к ФПСУ в соответствии с заданными параметрами.

Чтобы инициировать подключение к ФПСУ необходимо выйти на главный экран приложения и нажать на кнопку «Подключить». При первом подключении операционная система попросит подтвердить внесение VPN-конфигурации. Для продолжения работы необходимо разрешить добавление конфигурации.

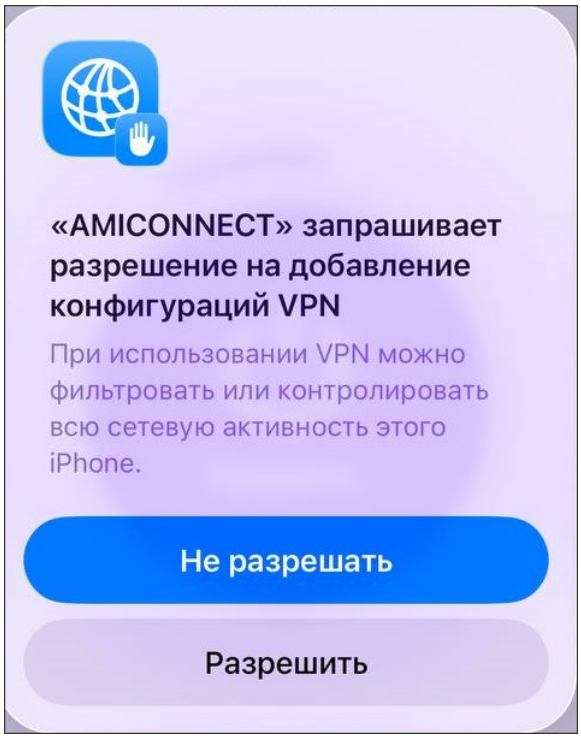

Рисунок 26 – Уведомление о разрешении настройки

Пользователь будет перемещён в окно системных настроек, в раздел

VPN-конфигураций. Если на устройстве установлен пароль, пользователю будет предложено ввести пароль и подтвердить тем самым свою личность и право внесения изменений в настройки.

После введения пароль пользователь снова будет перенаправлен в приложение Клиент АМИКОННЕКТ. В процессе подключения пользователю будет предложено ввести имя и пароль аутентификации одним из выбранных в настройке способов двухфакторной аутентификации.

При верно введённых данных и корректной настройке профиля состоится подключение к ФПСУ. Пользователь будет перенаправлен на главное окно приложения, в котором можно будет увидеть индикацию подключения зелёного цвета и надпись «Подключено» рядом с ним.

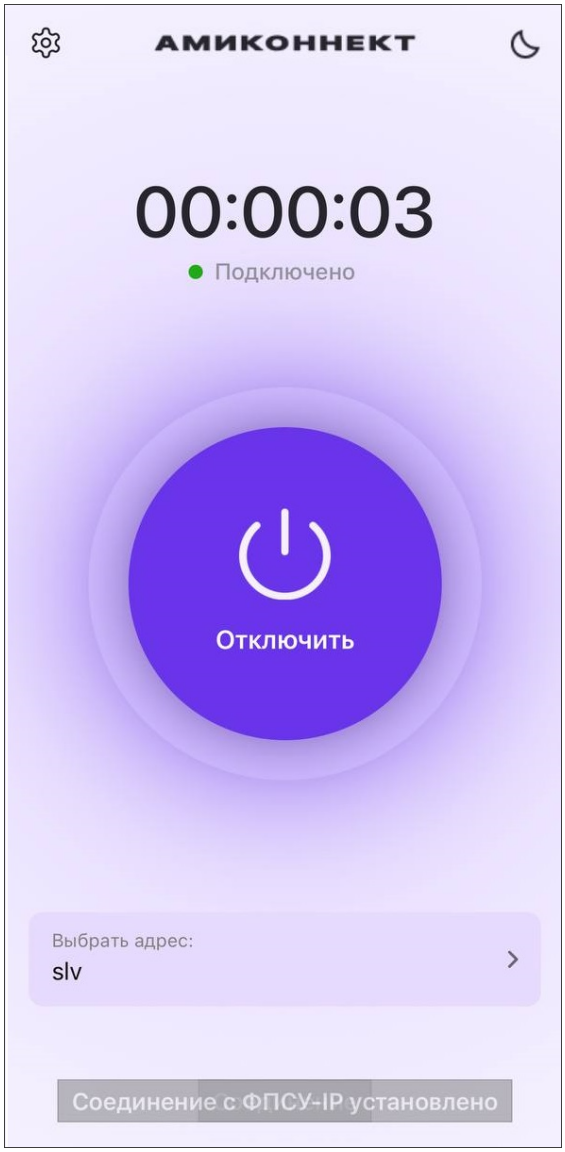

Рисунок 27 – Состояние «Подключено» на главном экране приложения

6. Сообщения об ошибках при соединении с ФПСУ

При ошибках соединения АМИКОННЕКТ с ФПСУ могут быть выданы указанные в файле со списком ошибок сообщения.