ООО «АМИКОН»

УТВЕРЖДЕН

РОФ.ПЕРС.00123-01 32-ЛУ

АМИКОННЕКТ
(для Android)

Руководство администратора

РОФ.ПЕРС.00123-01 32

Листов 18

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 Android. 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) 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 клиентом PKI частями организуется защищенное VPN-соединение, через которое могут передаваться данные L3-L7 уровня OSI.

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

VPN-протокол не чувствителен 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 информационными ресурсами реализована с применением технологий, облегчающих конфигурирование и управление сетевыми настройками клиентов, на ФПСУ-IP устанавливаются минимальные настройки клиентов PKI. Дополнительное (после первоначально аутентификации на ФПСУ-IP) решение по доступу клиента PKI к защищаемой сети может быть принято с помощью внешних по отношению к ФПСУ-IP сервисами RADIUS, DHCP, OCSP, Compliance (интеграция с Комплексом информационной безопасности САКУРА разработки компании «ИТ-Экспертиза»).

Система использует клиент-серверную архитектуру, предусматривающую наличие:

- VPN-клиента;

- VPN-сервера;
- Compliance-клиента;
- Compliance-сервера.

Данное решение может быть внедрено как в действующую систему с инфраструктурой PKI так и при развертывании новой.

Схема взаимодействия клиента PKI и ФПСУ-IP определяет, что пользователь клиента PKI получает от удостоверяющего центра сертификации (далее - УЦ) закрытый ключ и сертификат открытого ключа и устанавливает закрытый ключ и сертификат 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. Если статус сертификата действующий, клиент PKI авторизуется в защищенной сети.

Клиент PKI для Android использует штатные хранилище операционной системы при взаимодействии с локальными сертификатами.

При подключении клиента PKI может быть включена дополнительная проверка устройства. Идентификация устройства клиента PKI реализуется совместно с Compliance-модулем (Комплексом информационной безопасности САКУРА) по MAC-адресу сетевого адаптера, через который осуществляется подключение клиента PKI к ФПСУ-IP.

В зависимости от настроек NAT клиент PKI авторизуется с реальным IP адресом или IP адресом, полученным от настроенного DHCP-сервера.

Место хранения сертификатов при работе с клиентом PKI в ОС Android

реализовано с использованием штатного хранилища операционной системы.

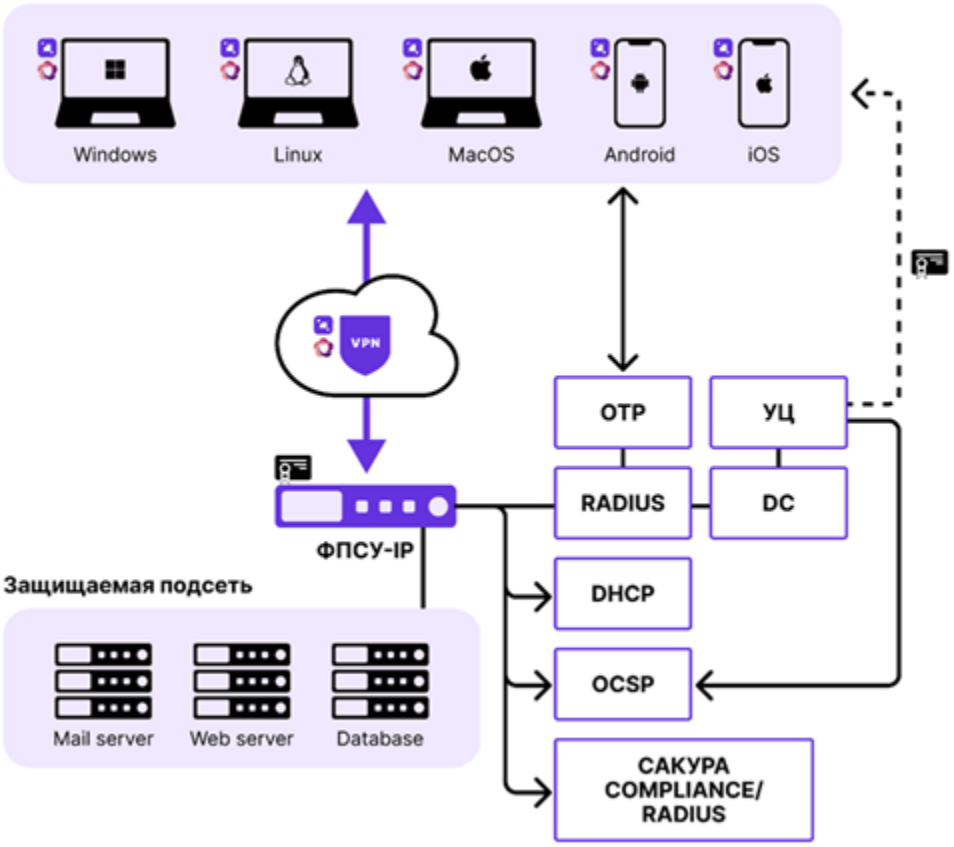

Рисунок 1 - Общая схема применения

3. Инсталляция АМИКОННЕКТ

Клиент устанавливается на мобильное устройство под управлением ОС Android, подключенное к IP-сети передачи данных, которая обеспечивает доставку пакетов до ФПСУ с установленной подсистемой «PKI-Клиенты».

Для установки актуальной версии приложения АМИКОННЕКТ необходимо зайти с мобильного телефона, подключенного к сети интернет, в магазин приложений RuStore и в поисковой строке написать название приложения – «АМИКОННЕКТ». В результатах поиска появится приложение. Далее необходимо выполнить следующие действия:

- пройти на страницу мобильного приложения;
- убедиться, что издателем является компания «АМИКОН» и инициировать загрузку приложения на мобильный телефон.

4. Запуск, настройка и удаление АМИКОННЕКТ

При первом запуске приложения администратору необходимо загрузить сертификаты: корневой CA в формате .cer и личный из одной цепочки доверия в формате .pfx. Это необходимо для установки будущего соединения с центральным компонентом ПАК ФПСУ.

Рисунок 2 – Главное окно

4. 1. Установка сертификатов

На главном экране приложения необходимо найти значок Настройки (шестерёнка в верхнем правом углу); после нажатия на значок откроется окно настроек.

В настройках можно увидеть строки «Сертификат» для загрузки личного сертификата и строку «Корневой сертификат» для загрузки корневого сертификата.

Доступ в хранилище будет открыт, только в том случае, если на устройстве установлен пароль. В противном случае на экране устройства появится уведомление с просьбой обеспечить на устройстве аутентификацию.

Для ручной загрузки сертификатов необходимо нажать на строку корневого или личного сертификата.

Для загрузки корневого сертификата (.cer) из системного хранилища нужно заранее установить его в хранилище доверенных сертификатов устройства. Примерный путь (для Android ver.16): Дополнительные настройки – Шифрование и учетные данные – Установка сертификатов – Сертификат центра сертификации.

Если сертификаты не были установлены в системное хранилище, при загрузке необходимо выбрать пункт «Из файла». В этом случае откроется папка загруженных файлов. В ней необходимо найти соответствующие для каждого пункта («Сертификат» и «Корневые сертификаты») сертификаты и загрузить их в приложение АМИКОННЕКТ.

Для установки личного сертификата может понадобиться пароль, установленный на него при генерации сертификата.

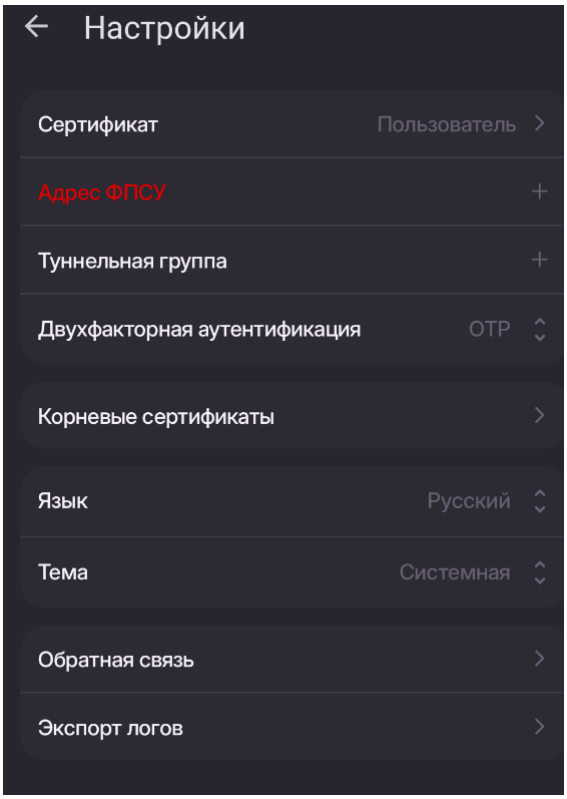

Рисунок 3 – Окно настроек

4. 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.

4. 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.

4. 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.**

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. 5. Удаление VPN-профиля

При необходимости VPN-профиль (профиль пользователя) может быть удален. Чтобы удалить VPN-профиль, необходимо удалить личный сертификат в настройках. После удаления личного сертификата автоматически удалятся привязанные к нему: адрес подключения, имя туннельной группы и настройка аутентификации. Корневой сертификат останется в настройках. При необходимости его можно удалить отдельно.

4. 6. Удаление приложения АМИКОННЕКТ

Удаление приложения АМИКОННЕКТ производится обычным способом. Удалить его можно через настройки: Настройки – Приложения – Показать все приложения.

Далее в списке приложений необходимо найти приложение АМИКОННЕКТ, пройти в настройки приложения и нажать на кнопку «Удалить». Приложение будет удалено.

При удалении приложения, 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 конфигурацию.

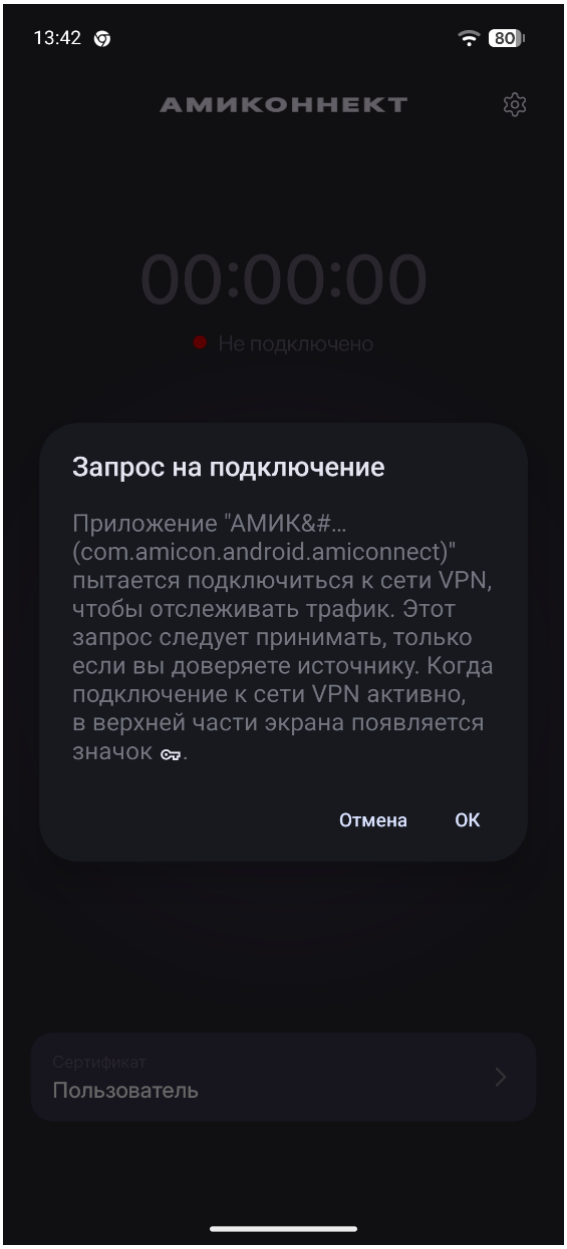

Рисунок 4 – Уведомление о разрешении настройки

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. На главном экране подключения можно будет увидеть индикацию подключения и надпись «Подключено» рядом с ним.

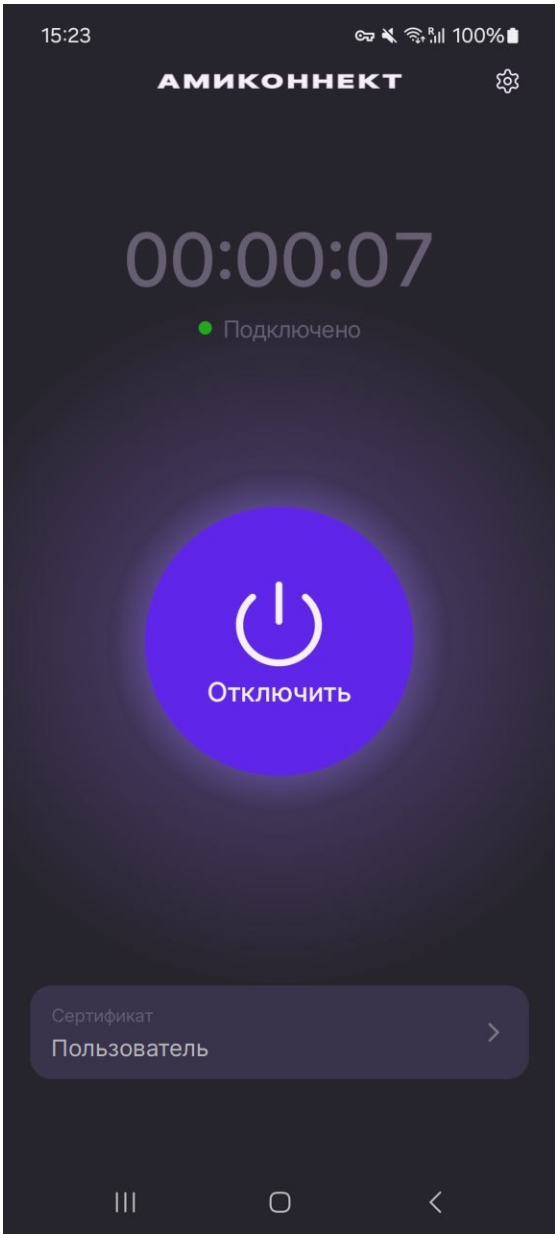

Рисунок 5 – Состояние «Подключено» на главном экране приложения