ООО «АМИКОН»

УТВЕРЖДЕН

РОФ.ПЕРС.00122-01 32-ЛУ

АМИКОННЕКТ
(для macOS)

Руководство администратора

РОФ.ПЕРС.00122-01 32

Листов 53

2026

Аннотация

Настоящее руководство предназначено для администраторов систем защищенного удаленного доступа к корпоративной сети на основе Амиконнект и ФПСУ, работающих на ПЭВМ в операционных системах macOS. 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 и Амиконнектом организуется защищенное VPN-соединение, через которое могут передаваться данные L3-L7 уровня OSI.

Взаимная двухсторонняя аутентификация клиентов Амиконнект и ФПСУ производится с использованием сертификата открытого ключа пользователя и собственного сертификата ФПСУ. Пользователь Амиконнекта идентифицируется реквизитами своего сертификата. На ФПСУ 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. Амиконнект поддерживает работу на каналах связи с задержками более 300 мс.

Организация VPN-соединения между Амиконнектом и ФПСУ для доступа к информационным ресурсам реализована с применением технологий, облегчающих конфигурирование и управление сетевыми настройками клиентов, на ФПСУ устанавливаются минимальные настройки. Дополнительное (после первоначально аутентификации на ФПСУ) решение по доступу к защищаемой сети может быть принято с помощью внешних по отношению к ФПСУ 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 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 Амиконнект. На ФПСУ должны быть загружены ключевая пара – закрытый ключ и собственный сертификат самого ФПСУ, а также сертификаты Удостоверяющих центров, выдавших клиентские сертификаты Амиконнект. При подключении Амиконнекта к защищенной сети ФПСУ 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 Амиконнект авторизуется в защищенной сети.

Амиконнект для macOS использует штатные хранилище операционной системы при взаимодействии с локальными сертификатами.

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

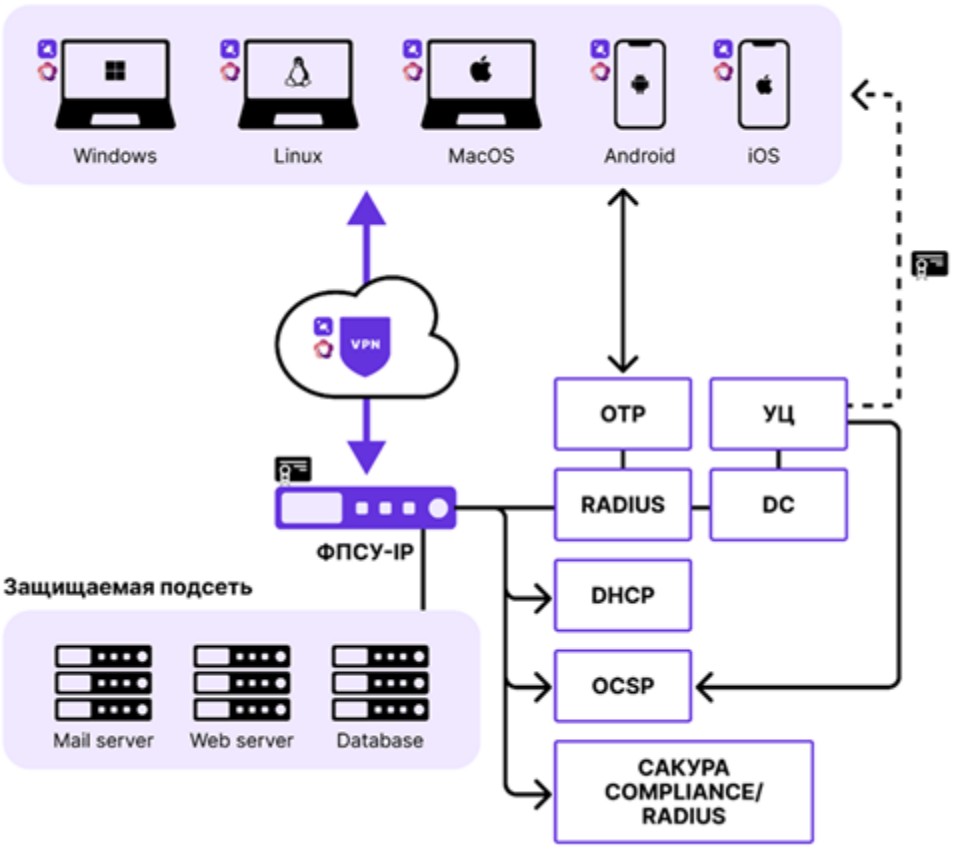

Рисунок 1 - Общая схема применения

3. Инсталляция Амиконнект

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

- операционная система MacOS версия 13.x или выше;
- аппаратные требования: в соответствии с требованиями операционной системы.

Все скриншоты и примеры в данном документе приводятся для macOS версии 15. При установке и использовании ПО в иных операционных системах во внешнем виде интерфейса, последовательности действий при установке могут наблюдаться отличия от приведенных примеров.

Для установки Амиконнект на ПК под управлением операционной системы macOS версии 15 необходимо:

1. Открыть пакет «AMICONNECT_X_X_MAC.dmg» с клиентом. Выбрать amiconnect.pkg:

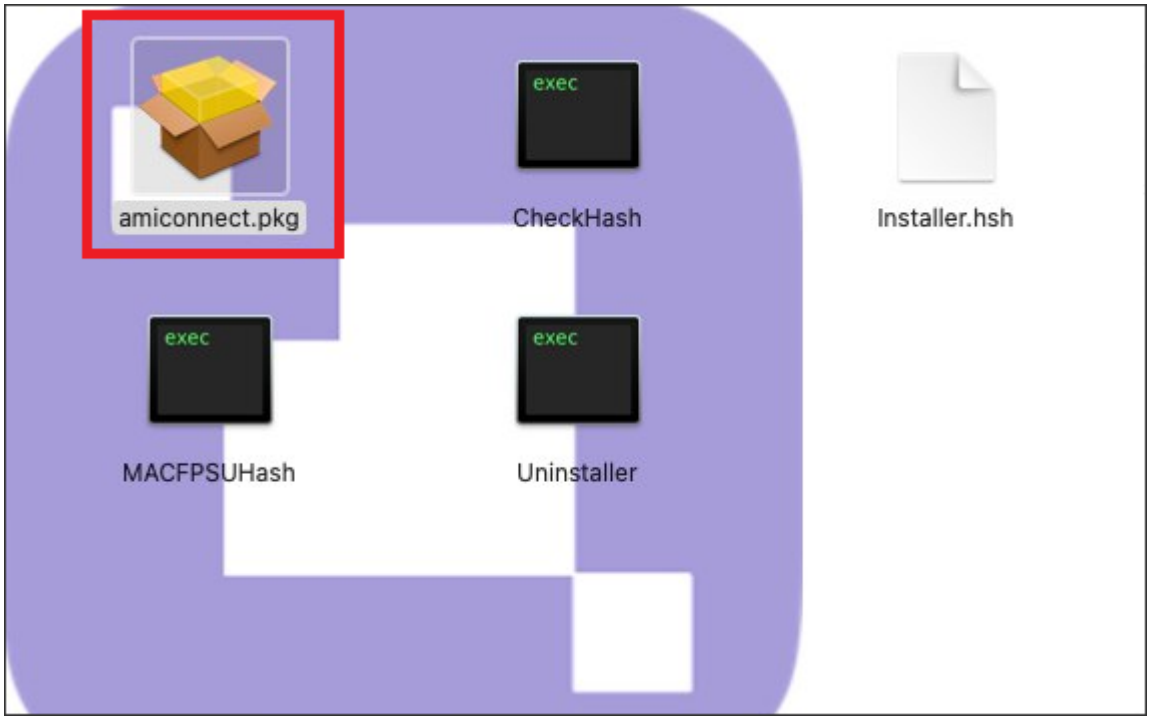

Рисунок 2 – Выбор файла для запуска

2. Система может выдать предупреждение о невозможности открытия файла:

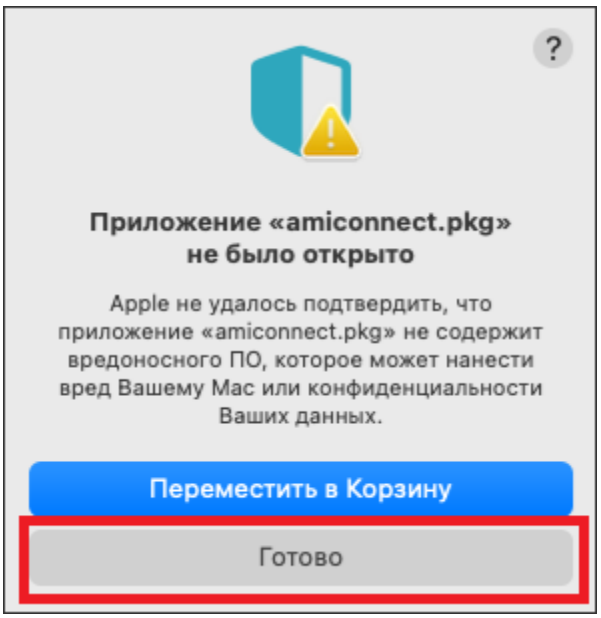

Рисунок 3 – Предупреждение о невозможности открыть файл

Дальнейшие действия по установке ПО на разные версии операционных систем могут отличаться. В данном руководстве представлено описание инсталляции Амиконнект на ПК под управлением macOS версии. Если уведомление о невозможности установки появилось, то необходимо выполнить шаги, описанные ниже, а именно:

- Выбрать «Готово»:

- Перейти в раздел настроек «Конфиденциальность и безопасность» и в самом низу страницы выбрать «Все равно открыть» для файла «amiconnect.pkg»:

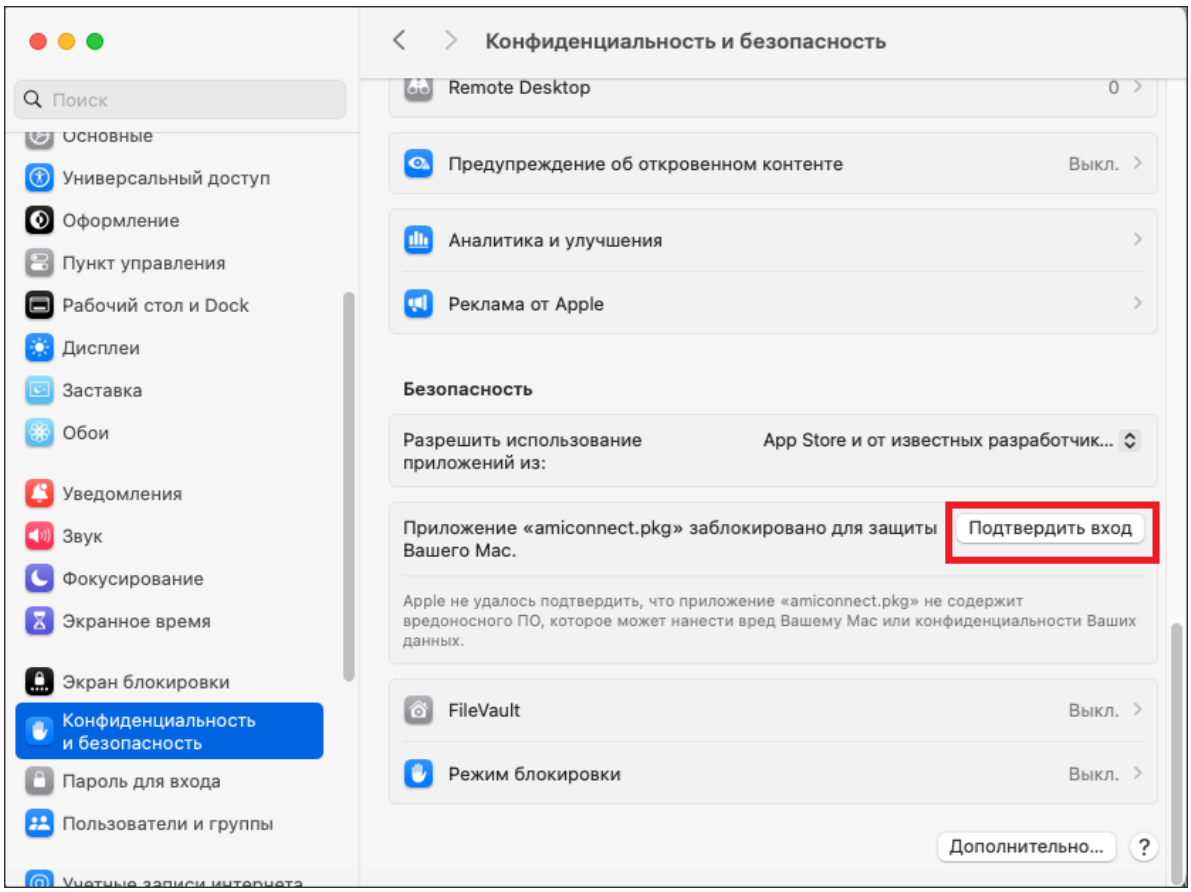

Рисунок 4 – Раздел «Конфиденциальность и безопасность»

- В открывшемся окне выбрать «Открыть все равно»:

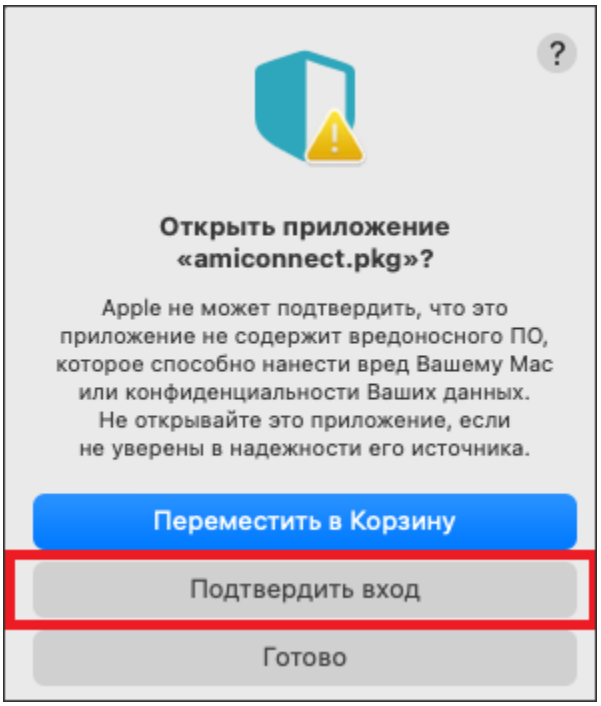

Рисунок 5 – Окно запроса разрешения на открытие файла

- Ввести пароль от учетной записи и подтвердить его ввод нажатием кнопки «ОК»:

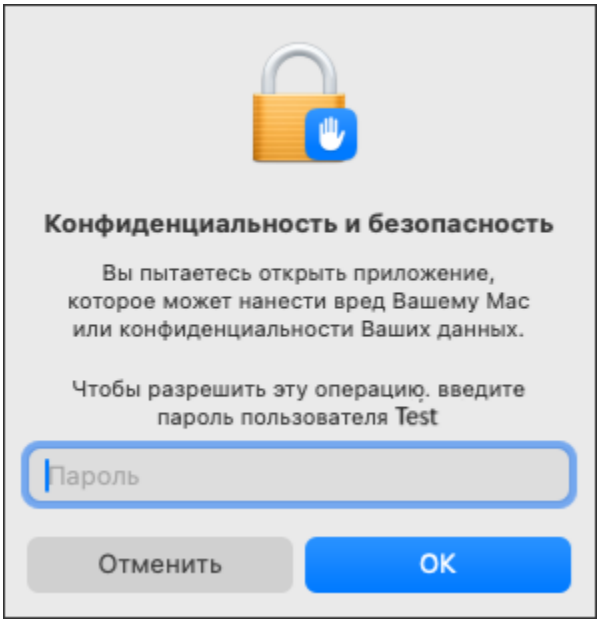

Рисунок 6 – Окно ввода пароля

3. Далее (и в том случае, если описанные выше шаги не потребовались) следует пройти все этапы инсталляции в обычном порядке, а именно:

- Дистрибутив поставляется в пакете «AMICONNECT_X_X_MAC.dmg». После открытия пакета необходимо запустить «amiconnect.pkg». Откроется приветственное окно мастера установки, в котором необходимо нажать кнопку «Продолжить».

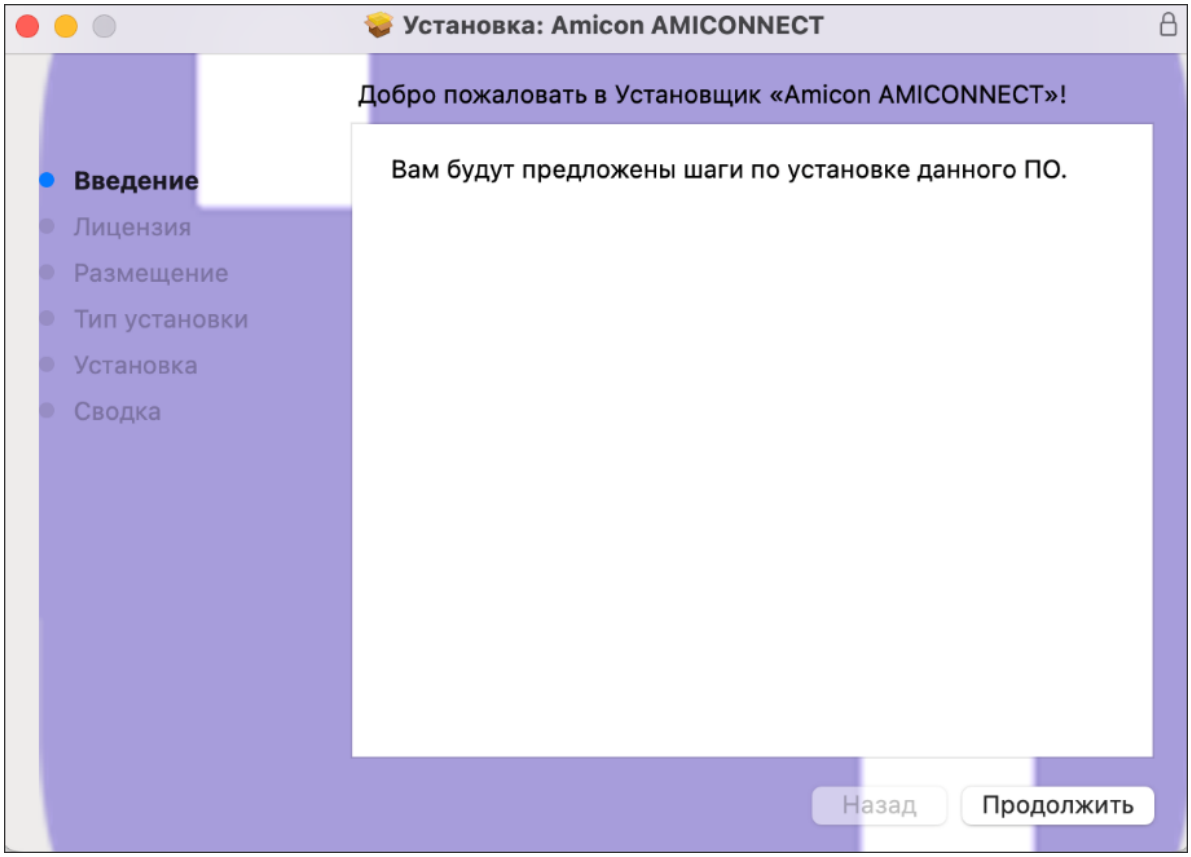

Рисунок 7 – Начало установки

Программа установки выдаст на экран лицензионное соглашение между пользователем Амиконнект и ООО «АМИКОН». Для прочтения условий соглашения необходимо нажать кнопку «Продолжить», в противном случае отказаться от инсталляции при помощи кнопки «Назад».

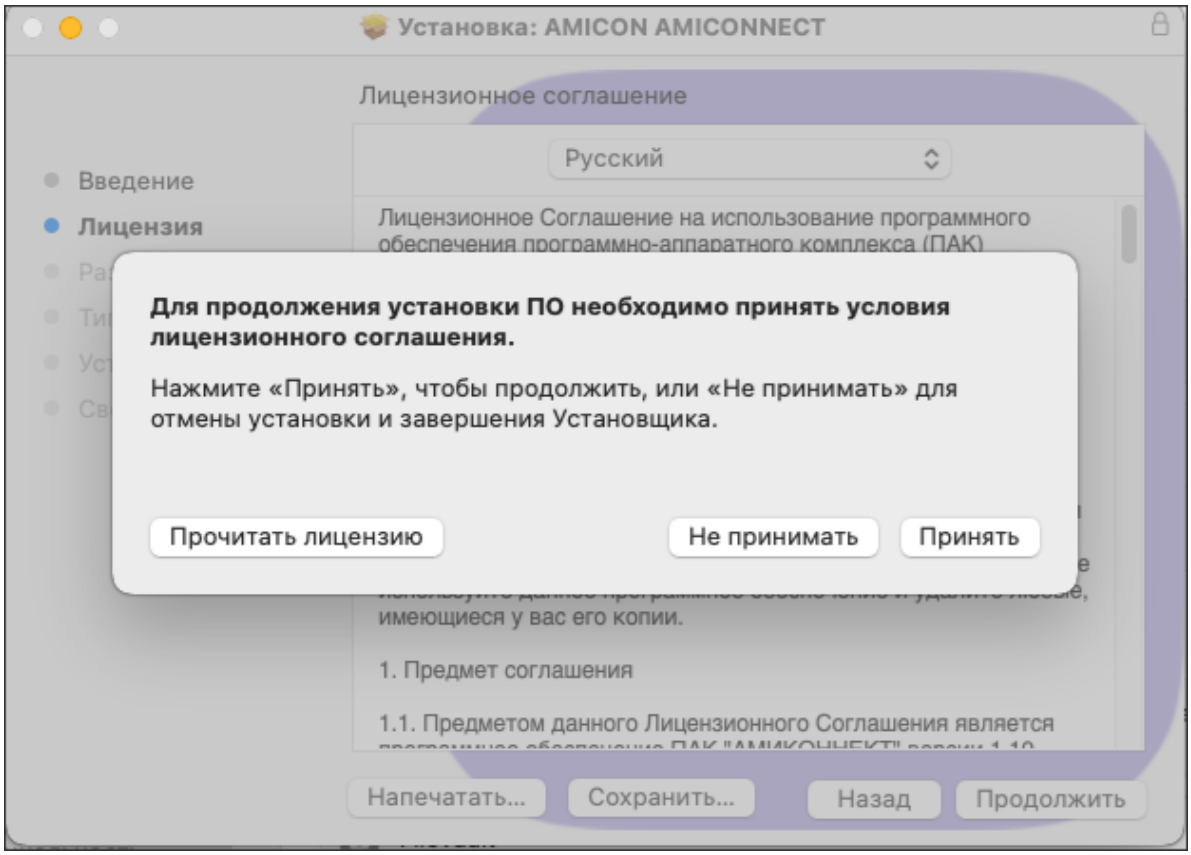

Рисунок 8 – Лицензионное соглашение

- На экране лицензионного соглашения необходимо нажать кнопку «Продолжить», после чего программа выдаст сообщение для принятия соглашения.

После нажатия кнопки «Принять» программа установки выведет информационное окно выбора варианта установки ПО:

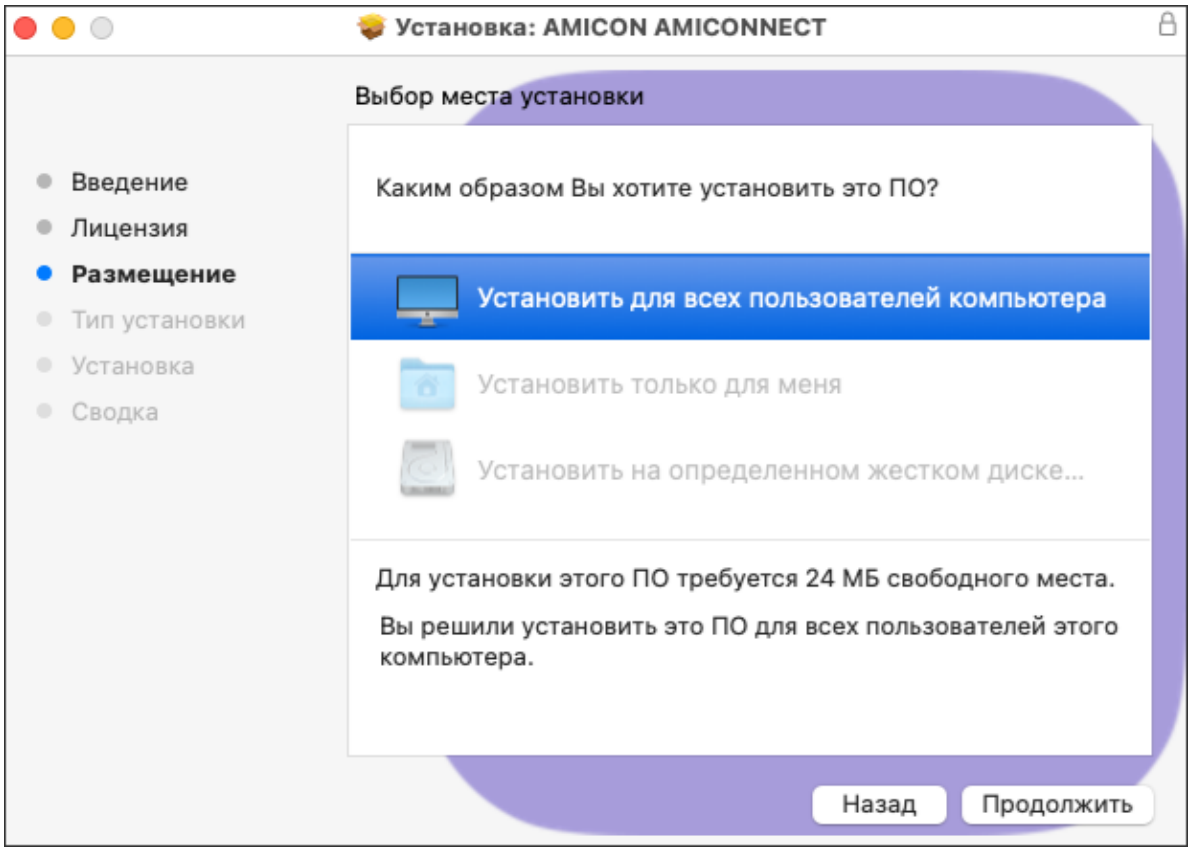

Рисунок 9 – Окно выбора места установки

В открывшемся окне «Выборочная установка на macXXX» необходимо подтвердить действие так же нажатием кнопки «Продолжить»:

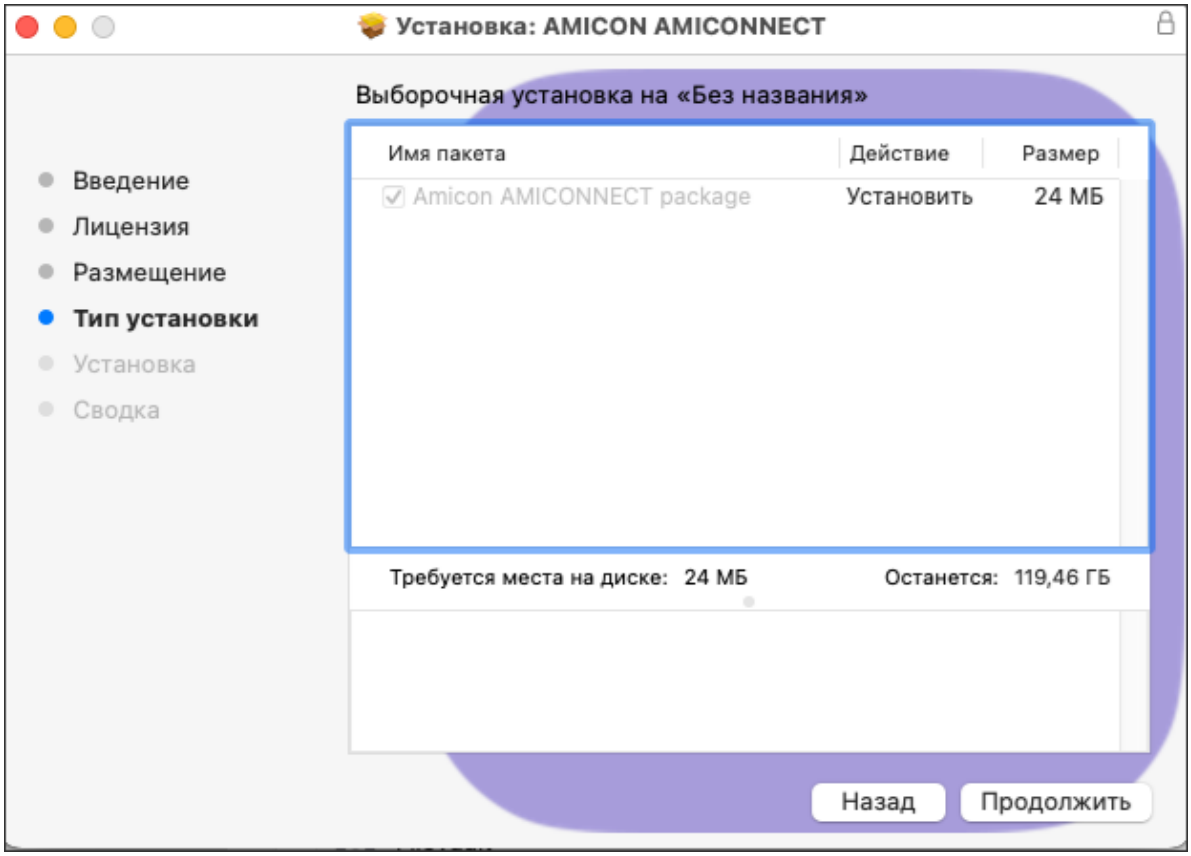

Рисунок 10 – Сообщение о стандартном типе установки

В открывшемся окне, при необходимости, предоставляется возможность изменить каталог установки (нажатием кнопки «Изменить размещение установки...» и выбором необходимого каталога):

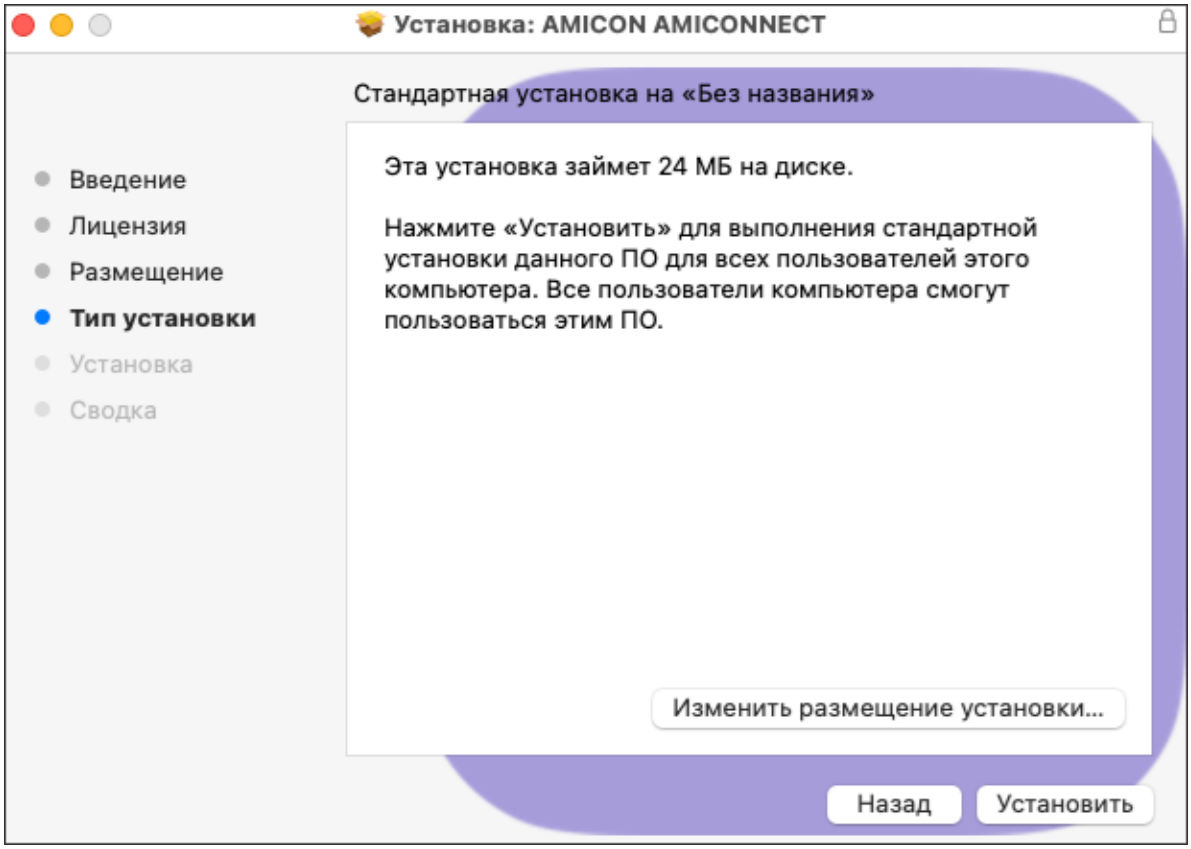

Рисунок 11 – Изменение каталога установки (при необходимости)

Подтверждение выбора каталога установки происходит нажатием кнопки «Установить».

- В открывшемся по кнопке «Установить» окне аутентификации необходимо ввести пароль и нажать кнопку «Установить ПО»:

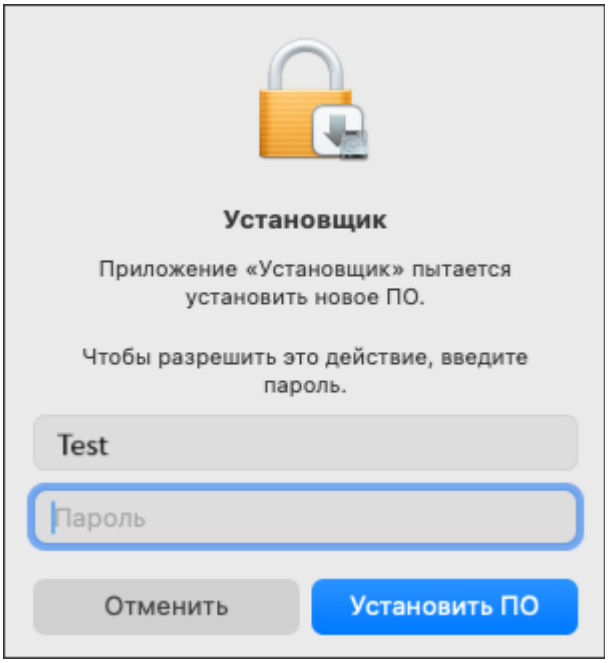

Рисунок 12 – Окно ввода пароля для разрешения установки ПО

Мастер установит файлы ПО Амиконнект, по завершении выдав информационное окно «Установка была успешно завершена»:

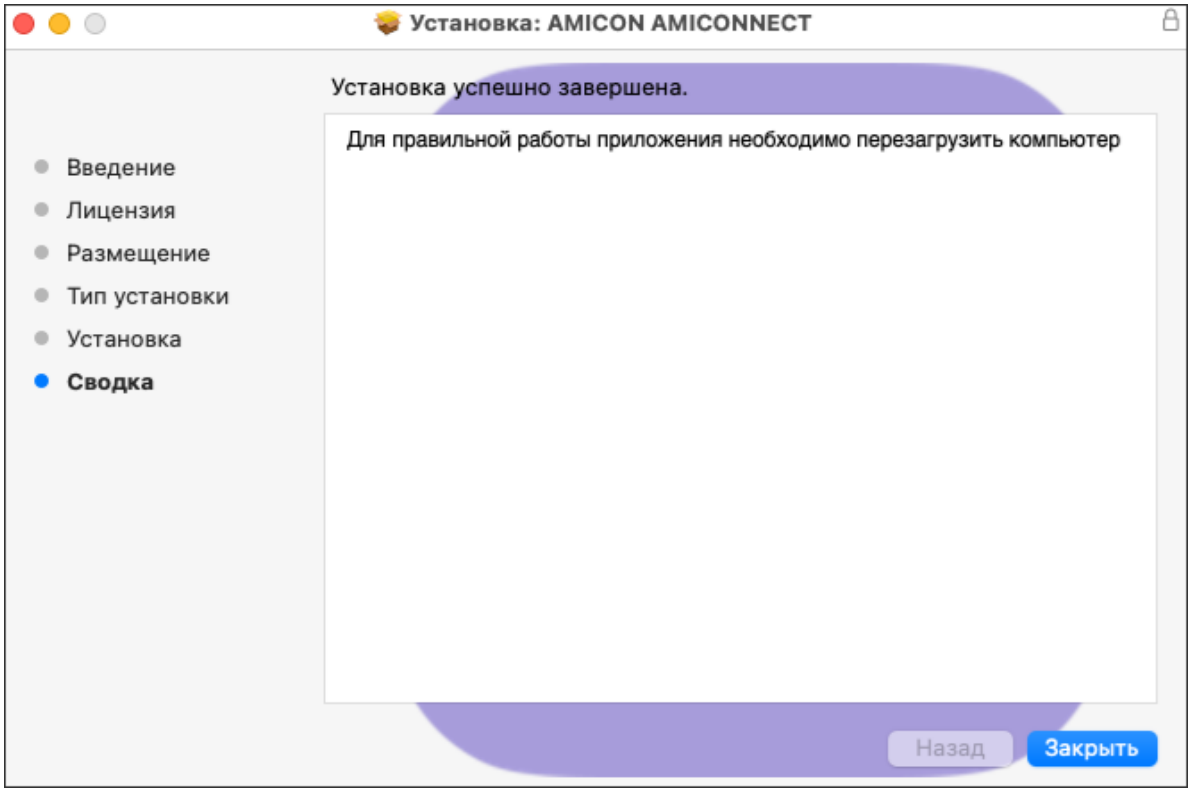

Рисунок 13– Завершение установки

Для завершения процесса следует нажать кнопку «Закрыть». Перед дальнейшим использованием Амиконнект необходимо перезагрузить компьютер.

После перезагрузки следует выполнить действия по предоставлению разрешений приложениям (см. п. Особые требования к установке Амиконнект на ПК под управлением macOS 15).

3. 1. Особые требования к установке АМИКОННЕКТ на ПК под управлением macOS 15

После регистрации и входа пользователя в операционную систему после

перезагрузки для корректной работы с Амиконнект требуется дать разрешение на работу Амиконнект и разрешение на инспекцию трафика, а именно:

- В открывшемся после перезапуска уведомлении о запросе на использование системного расширения нажать кнопку «Открыть Системные настройки»:

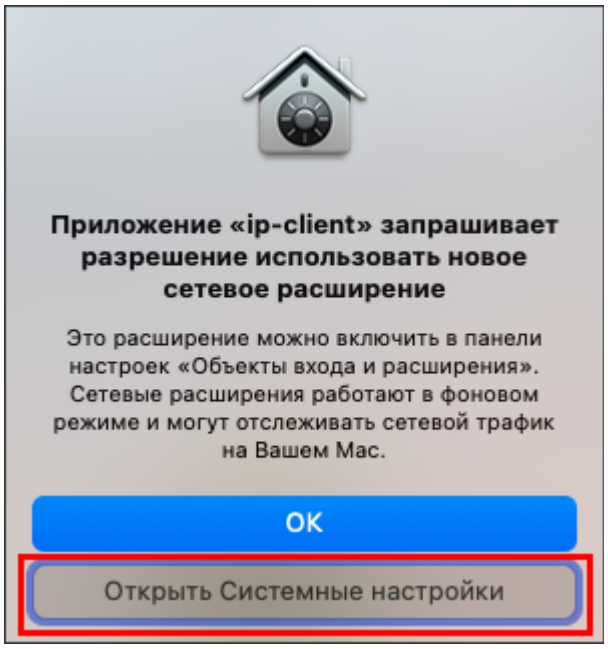

Рисунок 14 – Запрос разрешения на использование нового расширения

- Далее необходимо войти в систему и открыть пункт «Настройки Основные Объекты входа и расширения»:

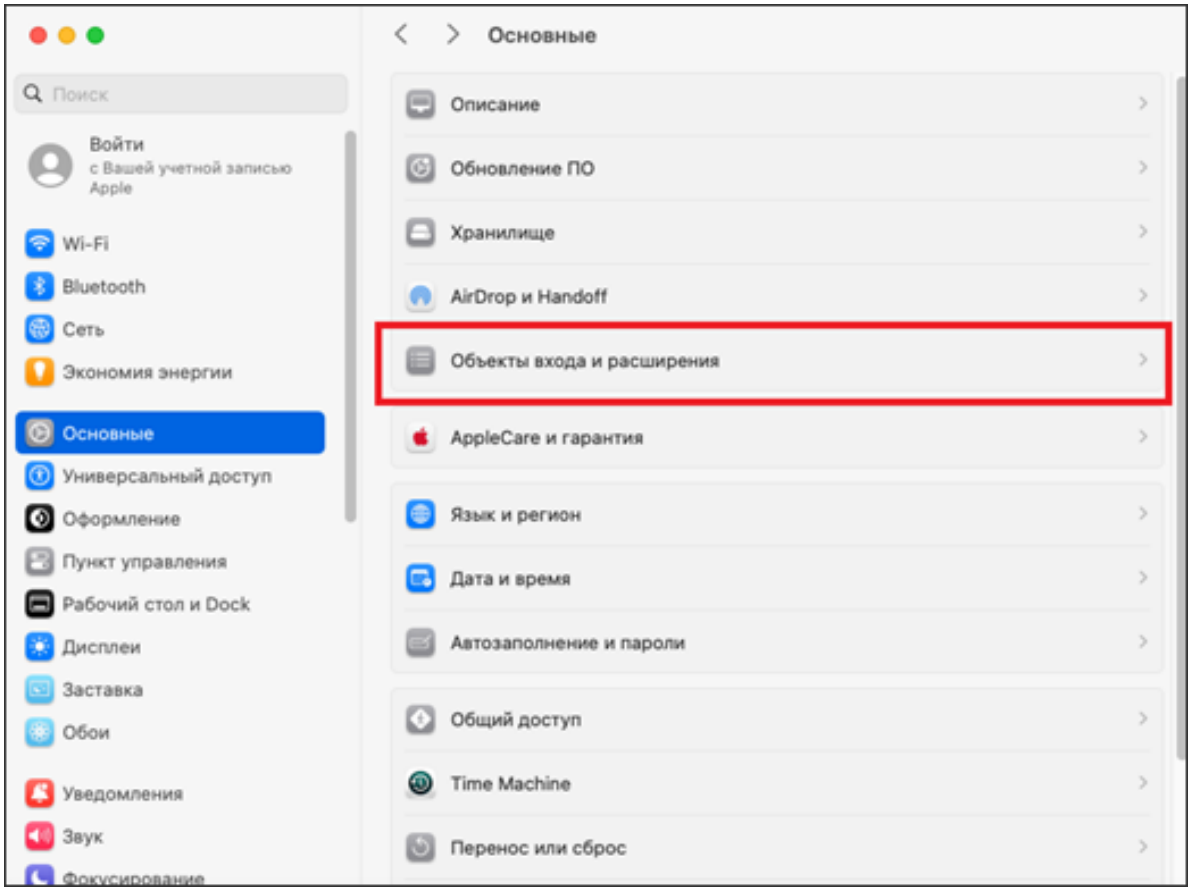

Рисунок 15 – Окно основных настроек ОС

- Далее необходимо нажать на знак «i», расположенный справа от пункта «Сетевые расширения»:

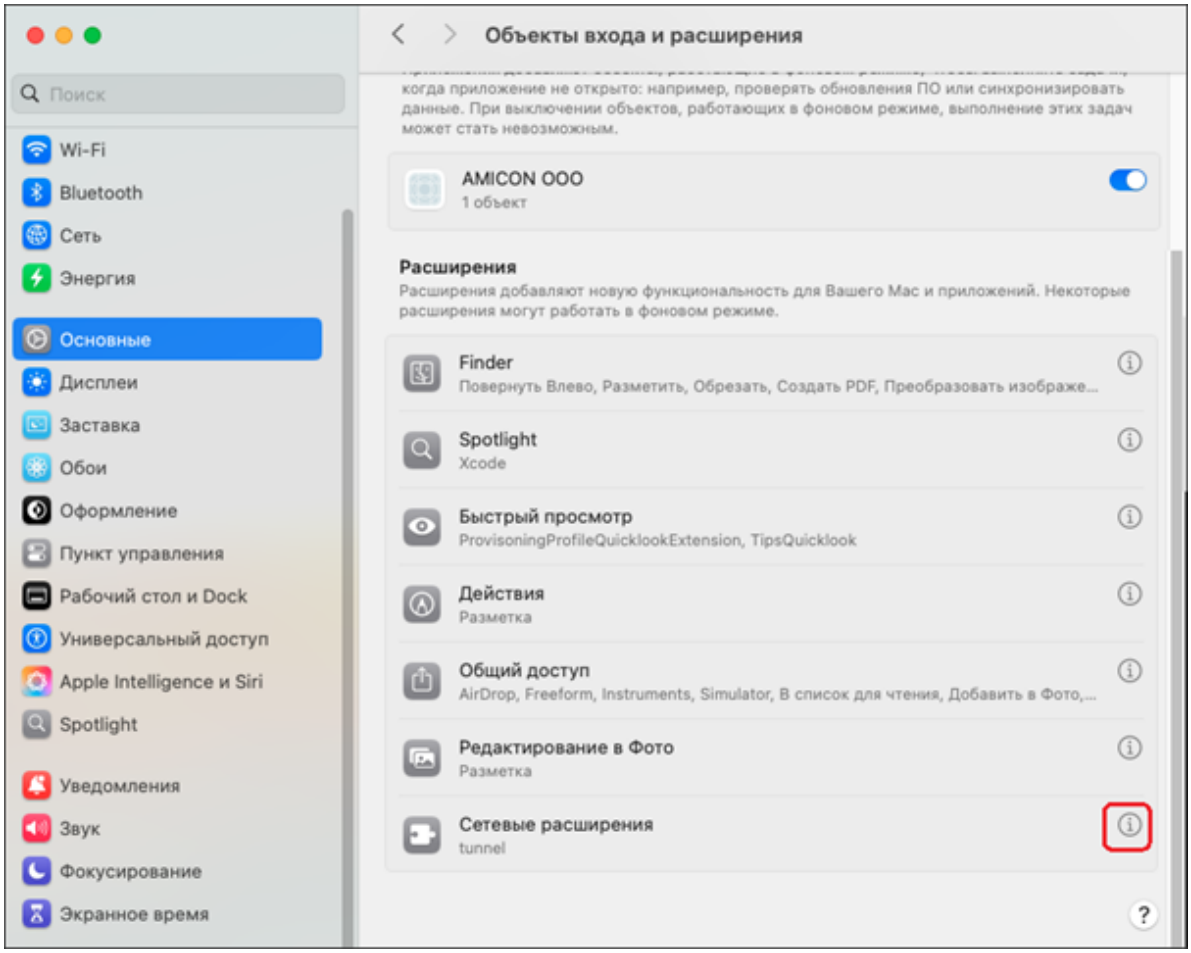

Рисунок 16 – Окно настройки объектов входа и расширения

- В открывшемся окне необходимо установить переключатель для пункта «tunnel» в положение «Вкл» (перевести бегунок вправо):

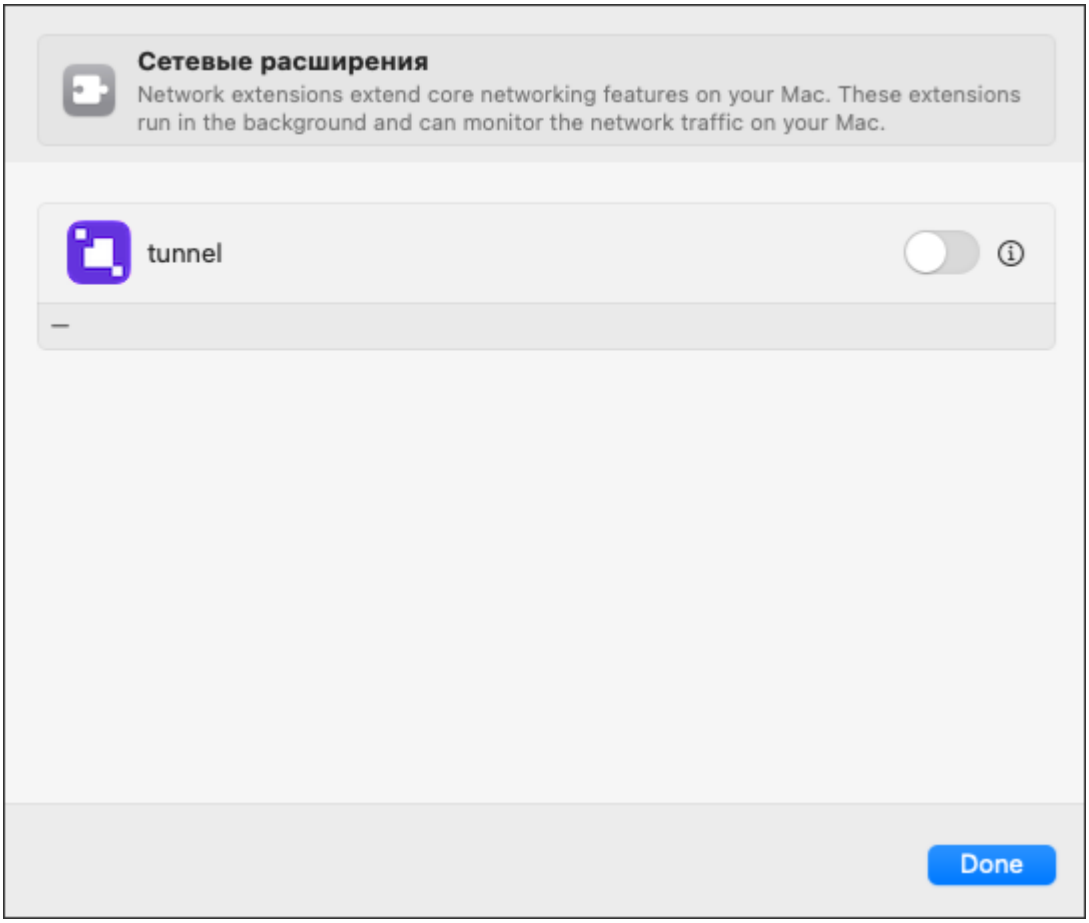

Рисунок 17 – Разрешение на работу с сетевым расширением

- После этого на экран будет выведено окно, в котором следует ввести пароль от учетной записи и подтвердить его ввод нажатием кнопки «ОК»:

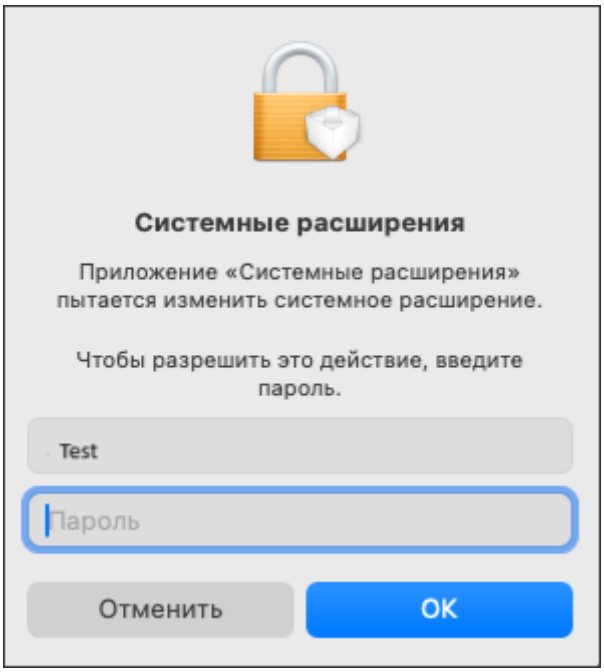

Рисунок 18 – Ввод пароля для разрешения работы с сетевым расширением

- Далее для корректной работы программы необходимо дать разрешение на фильтрацию сетевого траффика нажатием кнопки «Разрешить»:

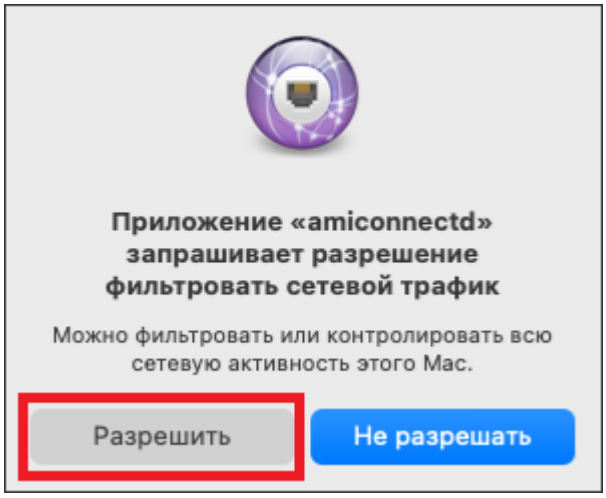

Рисунок 19 – Разрешение на фильтрацию сетевого трафика

- Переключатель будет переведен в положение «Вкл.»; для завершения процесса в нижней части окна необходимо нажать кнопку «Готово»:

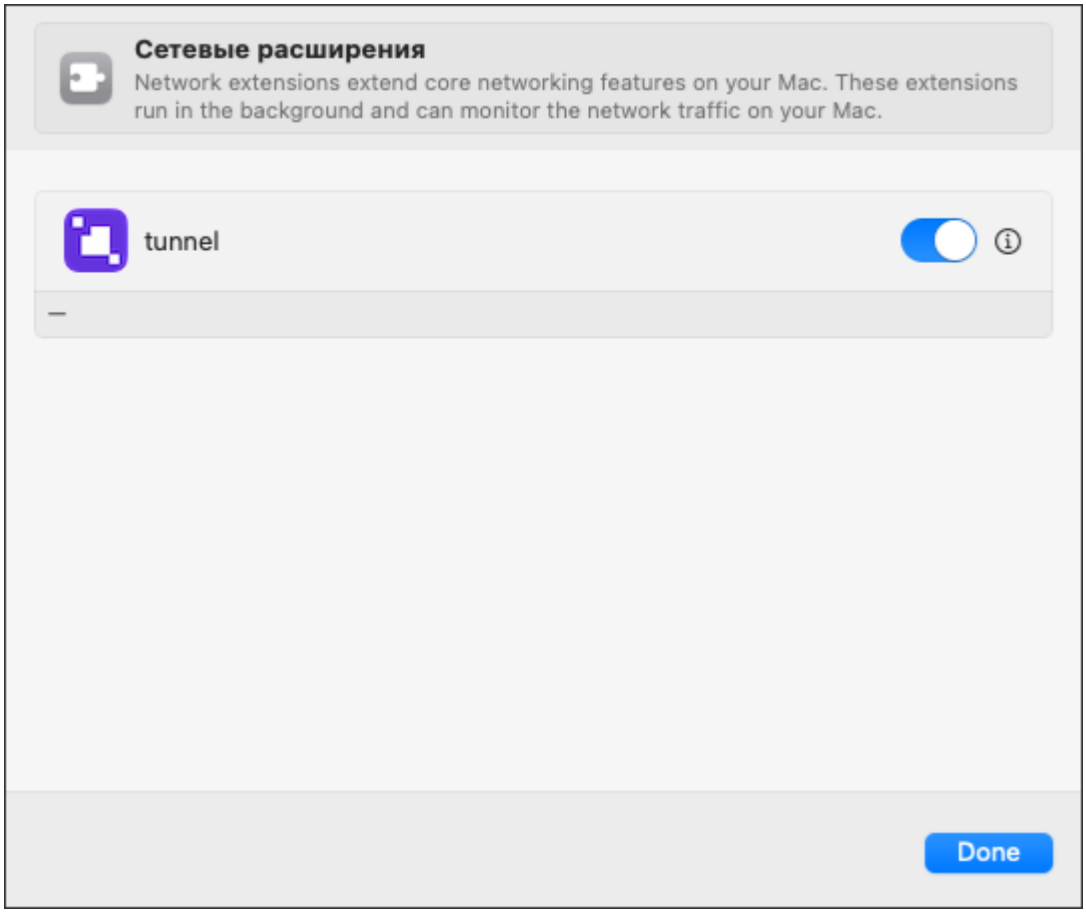

Рисунок 20 – Использование расширения включено

После перезагрузки ОС Амиконнект будет активирован.

4. Установка сертификатов

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

4. 1. Установка корневого сертификата

Откройте размещение сертификата:

- Выберите необходимый корневой сертификат и нажмите на него 2 раза.
- Следующим шагом будет предложение добавить сертификат в одну из областей «Связки ключей». Необходимо выбрать – Систему и нажать «Добавить». После ввести пароль от учетной записи. Сертификат загрузится на рабочую станцию.
- Пройдите в приложение Связка ключей и выберите загруженный сертификат.
- В настройках сертификата выберите вкладку Доверие и в пункте Параметры использования сертификата выберите «Всегда доверять».
- Подтвердите свои полномочия вводом пароля администратора.

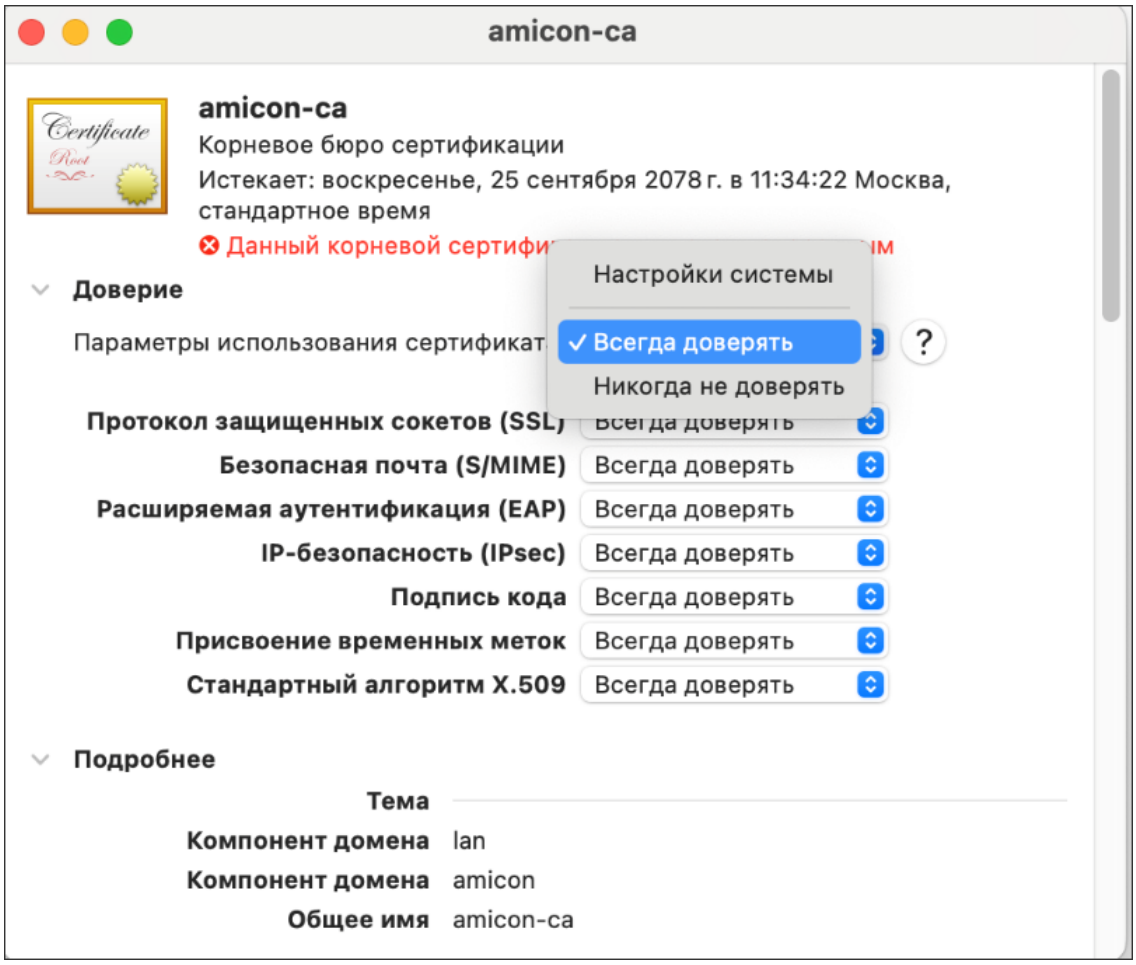

Рисунок 21 – Окно установки корневого сертификата

4. 2. Установка пользовательского сертификата

Откройте размещение сертификата:

- Выберите необходимый сертификат пользователя и нажмите на него 2 раза.

- Введите пароль, установленный при генерации сертификата. Для подтверждения прав также необходимо подтвердить свои действия вводом пароля администратора. После сертификат загрузится на рабочую станцию.

- Пройдите в приложение Связка ключей и выберите загруженный сертификат.

- В настройках сертификата выберите вкладку Доверие и в пункте Параметры использования сертификата выберите «Всегда доверять».

- Подтвердите свои полномочия вводом пароля администратора.

После установки сертификатов убедитесь, 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.

5. Установка VPN-соединения с ФПСУ

5. 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.

5. 2. Соединение через окно подключения

Соединение с ФПСУ также можно осуществить через специальное окно подключения. Чтобы вызвать окно подключения необходимо дважды нажать мышью значок 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.

6. 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:

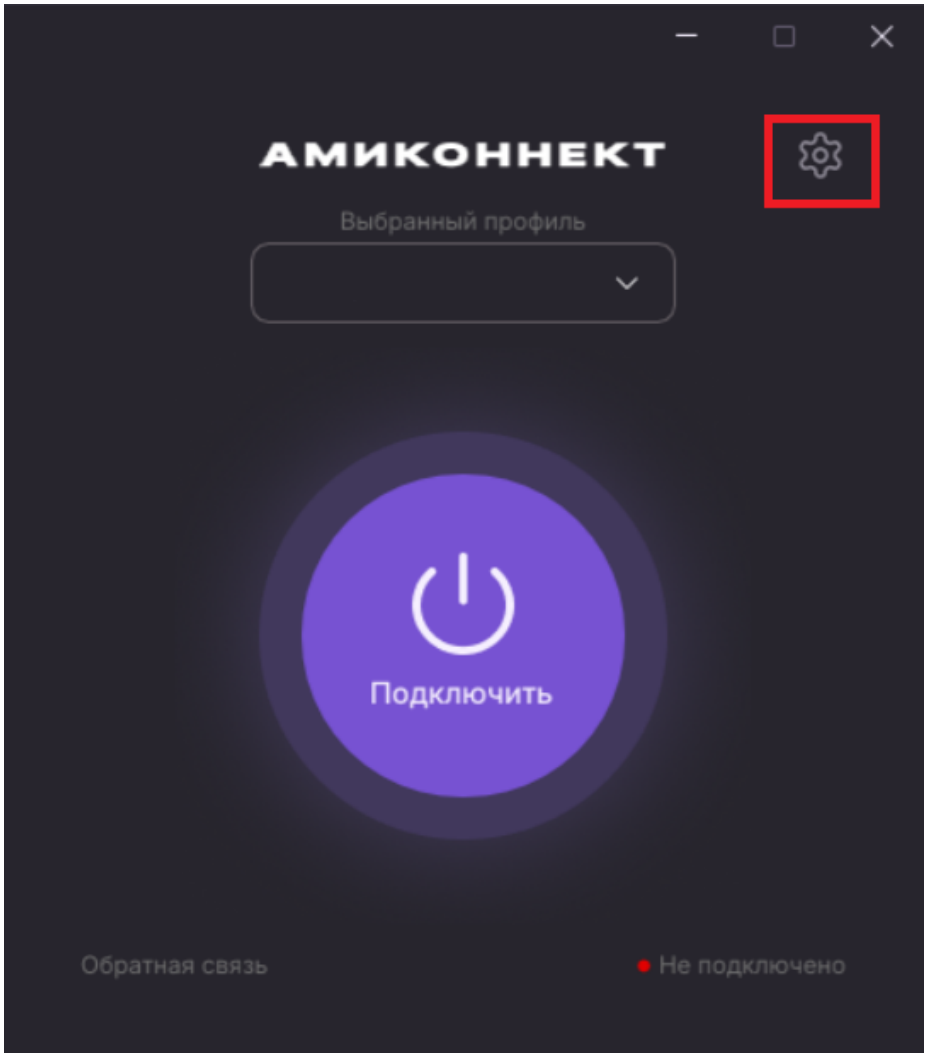

Рисунок 22 – Значок настроек

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.

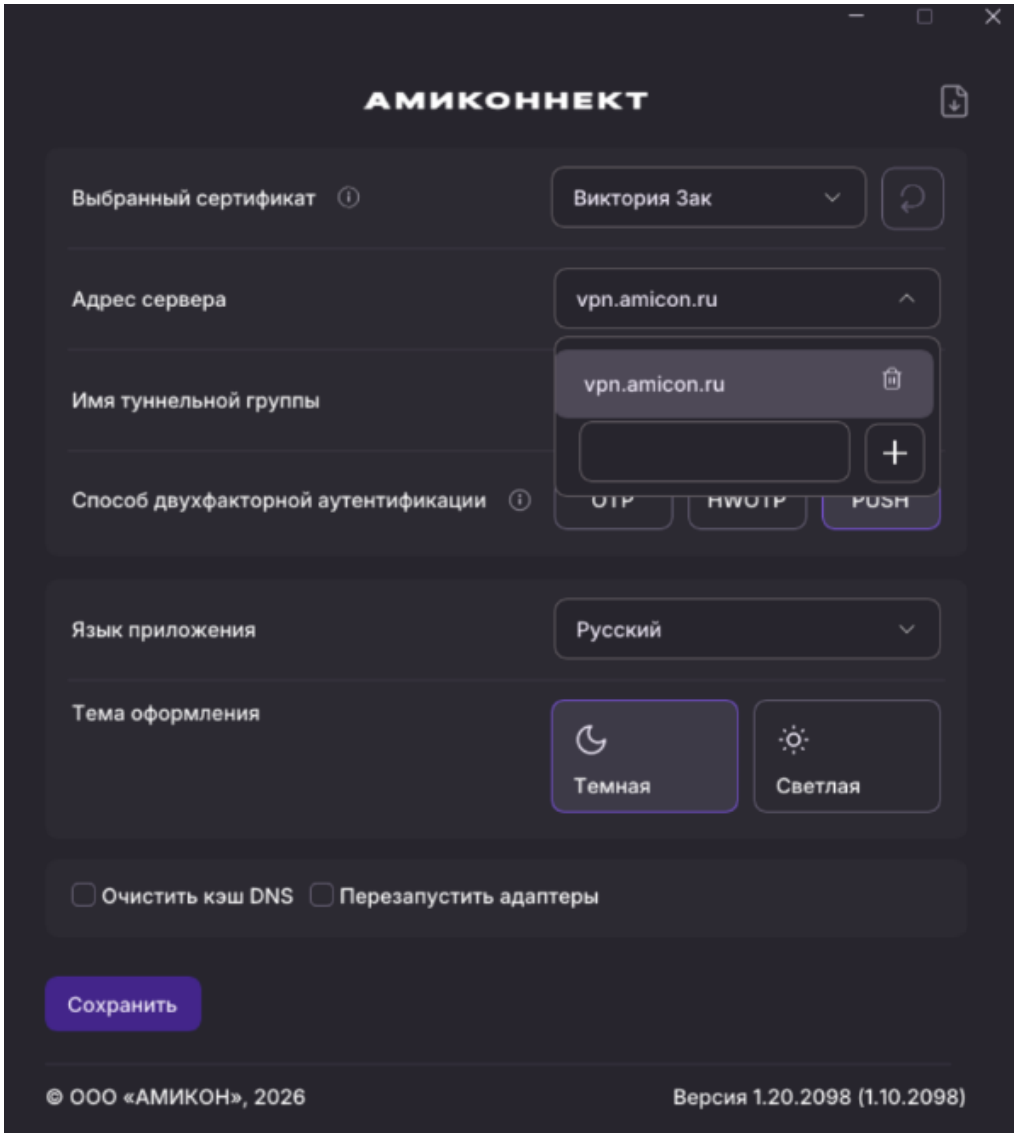

Рисунок 23 – Настройки Амиконнект

6. 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:

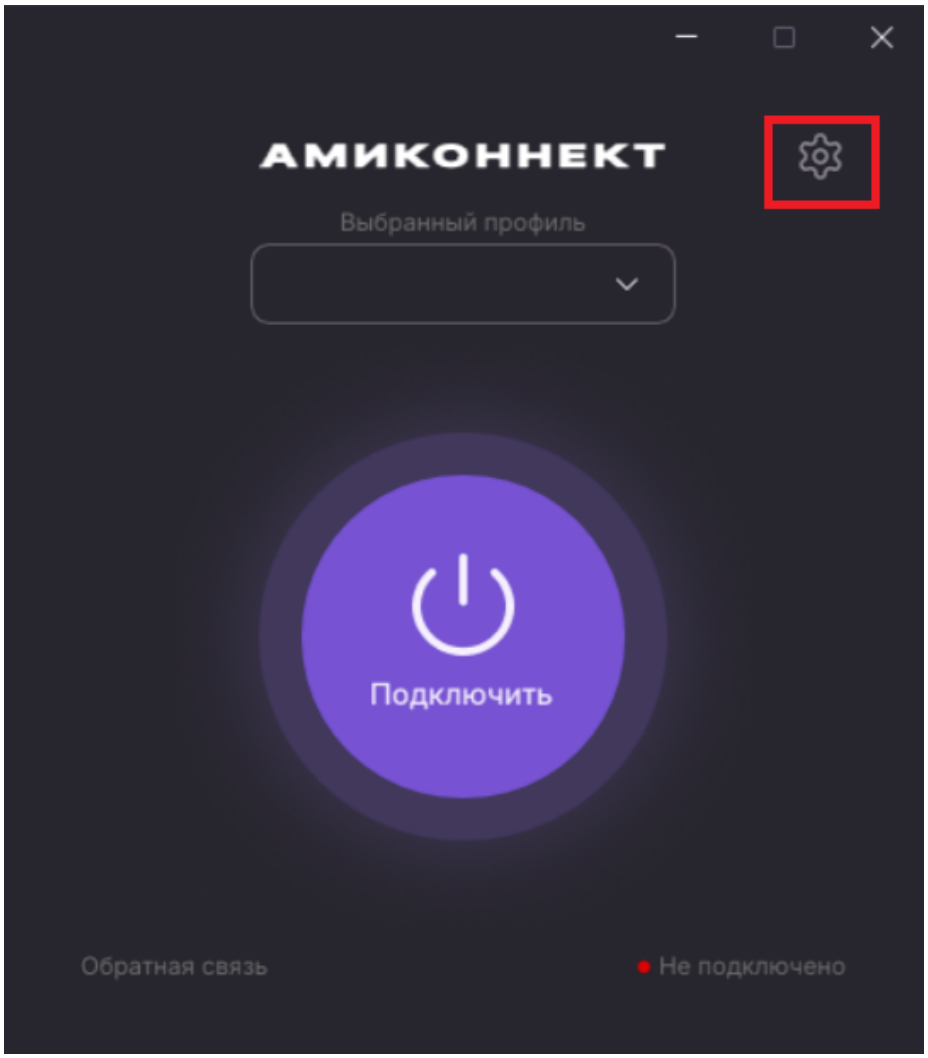

Рисунок 24 – Значок настроек

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.

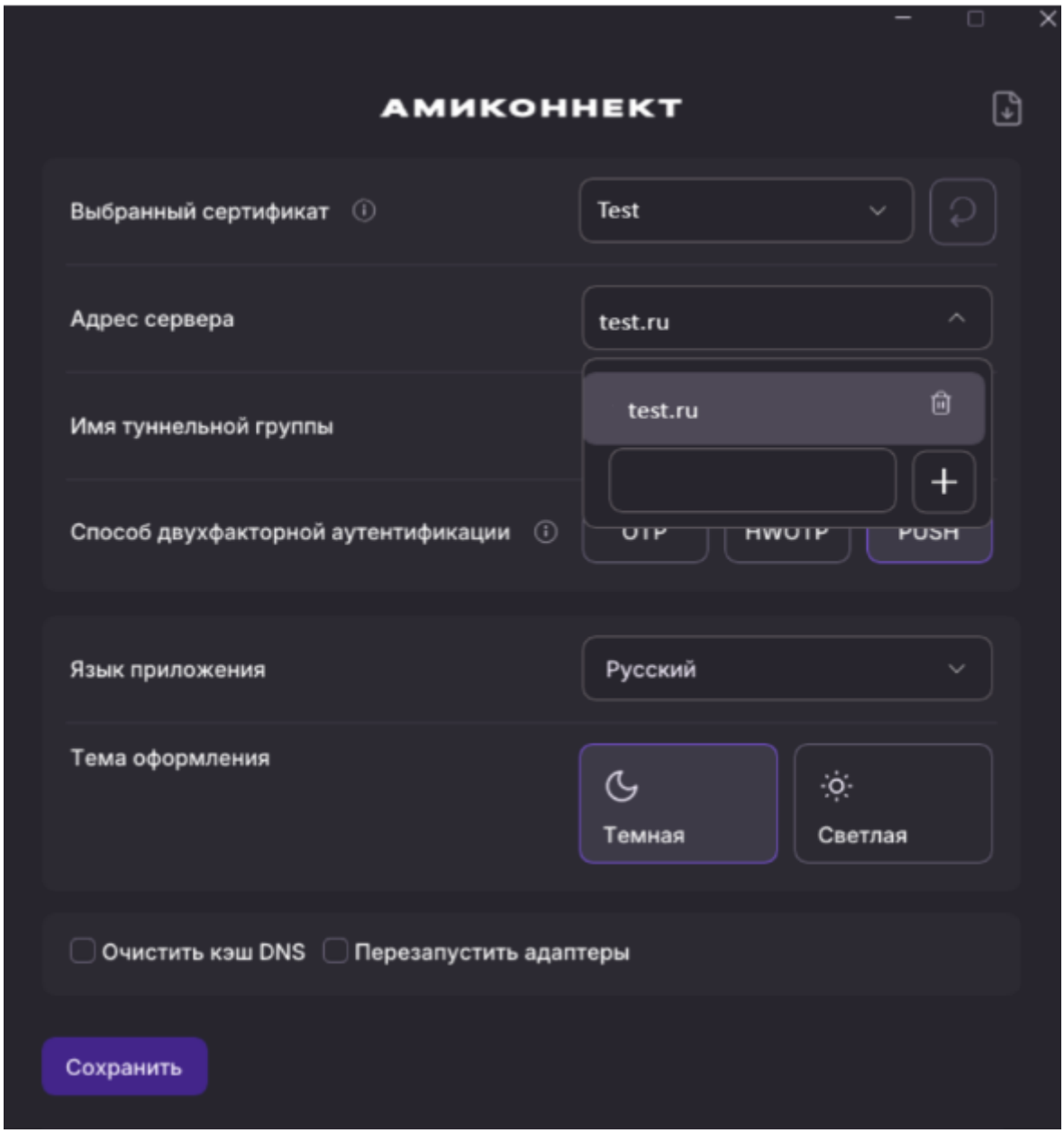

Рисунок 25 – Настройки Амиконнект

Удаление адреса возможно по кнопке удаления  .

6. 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:

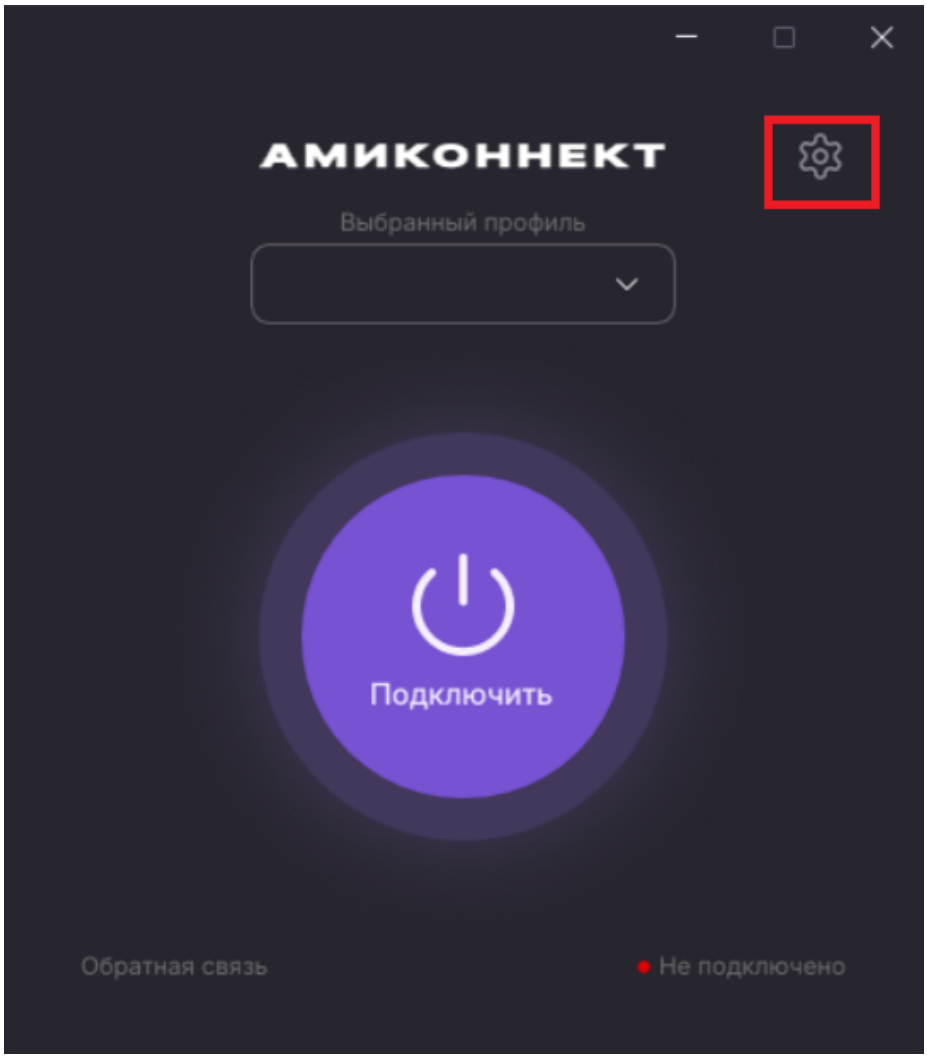

Рисунок 26 – Значок настроек

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.

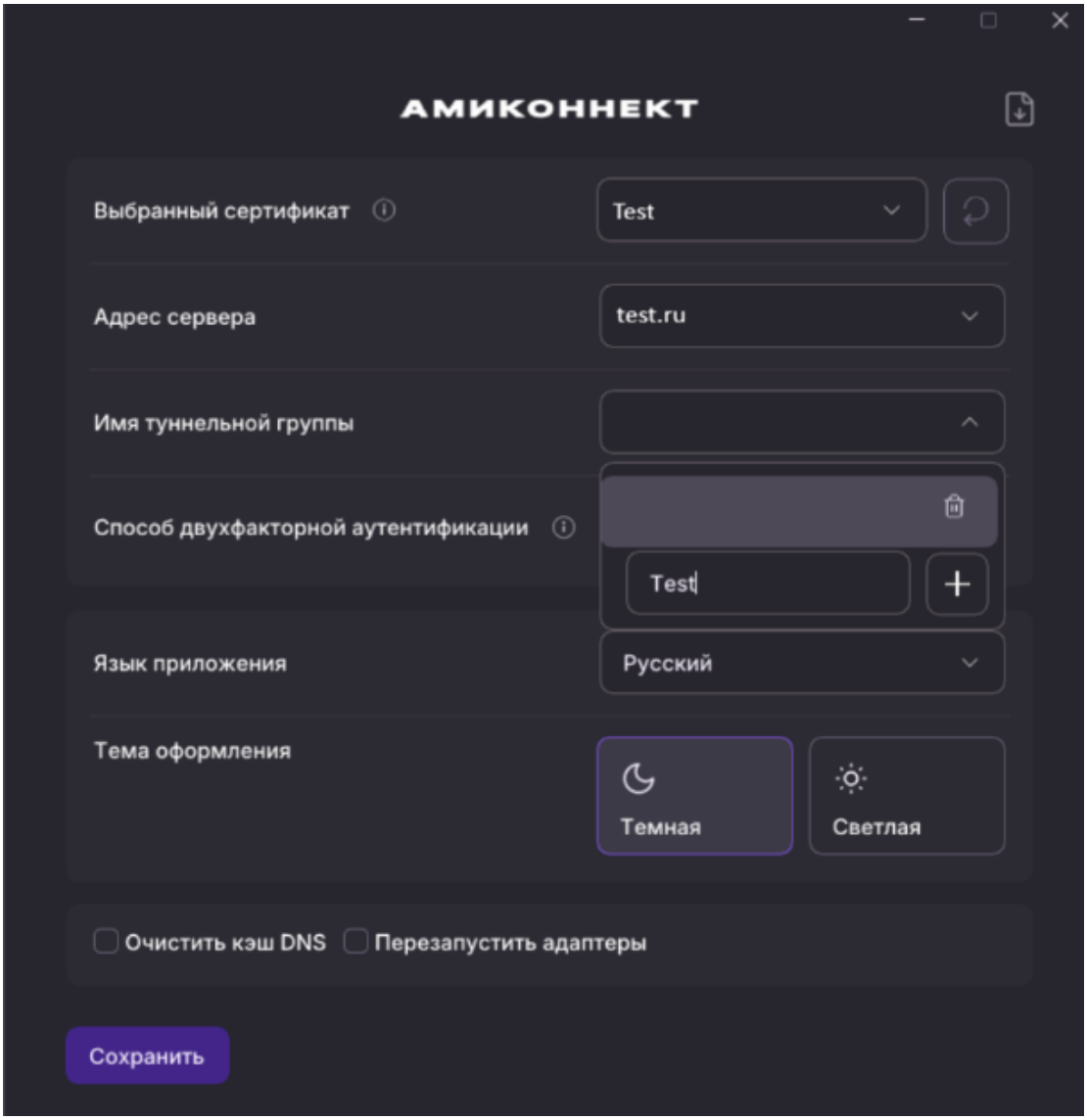

Рисунок 27 – Настройки Амиконнект

Удаление туннельной группы возможно по кнопке удаления  .

6. 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.

6. 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.

7. Запуск АМИКОННЕКТ

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

После авторизации пользователя в операционной системе, в области уведомлений в трее 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 клавишей мыши на значке программы. На экран будет выдано меню Амиконнект, содержащее следующие команды:

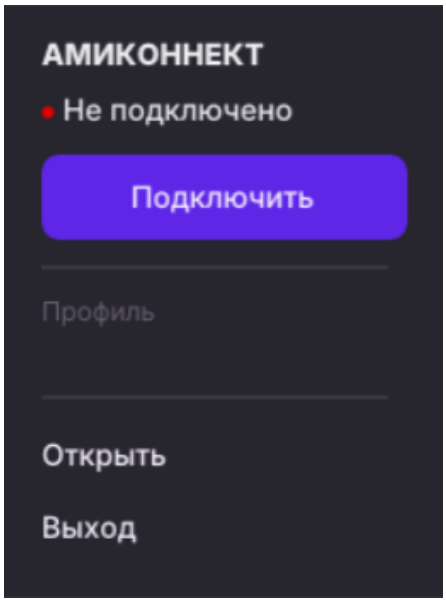

Рисунок 28 – Меню Амиконнект

7. 1. Папки и системные компоненты, затрагиваемые установкой АМИКОННЕКТ

Папка установки Амиконнект по умолчанию: /Library/Amiconnect:

- Общие конфигурационные файлы.
- Общие пользовательские настройки.
- Управляющие исполняемые скрипты:

  checkhashes – проверка контрольных сумм

  restartdaemon – перезапустить фоновый процесс

  startup – запуск фонового процесса

  uninstall – удаление Амиконнект

Каталог log с протоколом работы фонового процесса:

- Логи каждого пользователя находятся в папке настроек пользователя в подпапке log\ClientLog.csv
- Логи сервиса в папке установки в подпапке log\SrvLog.csv
- Папка настроек пользователя: /amiconnect

Пакет приложения называется Amiconnect.app, он устанавливается в папку /Applications.

Фоновый процесс называется amiconnectd, расположение Amiconnect.app/Contents/PlugIns/amiconnectd.app/Contents/MacOS/amiconnectd

Файл настройки автоматического запуска фонового процессарасположен в

каталоге /Library/LaunchDaemons/amiconnect.dmn.plist

В качестве драйвера-фильтра используется системное расширение (сетевое расширение tunnel), которое необходимо включить после установки программы в объектах входа и расширениях.

Аргументами фонового процесса являются следующие команды:

- run_as_process – запустить как процесс, а не как демон;
- instdrv – запрос активации системного расширение tunnel;
- unistdrv – запрос деактивации системного расширение tunnel.

Значение имеет только первый аргумент, остальные игнорируются.

Файл настроек пользователя cfg.ini располагается в папке настроек пользователя.

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

8. Деинсталляция ПО АМИКОННЕКТ

Амиконнект полностью удаляется с устройства, включая все связанные файлы, настройки и записи в реестре. Удаление можно произвести двумя способами:

1. Через "Программы".

2. С помощью деинсталлирующего файла, расположенного в папке /Library/Amiconnect/uninstall.

8. 1. Удаление через «Программы»

1. Закройте приложение в статус-баре, если оно открыто.

2. Откройте библиотеку приложений "Программы".

3. Найдите Амиконнект в списке.

4. Нажмите правой кнопкой мыши на иконку приложения. Выберите пункт "Удалить".

5. Дождитесь завершения процесса удаления.

6. Убедитесь, что приложение больше не отображается в списке установленных программ.

8. 2. Удаление через деинсталлятор

1. Откройте папку с компонентами приложения Амиконнект (/Library/Amiconnect/uninstall).

2. Запустите файл деинсталлятора.

3. Введите пароль администратора в окне деинсталлятора и нажмите «return».

4. После процесса удаления закройте окно деинсталлятора.

Для завершения процесса удаления ПО требуется перезагрузить рабочую станцию.

8. 3. Удаление сертификатов

В целях безопасности после удаления с рабочей станции приложения Амиконнект рекомендуем удалить корневые и пользовательские сертификаты из соответствующих хранилищ сертификатов.

8. 3. 1. Удаление корневого сертификата

Откройте хранилище сертификатов Связка ключей:

- Выберите целевой сертификат и нажмите на него правой кнопкой мыши.

- Выберите пункт «Удалить»

- Убедитесь, что сертификат больше не отображается в списке сертификатов.

8. 3. 2. Удаление пользовательского сертификата

Откройте хранилище сертификатов Связка ключей:

- Выберите целевой сертификат и нажмите на него правой кнопкой мыши.

- Выберите пункт «Удалить»

- Убедитесь, что сертификат больше не отображается в списке сертификатов.

После выполнения всех описанных шагов убедитесь, 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 диагностики

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.

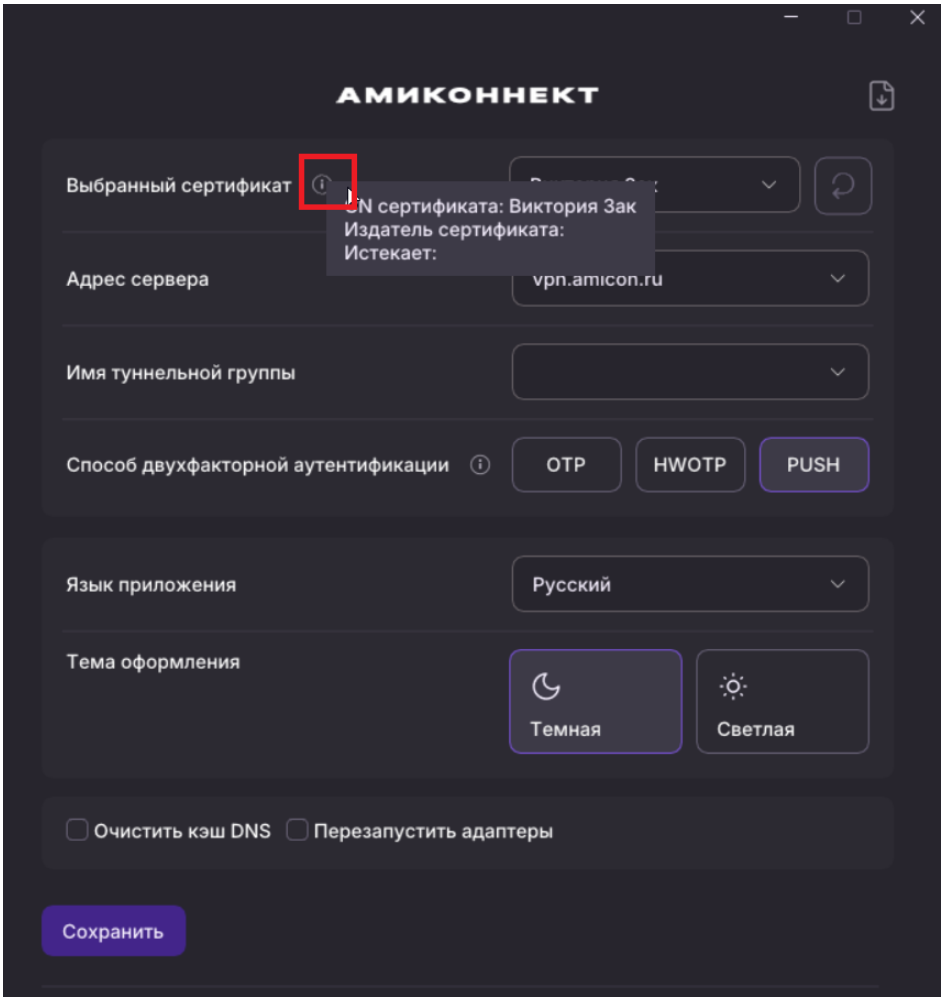

Рисунок 29 – Выбранный сертификат

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.

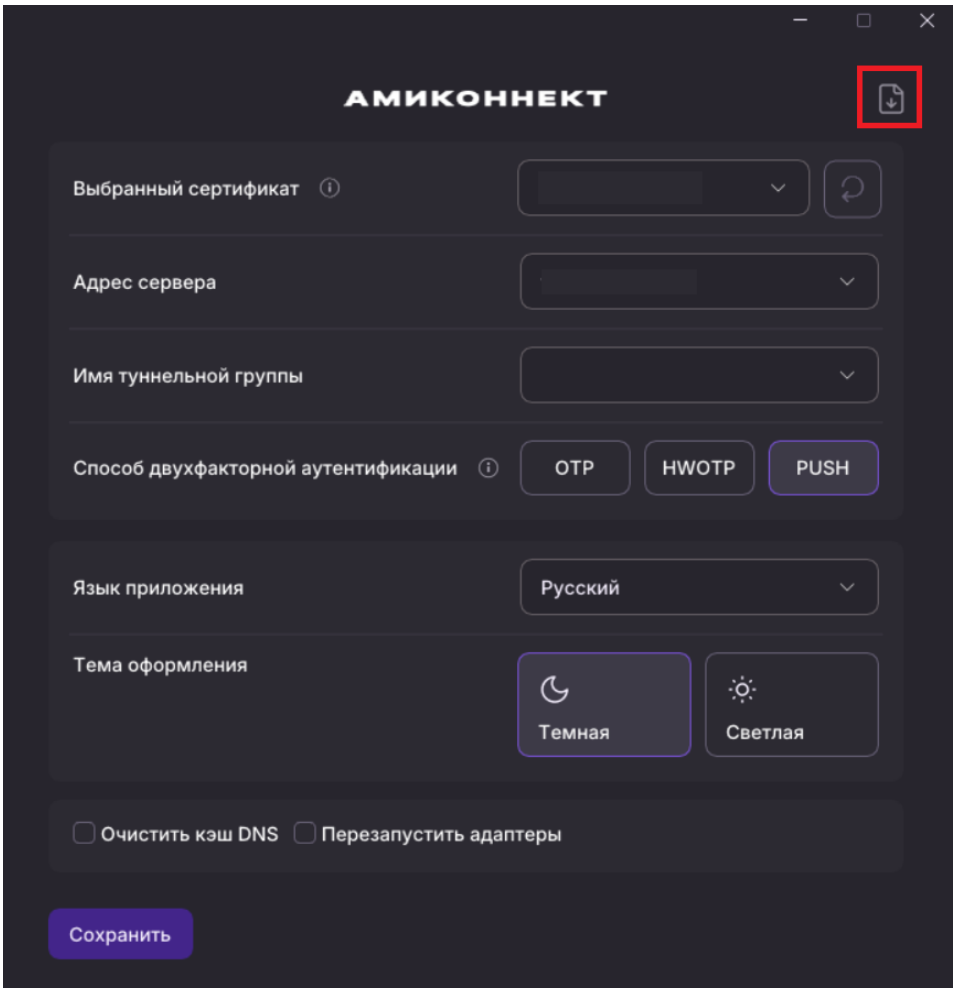

Рисунок 30 – Кнопка выгрузки логов

9. 3. Сообщения об ошибках при соединении с ФПСУ

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