Инструкция по настройке рабочего места с операционной системой Mac OS для работы с усиленной квалифицированной электронной подписью

Банк ВТБ (ПАО)

2025

Оглавление

1. Общие требования 2
2. Установка драйверов ключевого носителя 2
3. Настройка рабочего места 3
3.1. Установка СКЗИ КриптоПро 5.0 (сертифицированная версия) и плагина 3
3.2. Скачивание сертификатов 8
3.2.1. Доверенный корневой сертификат от Минцифры России 8
3.2.2. Сертификаты Удостоверяющего центра ВТБ и списка аннулированных сертификатов 8
3.3. Установка доверенных сертификатов Минцифры и Удостоверяющего центра ВТБ 9
3.4. Установка личного сертификата с ключевого носителя 10

1. Общие требования

Перед началом работы требуется внимательно ознакомиться с Руководством по обеспечению безопасности использования квалифицированной электронной подписи и учесть все рекомендации: https://www.vtb.ru/media-files/vtb.ru/sitepages/npb/temp-files/rukovodstvo_po_obespecheniyu_bezopasnosti_ispolzovaniya_kvalificirovannoy_....pdf.

Необходимо обязательно установить СВОЙ пин-код на носитель ключевой информации (usb-токен).

Обеспечить конфиденциальность своей электронной подписи – не передавать КЭП (usb-токен с ключами ЭП и квалифицированным сертификатом) для использования третьим лицам. Если нужно отойти от рабочего места – заберите usb-токен с собой и заблокируйте компьютер.

Следить за обновлением антивируса на компьютере, где будете работать с электронными документами.

Подготовить компьютер для работы с электронной подписью.

Необходимое программное обеспечение, которое должно быть установлено на рабочем месте:

- драйверы для используемого ключевого носителя (Рутокен, ESMART и т.д.);
- СКЗИ «КриптоПро CSP» версии 5.0 R3 (сертифицированная версия, требуется лицензия);
- плагин КриптоПро ЭЦП Browser Plug-in (входит в состав дистрибутива КриптоПро CSP сборки 13000);
- сертификаты Минцифры России и УЦ ВТБ;
- личный сертификат ключа электронной подписи, выданный УЦ ВТБ.

2. Установка драйверов ключевого носителя

Драйвер – программное обеспечение, которое помогает операционной системе распознать подключенное устройство и правильно работать с ним. Необходимо скачать и установить драйвер, соответствующий используемому носителю:

- ПО для работы со специальным ключевым носителем Рутокен: https://www.rutoken.ru/support/download/mac/
- ПО для работы с ПАК «ESMART® Token»: https://token.esmart.ru/downloads

При необходимости может потребоваться установка соответствующих плагинов для браузера.

3. Настройка рабочего места

3.1. Установка СКЗИ КриптоПро 5.0 (сертифицированная версия) и плагина

На данный момент популярные операционные системы по умолчанию не поддерживают российские криптографические алгоритмы, а для работы с электронной подписью, отвечающей требованиям закона, они необходимы.

КриптоПро CSP – специализированное программное обеспечение (криптопровайдер), добавляющее в операционную систему вашего устройства необходимые алгоритмы работы с российской криптографией. Установка программы позволяет работать с электронной подписью соответствующей Федеральному закону № 63-ФЗ «Об электронной подписи».

- Зарегистрируйтесь на сайте КриптоПро заполнив обязательные поля: https://www.cryptopro.ru/downloads
- Подтвердите ознакомление с лицензионным соглашением: https://cryptopro.ru/download?pid=1417
- Скачайте сертифицированную версию КриптоПро (сборка не ниже версии 13000), в состав дистрибутива уже входит плагин КриптоПро ЭЦП Browser Plug-in.

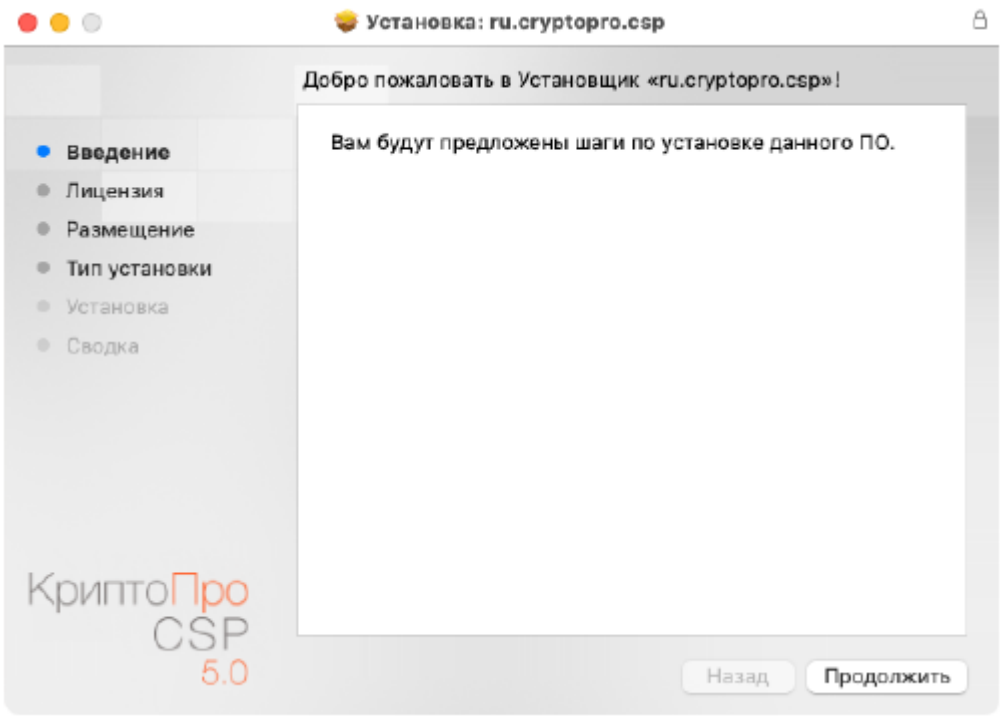
Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора — под учётной записью root или с использованием команды sudo. СКЗИ КриптоПро CSP требует следующей последовательности установки: сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

В ОС Mac OS X для установки, удаления и обновления ПО применяются пакеты (packages). Пакет — архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. Дистрибутив поставляется в упакованном виде, имеет формат .dmg и представляет собой образ диска, содержащий пакет.

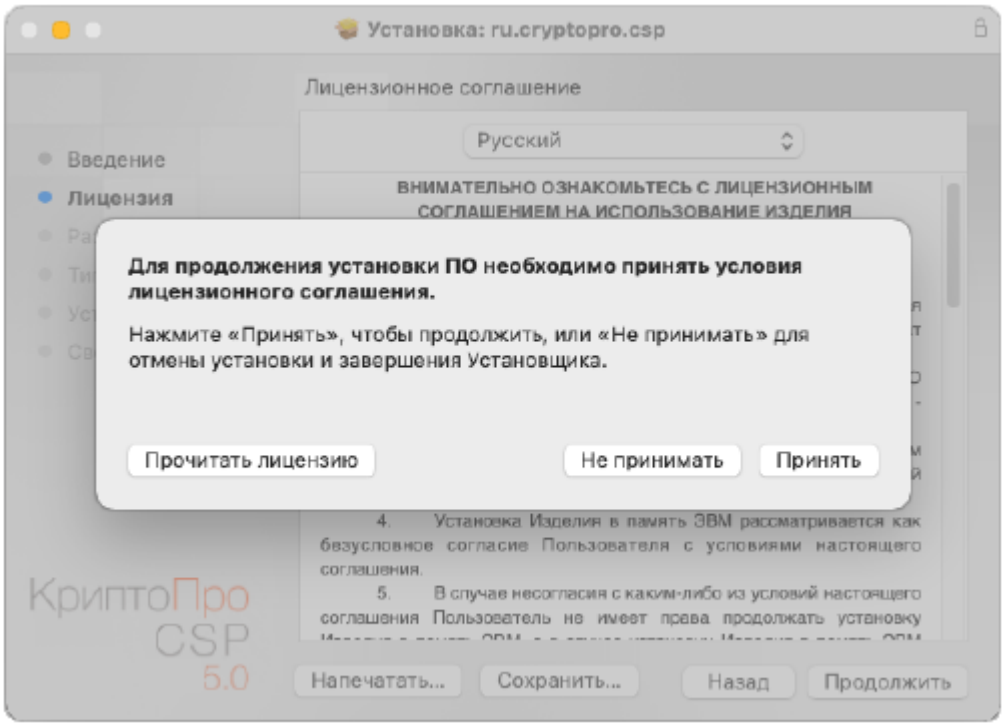
Для управления пакетами используются стандартные средства для управления пакетами Mac OS. Файлы из пакетов устанавливаются в /opt/cprocsp.

Для установки пакета через графический интерфейс откройте образ диска с дистрибутивом (ru.cryptopro.csp-5.0.XXXXX.dmg), а затем откройте файл пакета (ru.cryptopro.csp-5.0.XXXXX.pkg).

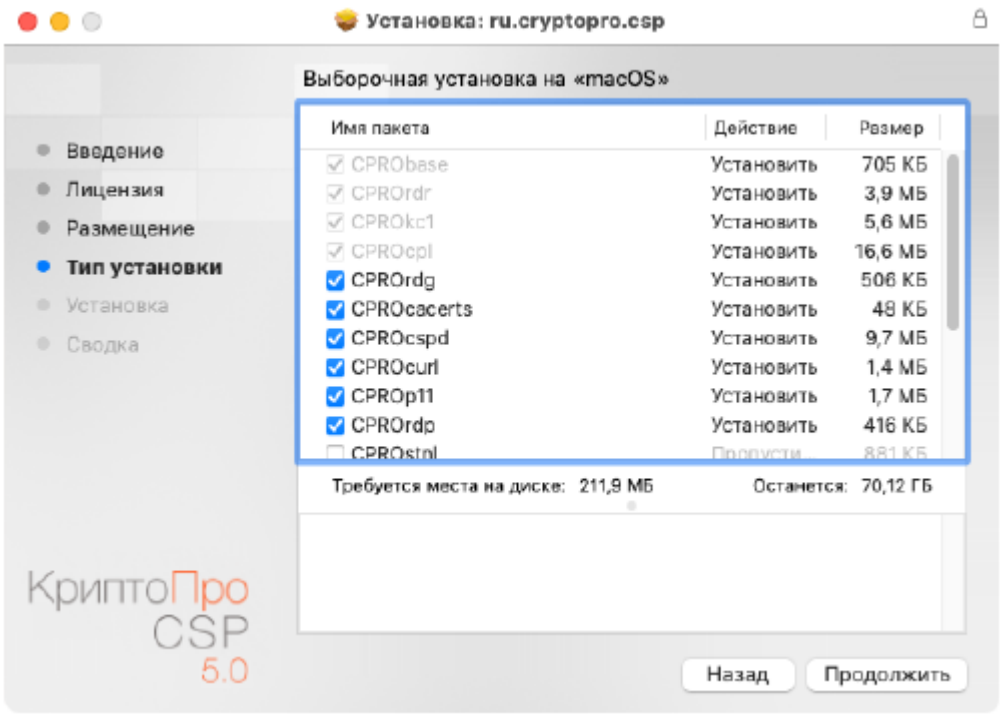
Разрешите запуск программы. Откроется приветственное окно инсталлятора СКЗИ:



Нажмите **Продолжить** для установки СКЗИ. Внимательно прочитайте лицензионное соглашение. Для продолжения установки необходимо **Принять** лицензионное соглашение, иначе установка будет отменена.



В следующем окне выводится список устанавливаемых пакетов. Отметьте пакеты, которые будут нужны при работе с СКЗИ, или оставьте выбор по умолчанию и нажмите **Продолжить**. При выборе пакета в нижней части окна выводится краткое описание назначения пакета.

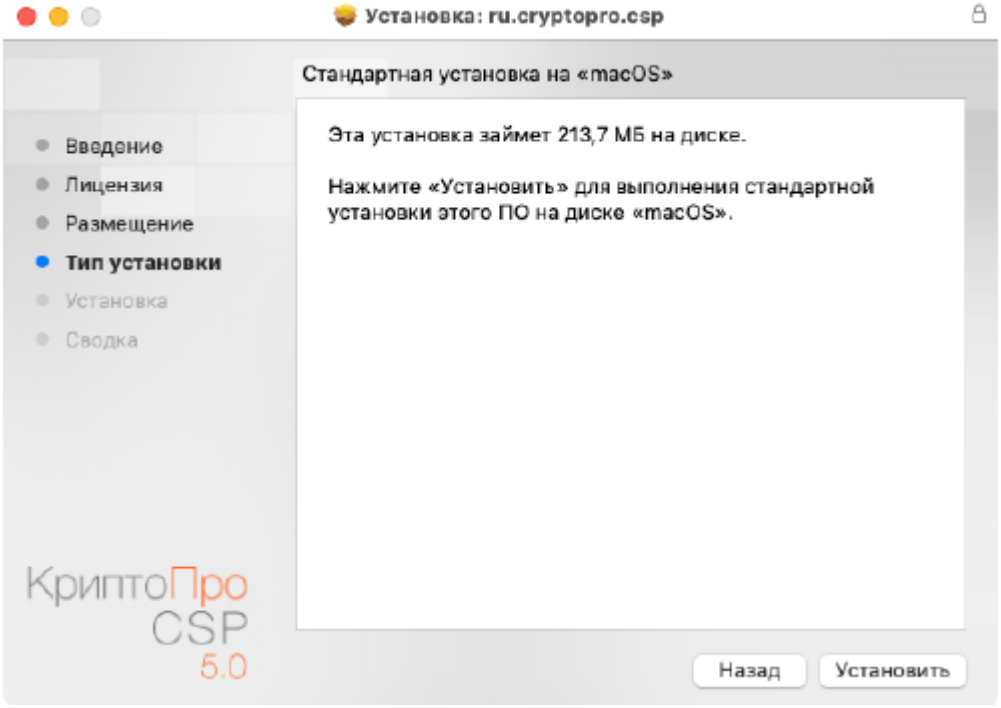


Доступны для выбора:

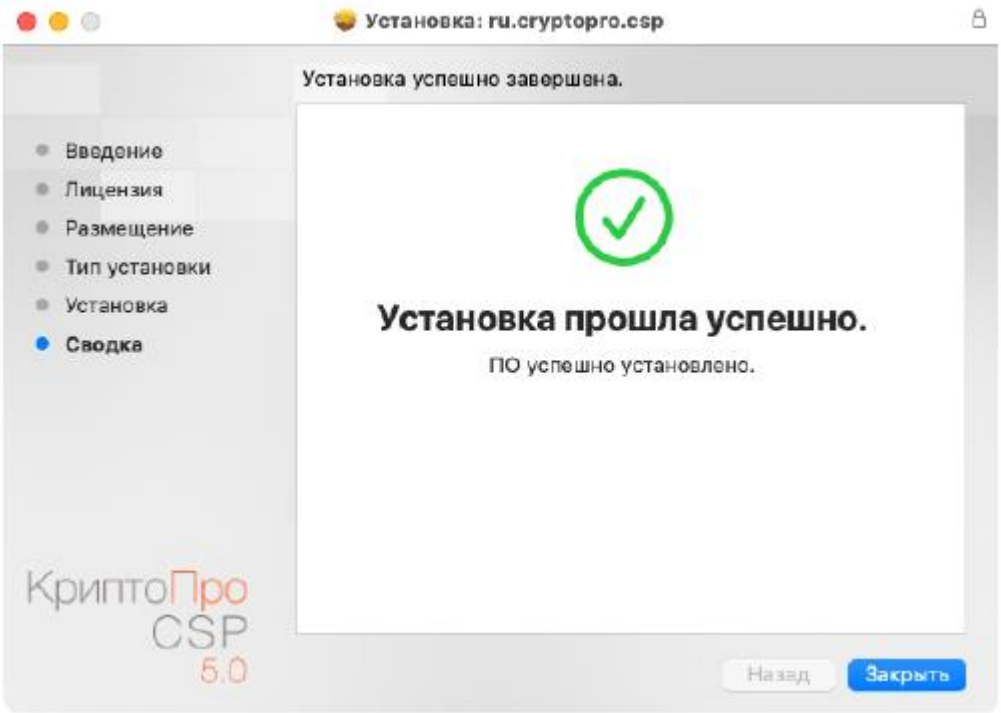
Имя пакета	Назначение пакета
Обязательные пакеты	
CPRObase	Базовый пакет КриптоПро CSP, устанавливается первым
CPROrdr	Модуль поддержки основных приложений, считывателей и ДСЧ
CPROkc1	Провайдер класса KC1
CPROcpl	CAPILite, программы и библиотеки для высокоуровневой работы с криптографией (сертификатами, CMS...)
Дополнительные пакеты	
CPROrdg	Графические диалоговые окна
CPROcacerts	Сертификаты доверенных корневых и промежуточных УЦ
CPROcspd	Пакет для разработчиков приложений, использующих КриптоПро CSP (SDK)
CPROcurl	Библиотека libcurl и приложение cURL (с поддержкой ГОСТ TLS)
CPROp11	Модуль поддержки PKCS#11
CPROrdp	Модули поддержки считывателей смарт-карт (PC/SC)
CPROstnl	Универсальный SSL/TLS туннель

CPROstnlm	Универсальный SSL/TLS туннель с поддержкой интерфейса msspi
CPROcptools	Графическое приложение для доступа к основным функциям и настройкам КриптоПро CSP
CPROrdcloud	Модуль взаимодействия с КриптоПро DSS — КриптоПро Cloud CSP
CPROimportcacerts	Модуль импорта корневых сертификатов ОС в доверенное корневое хранилище КриптоПро CSP
CPROlegacy	Устаревшие библиотеки КриптоПро CSP
cprocsp-pki-cades	Библиотеки и утилиты для КриптоПро ЭЦП SDK
cprocsp-pki-plugin	Библиотеки для КриптоПро ЭЦП Browser plug-in
Поддержка ключевых носителей	
CPROrdcpfkc	Модуль поддержки ФКН с поддержкой SESPAKE
CPROrdcryptoki	Модуль для поддержки внешних PKCS#11-носителей
CPROrdedoc	Модуль поддержки платформы eDoc (УЛГ)
CPROrdemv	Модуль поддержки смарт-карт Gemalto (EMV)
CPROrdesmart	Модуль поддержки носителей ESMART
CPROrdhvisdef	Модуль поддержки базового визуализатора подписи
CPROrdinfocrypt	Модуль поддержки носителей InfoCrypt
CPROrdinpaspot	Модуль поддержки смарт-карт Alioth
CPROrdjacarta	Модуль поддержки носителей JaCarta
CPROrdkst	Модуль поддержки смарт-карт MorphoKST
CPROrdmskey	Модуль поддержки носителей Multisoft MS_Key
CPROrdnova	Модуль поддержки смарт-карт Novacard
CPROrdrosan	Модуль поддержки смарт-карт Rosan
CPROrutoken	Модуль поддержки носителей Рутокен

После выбора пакетов нажмите **Установить**:



В открывшемся окне укажите пароль пользователя, имеющего права на установку ПО на данном компьютере. Начнется установка ПО СКЗИ. Прогресс установки отображается в окне инсталлятора. При успешной установке выводится соответствующее сообщение и инсталлятор можно закрыть.



Подробнее про установку СКЗИ КриптоПро на сайте продукта: https://cryptopro.ru/sites/default/files/private/csp/50/13000/doc-kc1.zip Руководство администратора безопасности. Использование СКЗИ под управлением Mac OS.

После скачивания, программа КриптоПро CSP 5.0 доступна 90 дней. Для продолжения работы необходимо приобрести лицензию на ПО КриптоПро CSP

3.2. Скачивание сертификатов

Сертификат Минцифры и Удостоверяющего центра ВТБ участвует в «цепочке доверия».

«Цепочка доверия» — это взаимосвязь нескольких сертификатов, которая позволяет проверить, действительна ли электронная подпись и можно ли доверять сертификату подписи.

Вы можете скачать на свой компьютер файлы сертификатов Минцифры России и УЦ ВТБ по следующим ссылкам:

3.2.1. Доверенный корневой сертификат от Минцифры России

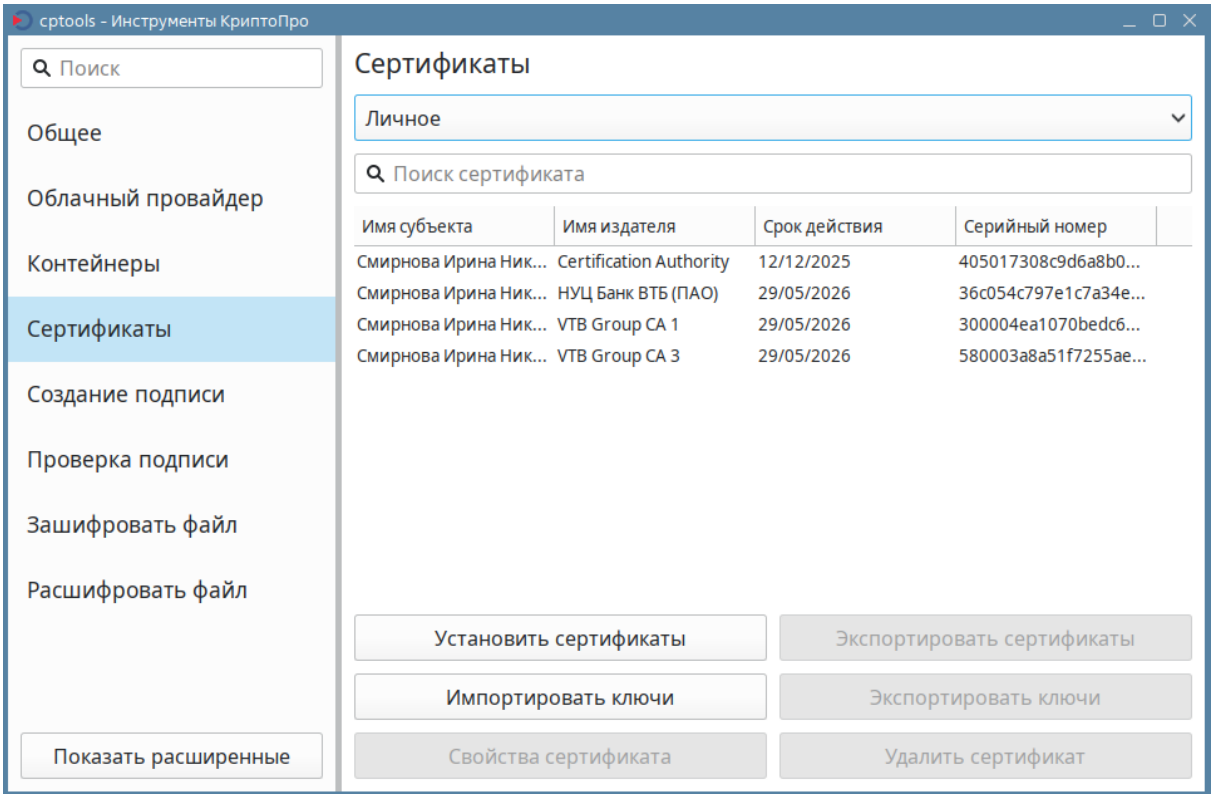
- Ссылка для скачивания файла корневого сертификата: https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/download/2F0CB09BE3550EF17EC4F29C90ABD18BFCAAD63A

3.2.2. Сертификаты Удостоверяющего центра ВТБ и списка аннулированных сертификатов

- Сертификат УЦ для установки в хранилище «Промежуточные доверенные корневые центры сертификации», адрес1: http://pki1.vtb.ru/aia/auc/vtba_2024.cer
- Сертификат УЦ для установки в хранилище «Промежуточные доверенные корневые центры сертификации», адрес2: http://ca.vtb.ru/aia/auc/vtba_2024.cer
- Список аннулированных сертификатов (crl), адрес1: http://pki1.vtb.ru/cdp/auc/vtba_2024.crl
- Список аннулированных сертификатов (crl), адрес2: http://ca.vtb.ru/cdp/auc/vtba_2024.crl

3.3. Установка доверенных сертификатов Минцифры и Удостоверяющего центра ВТБ

Откройте **Инструменты КриптоПро (**Finder – Программы - Инструменты КриптоПро). В левом меню выберите **Сертификаты**.

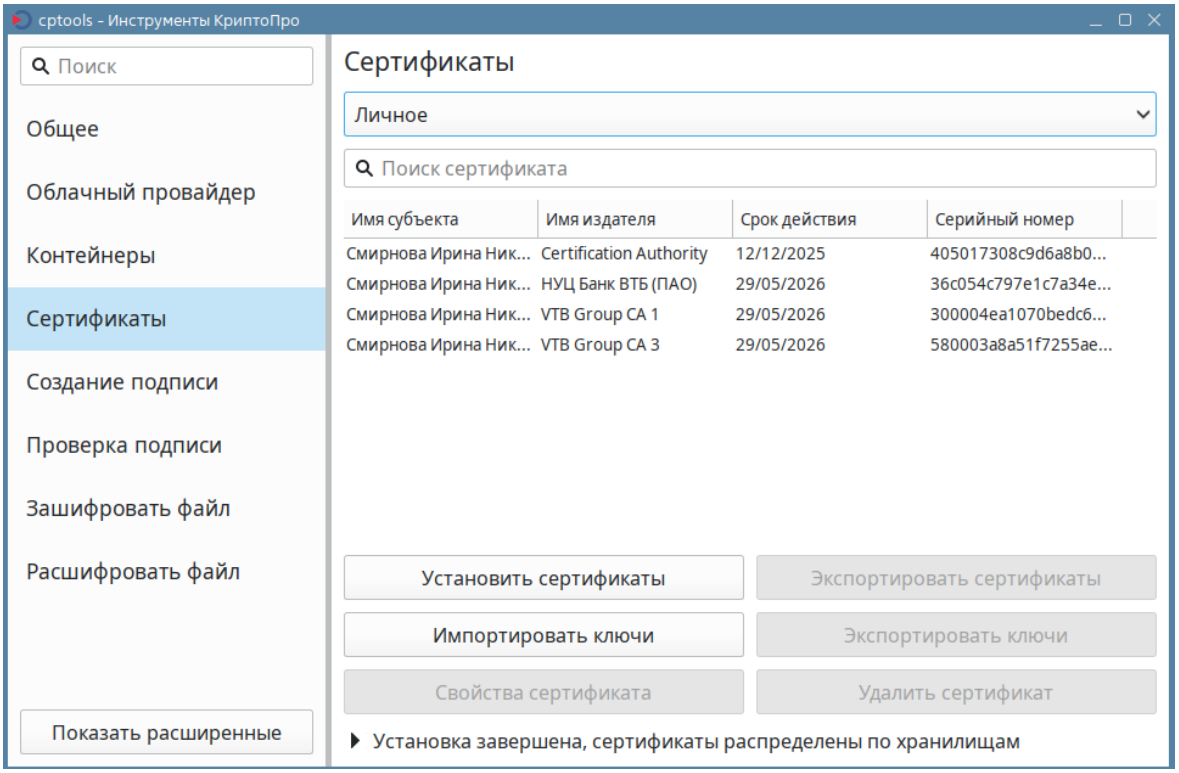


Нажмите **Установить сертификаты**,

Выберите файл сертификата Минцифры или Удостоверяющего центра ВТБ (обычно с расширением .cer или .crt).

Система самостоятельно определит файл в необходимое хранилище.

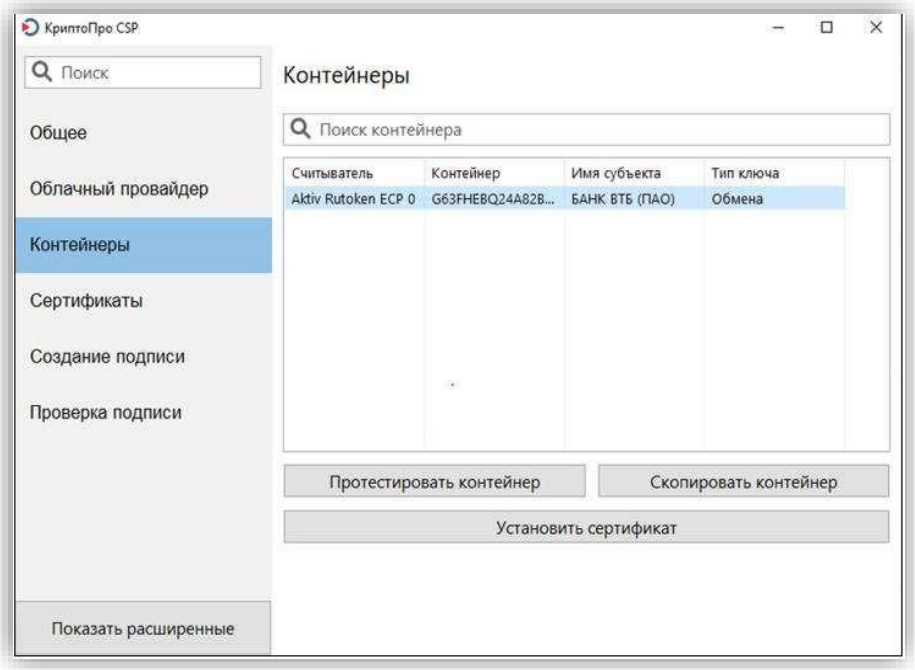
Дождитесь сообщения о завершении установки:



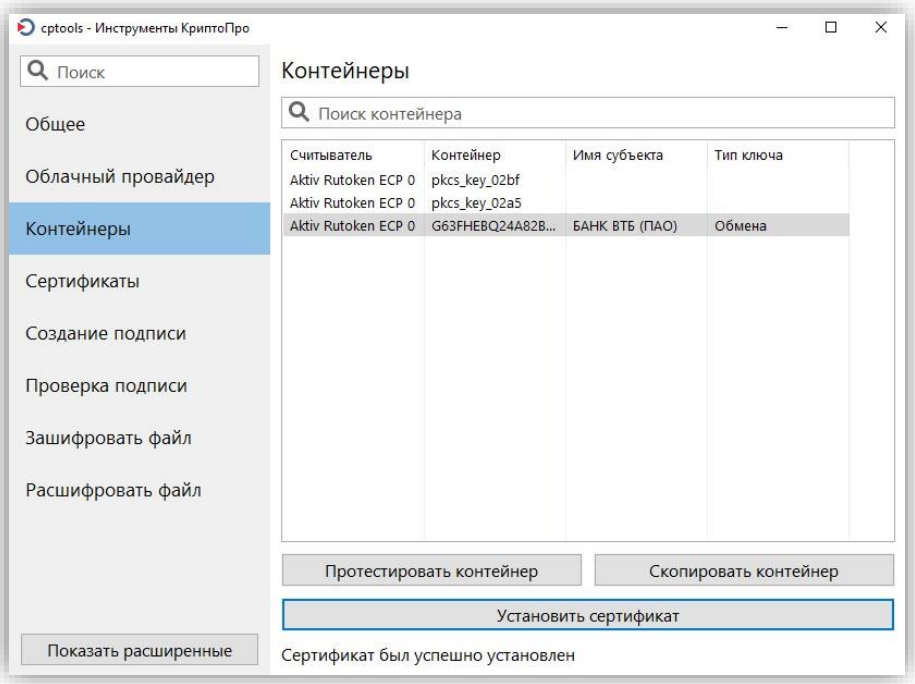
3.4. Установка личного сертификата с ключевого носителя

Подключите usb-токен. Откройте **Инструменты КриптоПро** (Finder – Программы - Инструменты КриптоПро).

В левом меню выберите **Контейнеры**. Выберите нужный ключевой контейнер и нажмите **Установить сертификат**.



Дождитесь сообщения об успешной установке сертификата:



Ваш компьютер настроен для работы с квалифицированной электронной подписью.