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

Банк ВТБ (ПАО)

2025

Оглавление

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.

Для работы с электронной подписью в различных сервисах и информационных системах рекомендуется использовать Браузеры:

- Яндекс.Браузер с КриптоПро (для организаций);
- Chromium GOST;
- CryptoPro Fox.

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/windows/
- 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

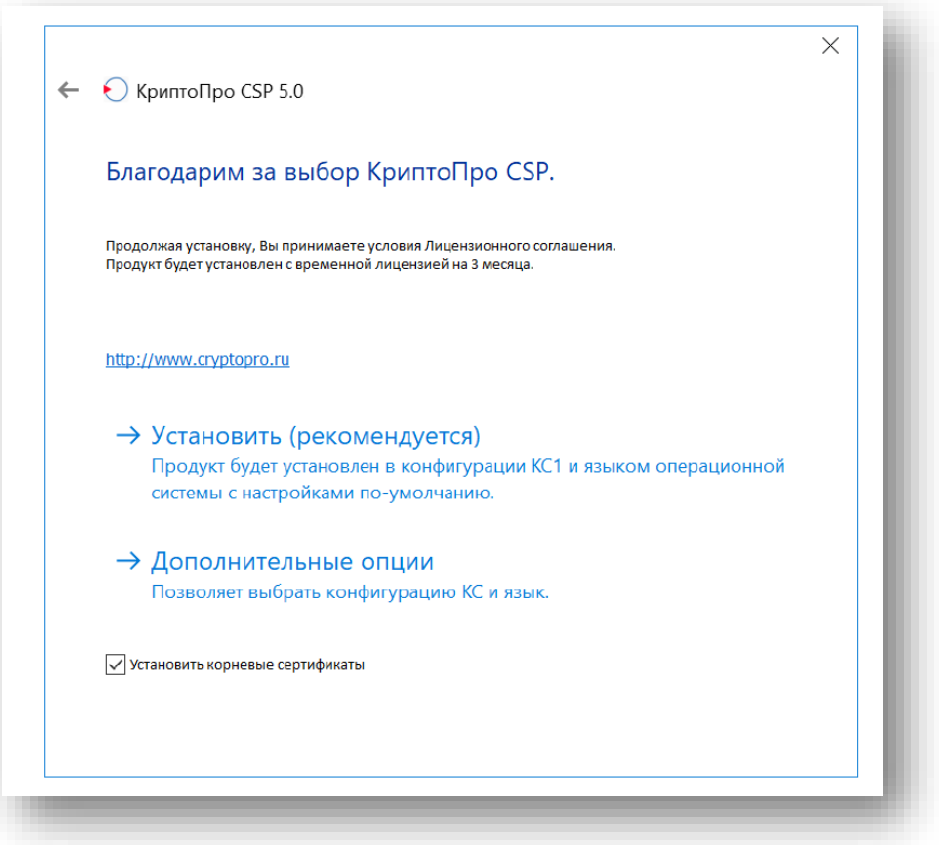
На данный момент популярные операционные системы по умолчанию не поддерживают российские криптографические алгоритмы, а для работы с электронной подписью, отвечающей требованиям закона, они необходимы.

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 дистрибутива КриптоПро CSP должна производиться пользователем, имеющим права администратора. Для установки СКЗИ КриптоПро CSP сначала необходимо установить провайдер, а затем устанавливать остальные модули, входящие в состав комплектации, в том числе специальный плагин КриптоПро ЭЦП Browser Plug-in (входит в состав дистрибутива).

В начальном окне Мастера установки нажмите **Установить**, чтобы начать установку КриптоПро CSP в конфигурации КС1 и языком операционной системы.



По умолчанию в окне установлен флаг «Установить корневые сертификаты».
При установке СКЗИ в случае отсутствия указанных сертификатов в хранилище «Доверенные корневые центры сертификации» локального компьютера устанавливаются следующие корневые сертификаты (перечислены значения соответствующих имен субъекта (CN)):

- CryptoPro GOST Root CA;
- Минкомсвязь России;
- Минцифры России;
- Головной удостоверяющий центр;
- НУЦ России.

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел или настроить криптопровайдер на использование службы хранения ключей.

Все эти настройки можно произвести в момент установки ПО, либо через «Панель управления» в любой момент после завершения установки.

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

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

3.2. Скачивание сертификатов

Сертификаты 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

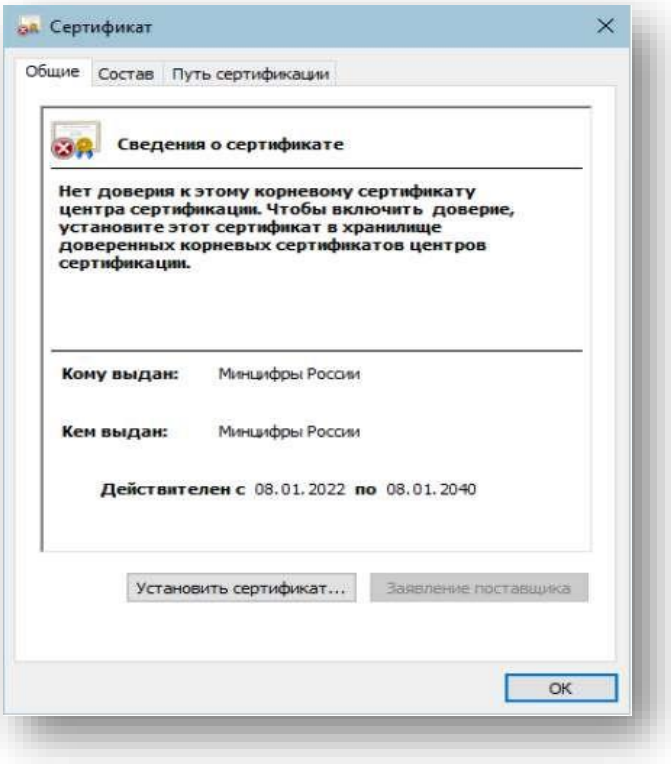
- Ссылка для скачивания файла корневого сертификата: https://e-trust.gosuslugi.ru/app/scc/portal/api/v1/portal/ca/download/2F0CB09BE3550EF17EC4F29C90ABD18BFCAAD63A

3.2.2. Сертификаты Удостоверяющего центра ВТБ и списки аннулированных сертификатов

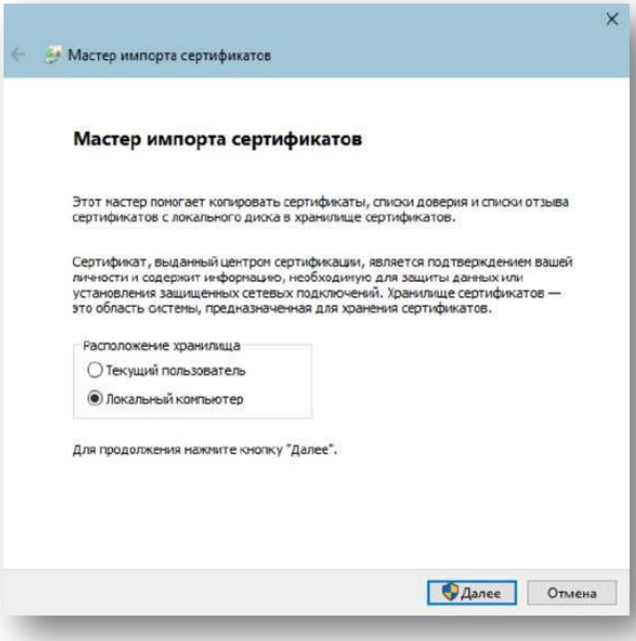
- Сертификат УЦ для установки в хранилище «Промежуточные доверенные корневые центры сертификации», адрес1: http://pki1.vtb.ru/aia/auc/vtba_2024.cer
- Сертификат УЦ для установки в хранилище «Промежуточные доверенные корневые центры сертификации», адрес2: http://ca.vtb.ru/aia/auc/vtba_2024.cer
- Список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

Для установки откройте файл сертификата и нажмите **Установить сертификат**:



Выберите расположение хранилища «Локальный компьютер» и нажмите **Далее**:



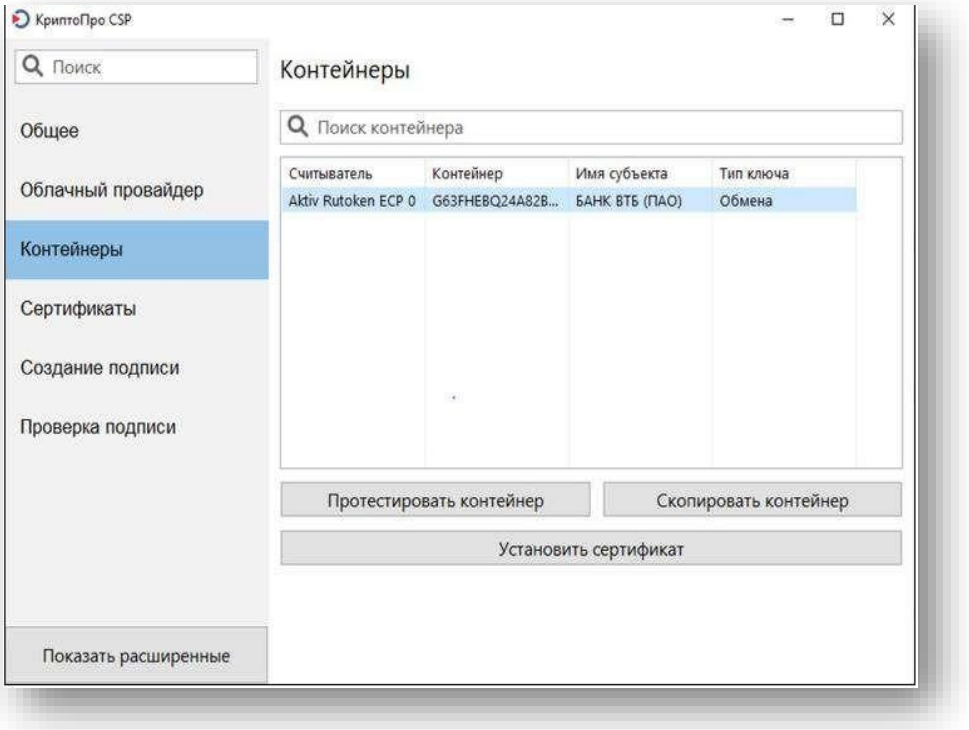
Необходимо выбрать соответственно следующие хранилища:

- **Доверенные корневые центры сертификации** - для установки корневого сертификата Минцифры России
- **Промежуточные центры сертификации** - для установки сертификата УЦ ВТБ и списков аннулированных сертификатов УЦ ВТБ.

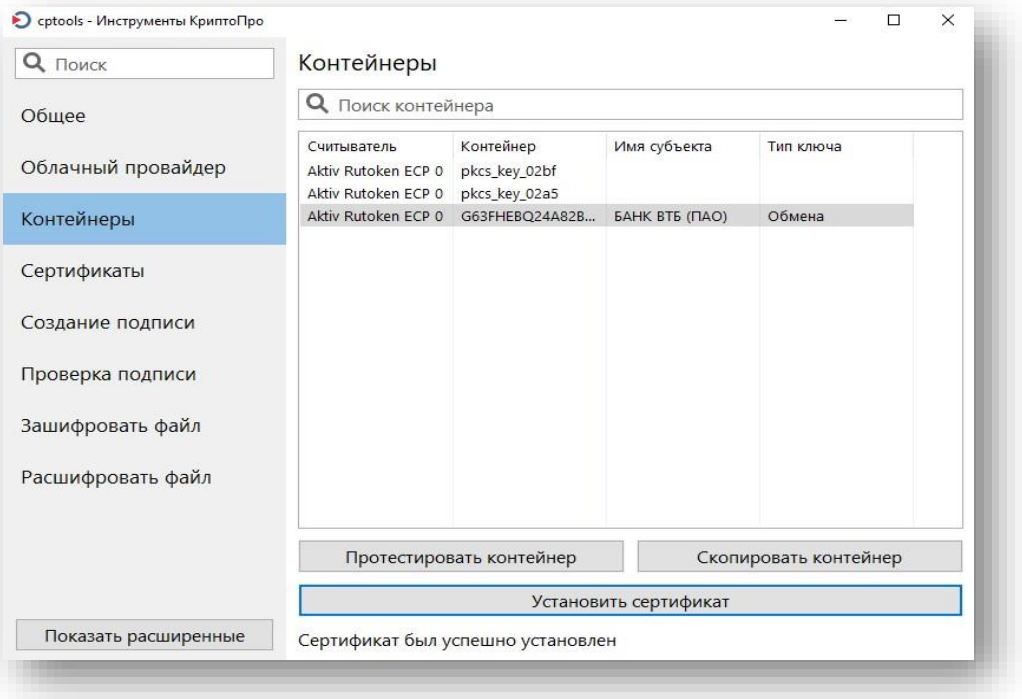
Последовательно нажать **Далее** и **Готово**.

3.4. Установка личного сертификата с ключевого носителя

Установите usb-токен в USB-порт компьютера. Из меню **Пуск** откройте **Инструменты КриптоПро** и выберите в меню слева **Контейнеры**. Выберите справа нужный контейнер и нажмите **Установить сертификат**:



Дождитесь сообщения об успешной установке сертификата:



Ваш компьютер настроен для работы с квалифицированной электронной подписью.