

Установка компонентов, необходимых для работы с электронной подписью

Удостоверяющий центр КОРУС Консалтинг СНГ

Оглавление

Установка СКЗИ КриптоПро CSP.....	4
Установка драйвера ключевого носителя Рутокен.....	5
Установка КриптоПро ЭЦП Browser Plug-in.....	5
Установка личного сертификата ключа подписи.....	6
Установка корневого сертификата.....	7
Расширение для браузера CryptoPro Extension for CAdES Browser Plug-in.....	9
Экспорт сертификата для загрузки во внешнюю систему.....	9
Загрузка сертификата в сервис СФЕРА Курьер.....	12

Все программы и компоненты можно скачать по ссылке, выбрав продукт «**Электронная подпись**»:
<https://www.esphere.ru/support/download>

При установке компонентов необходимы права администратора локального пользователя на рабочем месте.

Требования к рабочему месту локального пользователя для настройки электронной подписи:

- Windows 7, Windows 8, Windows 8.1, Windows 10 и выше;
- интернет-браузер;
- наличие USB-порта и доступ в интернет.

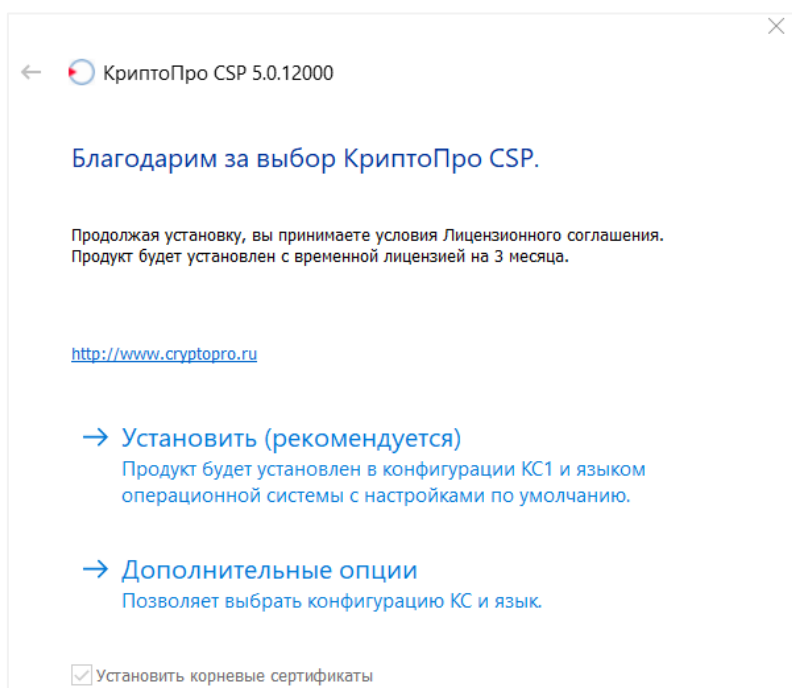
Дополнительные требования к браузеру или системе зависят от электронного сервиса или портала для работы с электронной подписью.

Установка СКЗИ КриптоПро CSP

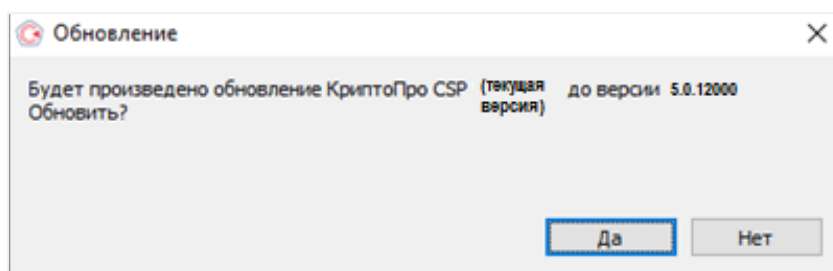
Скачайте дистрибутив по ссылке <https://www.esphere.ru/support/download> продукт «Электронная подпись» из раздела «**ДИСТРИБУТИВЫ ДЛЯ КРИПТОПРО CSP ДЛЯ WINDOWS**».

Рекомендована версия программы **5.0**

Запустите установочный файл, который скачали. В появившемся окне программы установки **КриптоПРО CSP** нажмите кнопку «**Установить (рекомендуется)**».



Если на компьютере уже есть КриптоПро CSP, то программа установки предложит обновить его. Для этого в открывшемся окне нажмите кнопку «**Да**», чтобы установить последнюю версию.



При первой установке КриптоПро CSP устанавливается временная лицензия на 3 месяца. По истечении лицензии и (или) при её отсутствии необходимо приобрести постоянную лицензию в удостоверяющем центре, в т. ч. **СБЕР КОРУС**.

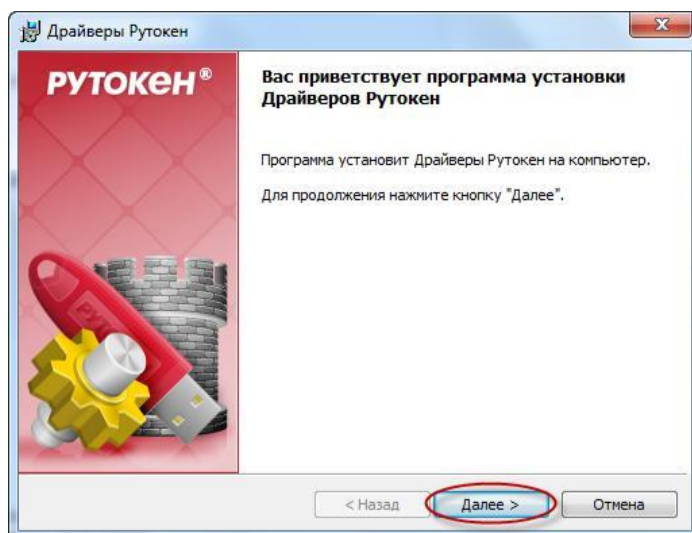
После установки программы необходимо перезагрузить компьютер.

Установка драйвера ключевого носителя Рутокен

Драйвер ключевого носителя Рутокен можно скачать по ссылке в разделе **«ДИСТРИБУТИВЫ ДЛЯ РУТОКЕН»**:
<http://www.esphere.ru/support/download/uc/>

Обратите внимание, что при установке драйвера ключевой носитель Рутокен не должен быть вставлен в USB-порт компьютера.

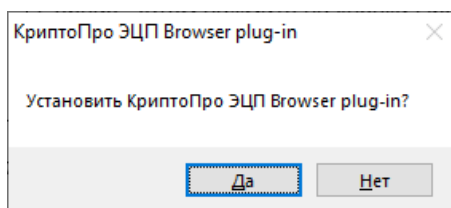
Запустите установочный файл драйвера. В открывшемся окне установки нажмите кнопку **«Далее»**, потом **«Установить»**.



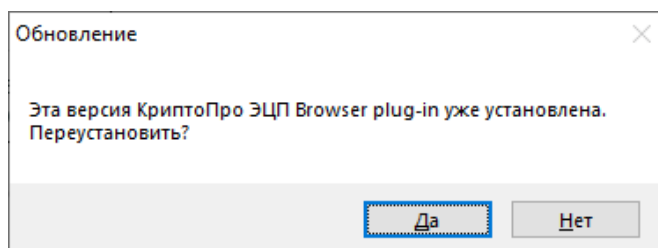
Для завершения установки драйвера нажмите кнопку **«Готово»**.

Установка КриптоПро ЭЦП Browser Plug-in

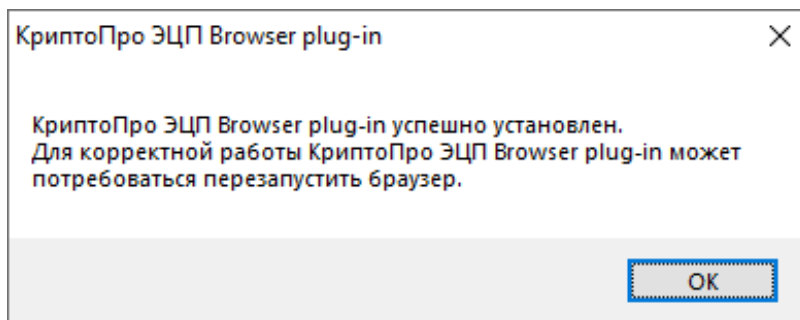
Скачайте [КриптоПро ЭЦП Browser Plug-in](#) и запустите скачанный файл. Нажмите кнопку **«Да»** для установки.



Если на компьютере уже установлен КриптоПро ЭЦП Browser Plug-in, то установщик предложит переустановить программу. Нажмите кнопку **«Да»**.



По клику «**ОК**» начните перезапуск браузера, закрыв браузер и открыв его снова.



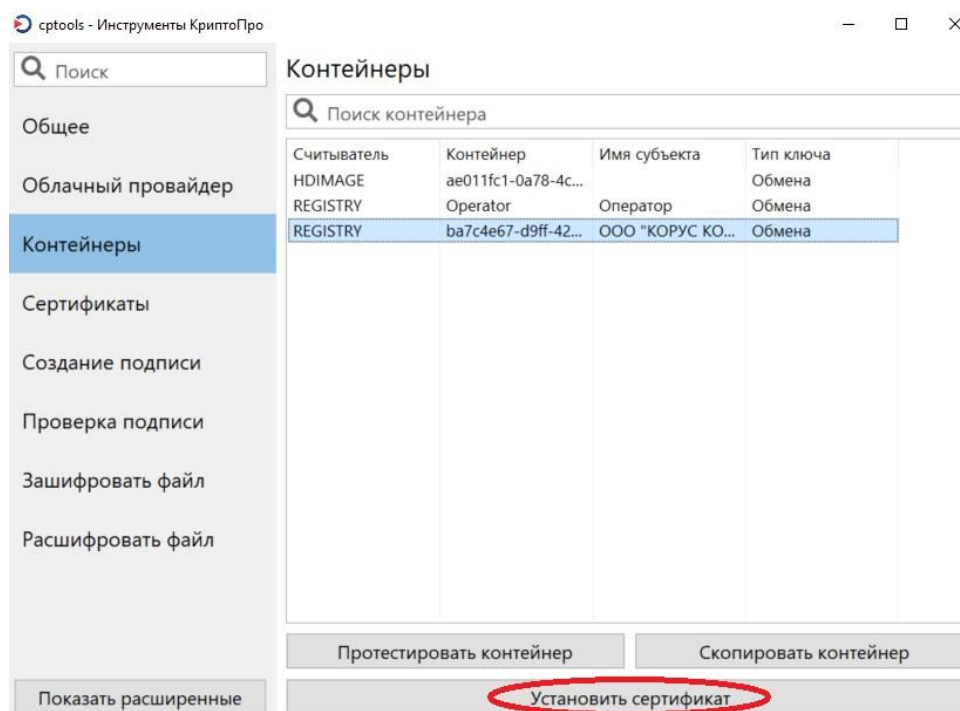
Установка личного сертификата ключа подписи

Перед установкой сертификата ключа подписи необходимо вставить носитель с электронной подписью в USB-порт компьютера.

По клику «**Пуск**» найдите приложение «**Инструменты КриптоПро**» и запустите его.

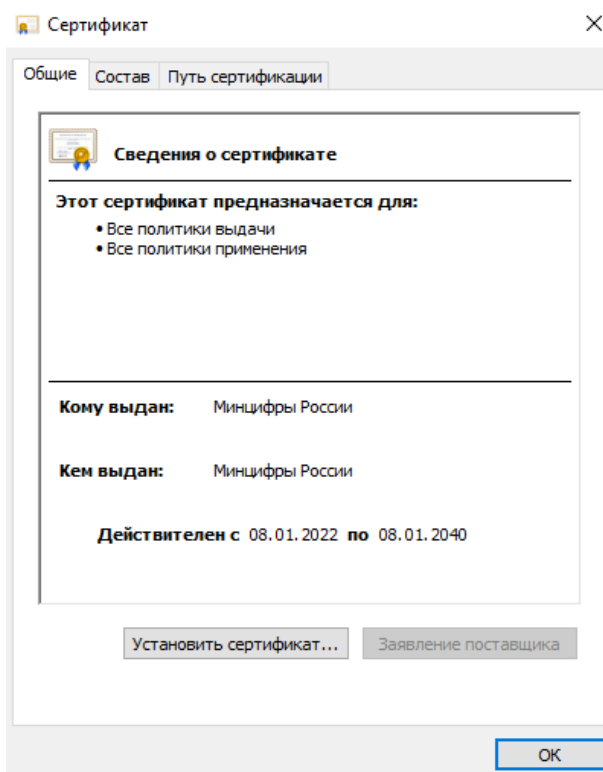
Если приложения нет, то установите КриптоПро CSP

В приложении перейдите в раздел «**Контейнеры**» и найдите контейнер закрытого ключа, затем нажмите кнопку «**Установить сертификат**».

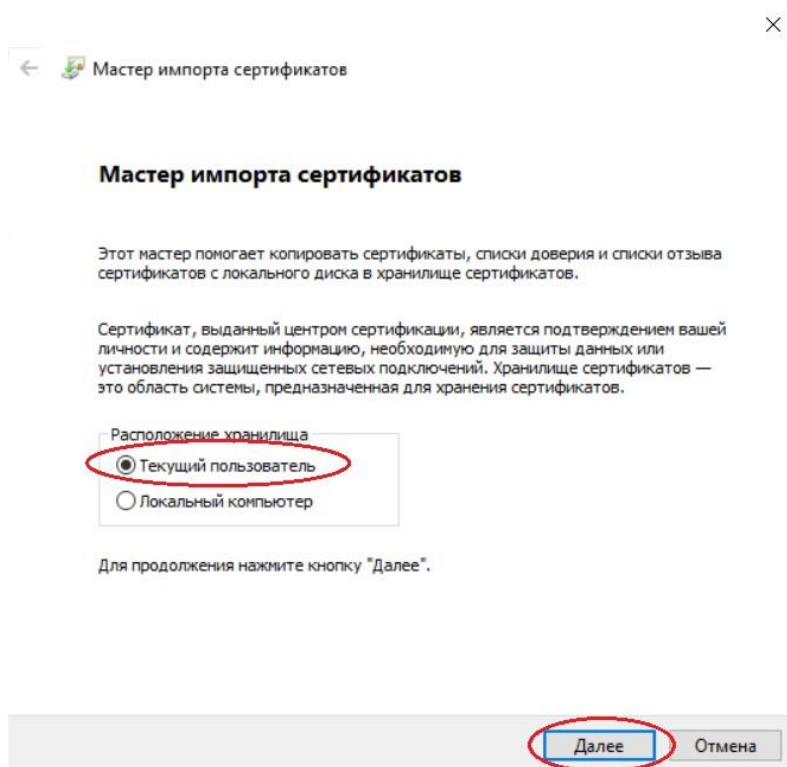


Установка корневого сертификата

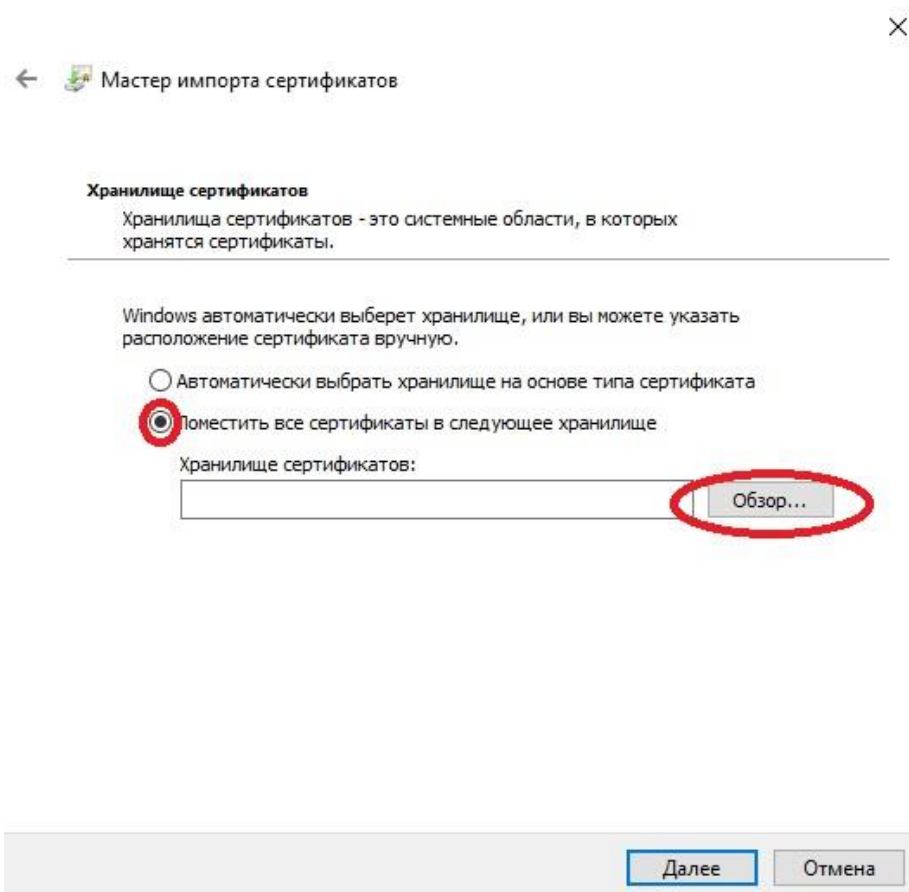
Скачайте и откройте файл [Корневой сертификат Головного удостоверяющего центра - ГОСТ Р 34.10-2012 от 05.05.22](#), в появившемся окне нажмите кнопку «**Установить сертификат**». После этого запустится «**Мастер импорта сертификатов**».



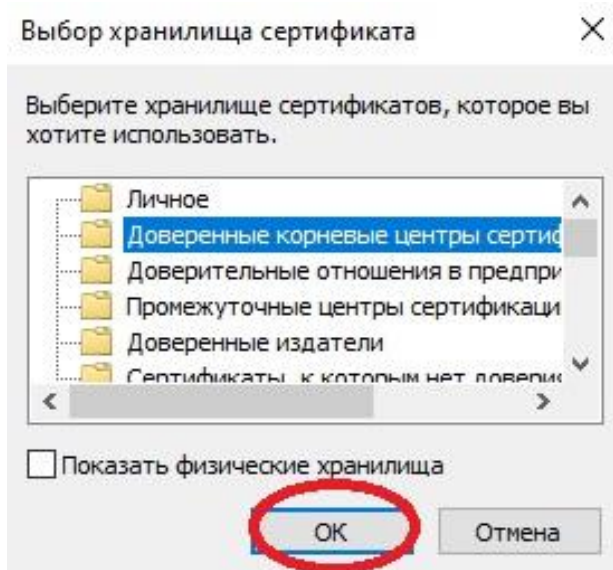
Для продолжения установки выберите расположение хранилища «**Текущий пользователь**». Нажмите «**Далее**».



В появившемся окне, поставьте галочку «**Поместить все сертификаты в следующее хранилище**» и нажмите кнопку «**Обзор**».




В списке хранилищ выберите хранилище «**Доверенные корневые центры сертификации**», нажмите «**ОК**» и «**Далее**».



Для завершения установки сертификата нажмите кнопку «**Готово**». При запросе системы подтвердить доверие данному издателю сертификата, необходимо нажать «**Да**».

Об успешном импорте сертификата в хранилище будет выдано сообщение «**Импорт успешно выполнен**».

Мастер импорта сертификатов

 Импорт успешно выполнен.

OK

Установка сертификата [Доверенный корневой сертификат УЦ ООО «КОРУС Консалтинг СНГ» от 03.08.2023](#) производится аналогично вышеуказанным пунктам, но сертификат устанавливается в хранилище **«Промежуточные центры сертификации»**.

Расширение для браузера CryptoPro Extension for CAES Browser Plug-in

При установке **КриптоПро ЭЦП Browser Plug-in** установите расширение для любого браузера. Для Internet Explorer данное программное обеспечение не доступно. Убедитесь, что расширение есть и включено. Перейдите в расширения вашего браузера. Для этого в новой вкладке введите соответствующий браузеру адрес и нажмите на кнопку **«Enter»**:

- **Chrome** – chrome://extensions/;
- **Firefox** – about:addons;
- **Opera** – opera://extensions/;
- **Yandex** – browser://tune/.

Найдите расширение **CryptoPro Extension for CAES Browser Plug-in** и убедитесь, что оно включено. Если расширения нет, то перейдите на его страницу и установите расширение для браузера:



Чтобы проверить работу электронной подписи, перейдите на [сайт проверки работы плагина КриптоПро](#) и нажмите кнопку **«Да»** в окне подтверждения доступа. Затем выберите сертификат и нажмите **«Подписать»**.

Данные для подписи:

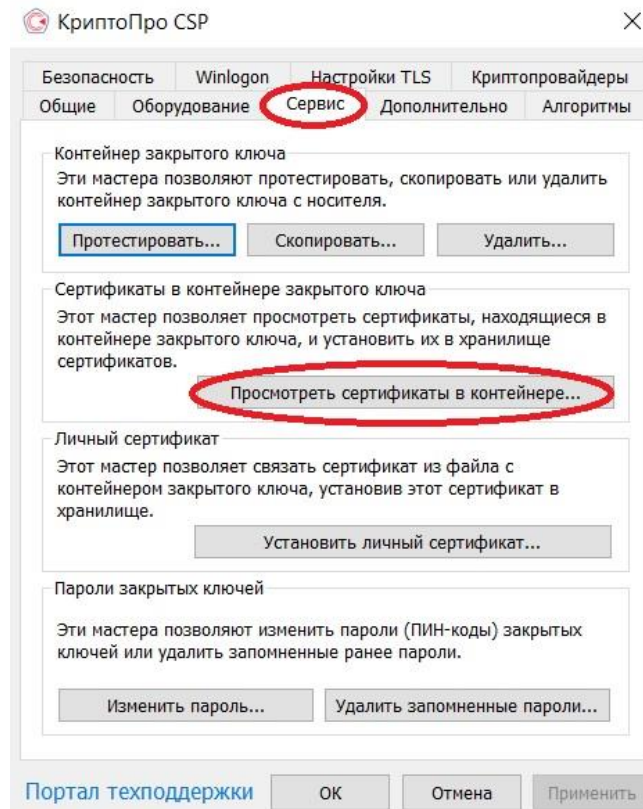
Hello World

Подписать

Экспорт сертификата для загрузки во внешнюю систему

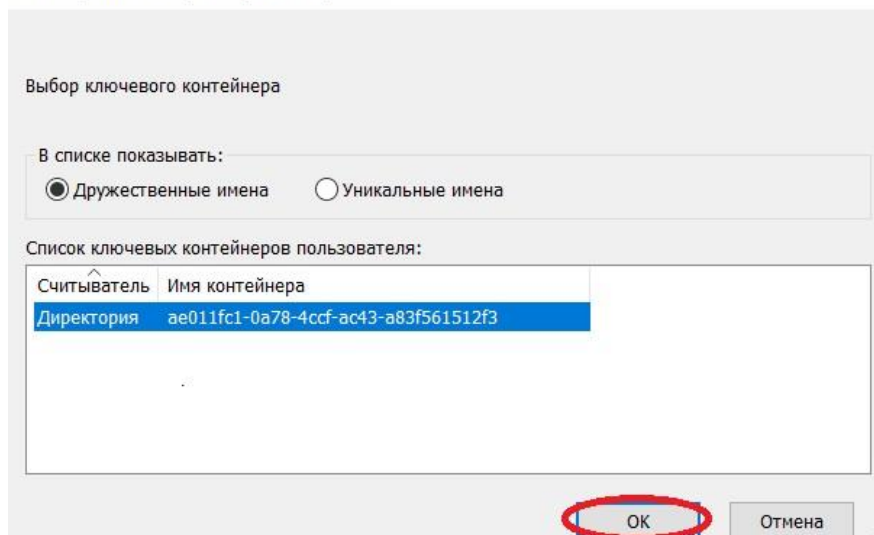
Если в системе есть требования по экспорту сертификата, то необходимо запустить **«КриптоПро CSP»**. Для этого перейдите в меню **«Пуск»**, далее **«Панель управления»** и выберите **«КриптоПро CSP»**.

Затем на вкладке «Сервис» нажмите кнопку «Просмотреть сертификаты в контейнере».

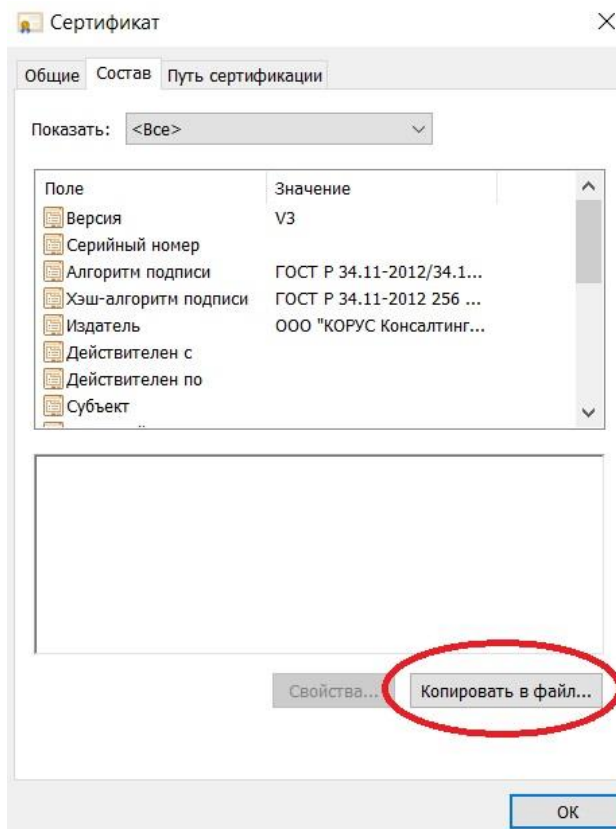


В открывшемся окне нажмите кнопку «Обзор». В списке ключевых носителей выберите личный сертификат и нажмите «ОК».

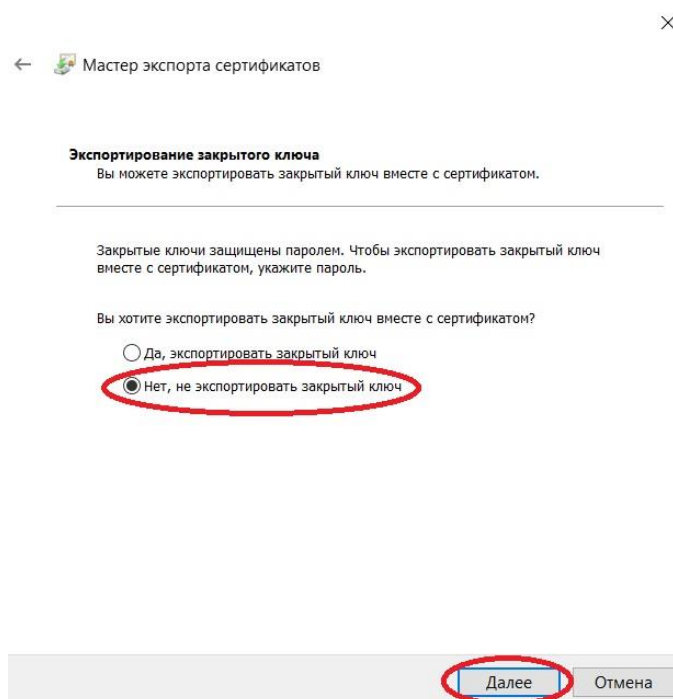
Выбор контейнера - КриптоПро CSP



В окне с информацией о выбранном сертификате нажмите кнопку «Свойства». На вкладке «Состав» нажмите кнопку «Копировать в файл».



После этого запустится «**Мастер экспорта сертификатов**». Для продолжения установки нажмите «**Далее**». В окне экспортирования закрытого ключа выберите вариант «**Нет, не экспортировать закрытый ключ**» и нажмите «**Далее**».



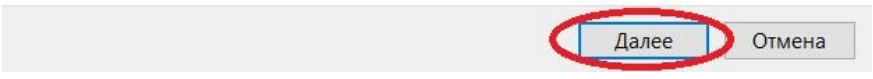
Выберите формат файла сертификата – **Файлы X.509 (.CER) в кодировке DER** – и нажмите «**Далее**».

Формат экспортируемого файла

Сертификаты могут быть экспортированы в различных форматах.

Выберите формат, который вы хотите использовать:

- Файлы X.509 (.CER) в кодировке DER
- Файлы X.509 (.CER) в кодировке Base-64
- Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)
 - Включить по возможности все сертификаты в путь сертификации
- Файл обмена личной информацией - PKCS #12 (.PFX)
 - Включить по возможности все сертификаты в путь сертификации
 - Удалить закрытый ключ после успешного экспорта
 - Экспортировать все расширенные свойства
 - Включить конфиденциальность сертификата
- Хранилище сериализованных сертификатов (.SST)



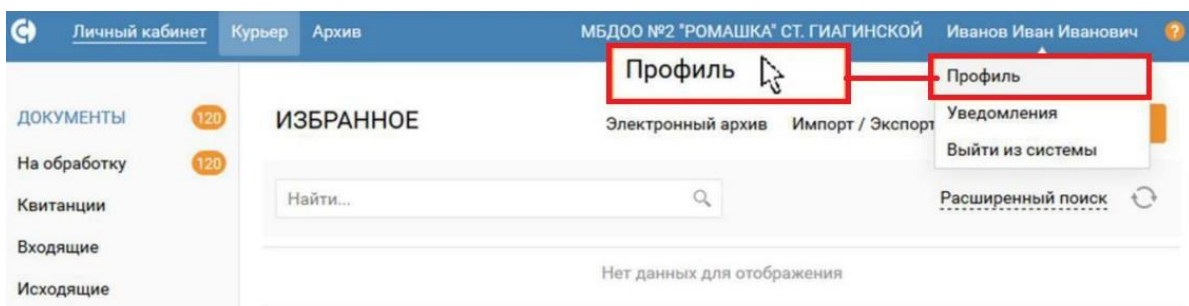
Чтобы добавить место для хранения экспортируемого файла, нажмите **«Обзор»** и выберите место для хранения. Задайте имя произвольно и нажмите **«Сохранить»**. Для продолжения работы мастера нажмите **«Далее»**. Завершите работу мастера экспорта сертификатов по клику **«Готово»**. Появится сообщение о том, что экспорт выполнен. Нажмите **«ОК»**.

Экспорт успешно выполнен.



Загрузка сертификата в сервис СФЕРА Курьер

В Сервисе СФЕРА Курьер наведите курсор на пользователя и нажмите кнопку **«Профиль»**.



Перейдите во вкладку «**Электронные подписи**» и нажмите кнопку «**Загрузить**», выберите ранее сохранённый **файл сертификата (*.cer)**.

