# СберБизнес

Установка и настройка компонентов для работы во внешних системах с электронной подписью в мобильном приложении СберПодпись Про

Для настройки рабочего места на компьютере локального пользователя должно быть установлено следующее программное обеспечение:

- Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003 и выше, Windows Server 2008 и выше, Windows Server 2012 и выше;
- интернет-браузер Chrome, Firefox, Opera, Yandex или Internet Explorer;

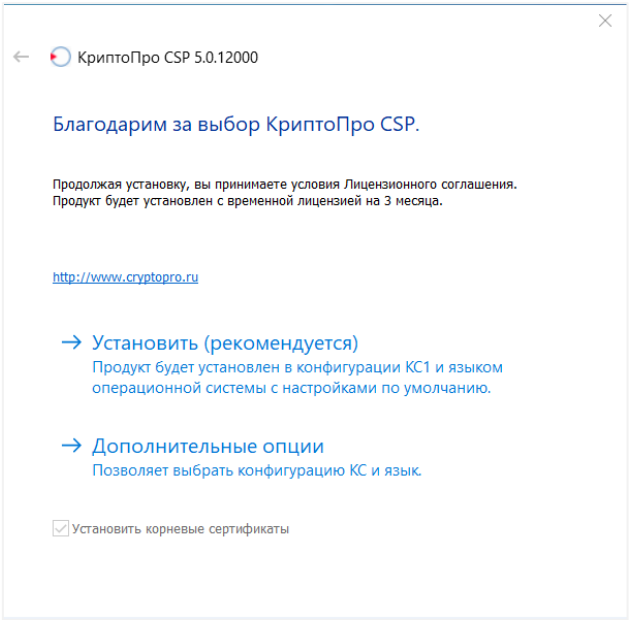
> Дополнительные требования к браузеру или системе зависят от электронного сервиса или портала для работы с электронной подписью.

- СКЗИ КриптоПро CSP версии 5.0 R2 и выше при наличии сертифицированных версий. Работа мобильного приложения с электронной подписью во внешних системах на других версиях невозможна;
- КриптоПро ЭЦП Browser plug-in версии 2.0;
- доступ в интернет.

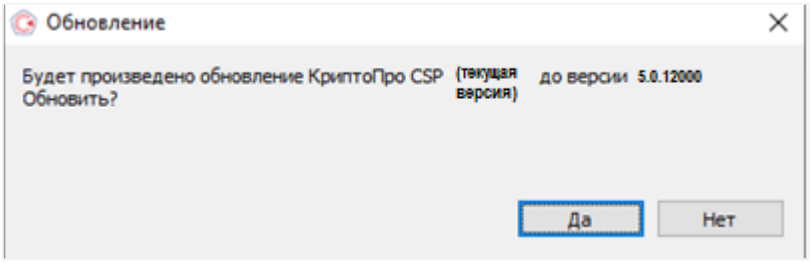
> Для установки вышеуказанных компонентов необходимы права администратора локального пользователя на рабочем месте.

## 1 Установите средство криптографической защиты информации КриптоПро CSP 5.0

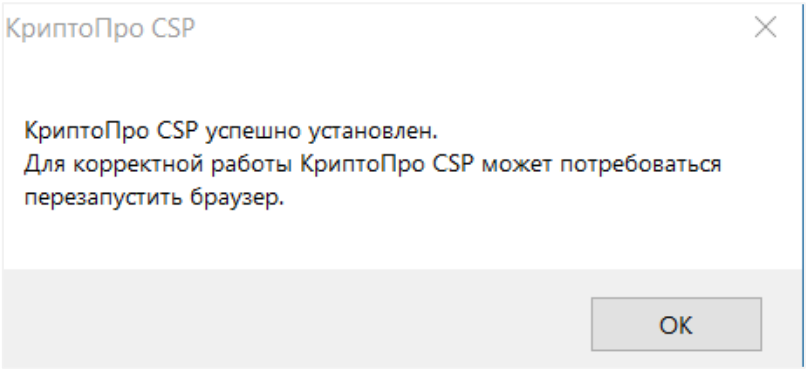
Скачайте и запустите файл для установки КриптоПро CSP 5.0, имя которого начинается с CSPSetup. В открывшемся окне нажмите кнопку **Установить.** После этого начнётся установка КриптоПро CSP, и компьютер перезагрузится.



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. В процессе установки компьютер будет перезагружен.



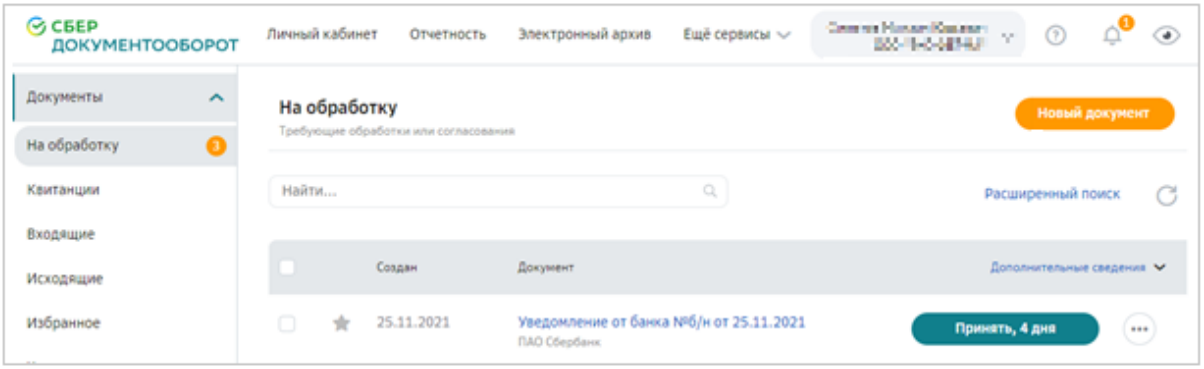

По клику **ОК** подтвердите завершение установки.



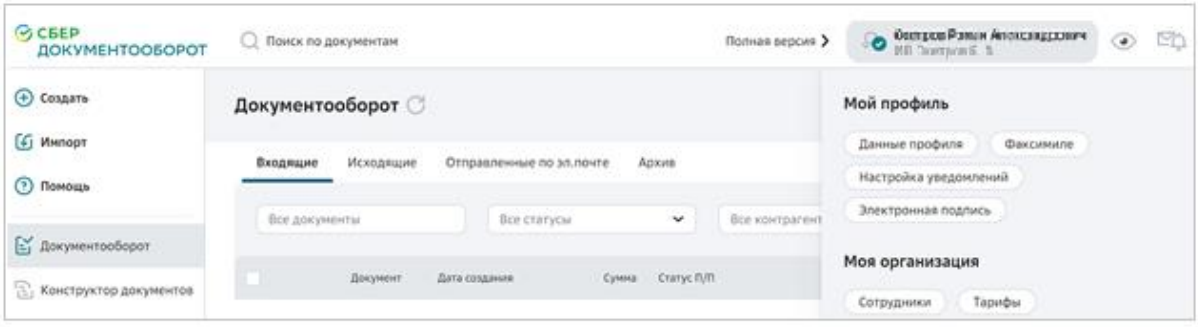

> При первой установке КриптоПро CSP устанавливается его временная лицензия на три месяца. По истечении и (или) при отсутствии введённой лицензии необходимо приобрести постоянную лицензию в удостоверяющем центре, в т. ч. СберКОРУС. Без неё использование сертификата во внешних системах невозможно.
>
> Для штатной эксплуатации средств СКЗИ КриптоПро CSP должно быть установлено с дистрибутива.

## 2 Настройте КриптоПро CSP 5.0

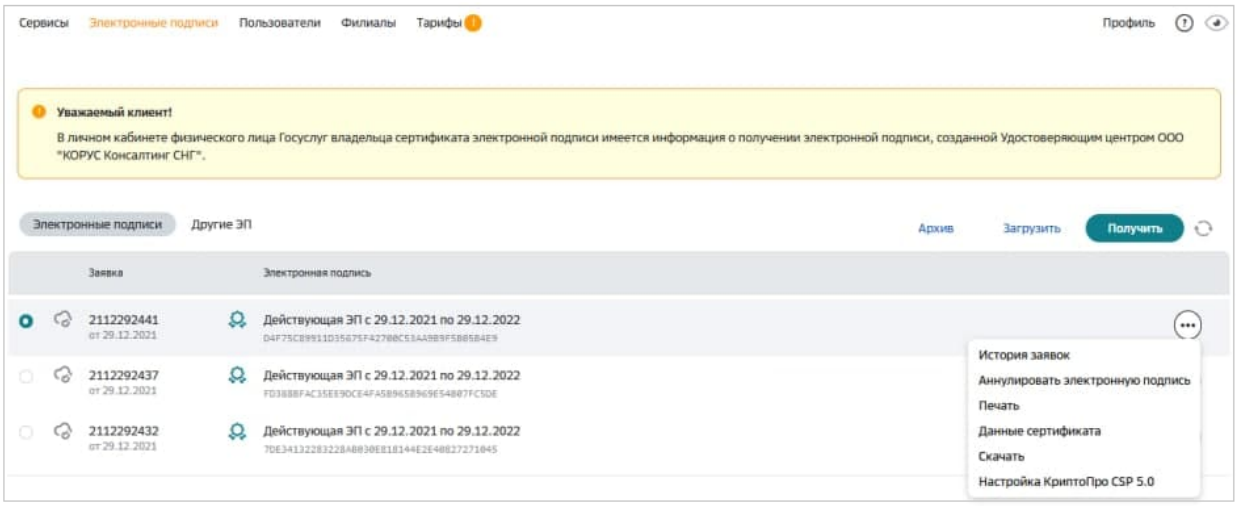
В СберБизнес в меню слева выберите раздел **Документооборот** и перейдите в сервис. Перейдите на вкладку **Личный кабинет**.



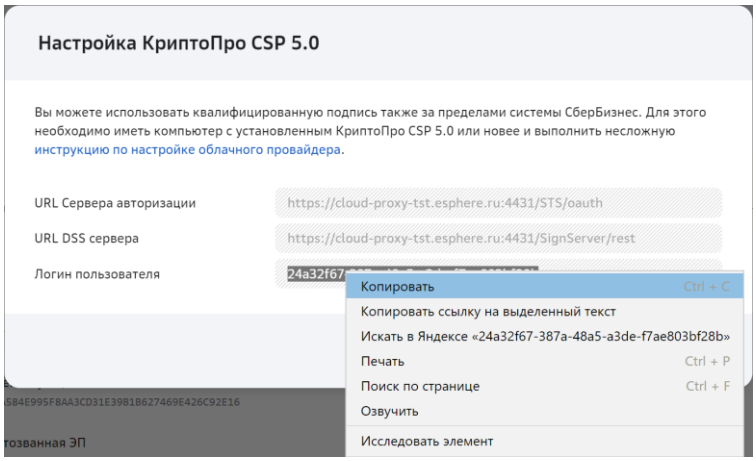
Если у вас упрощённая версия сервиса «Документооборот», в правом верхнем углу нажмите на название организации и выберите **Электронную подпись** или **Данные профиля.**



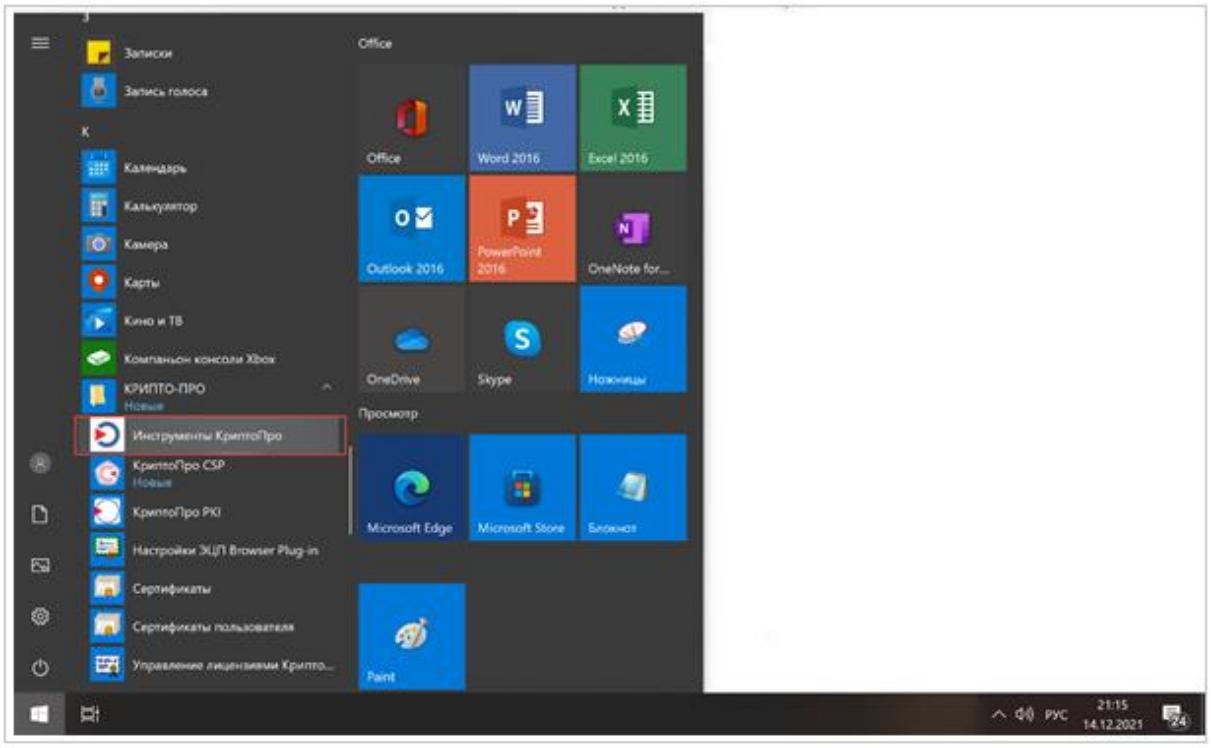

На вкладке **Электронная подпись** нажмите кнопку дополнительных действий ••• в строке с действующей активной электронной подписью, выпущенной в мобильном приложении СберПодпись Про, и выберите пункт **Настройка КриптоПро CSP 5.0**.




Скопируйте значение в поле **Логин пользователя.** Для этого выделите значение в строке, кликните правой кнопкой мыши и выберите пункт **Копировать.**



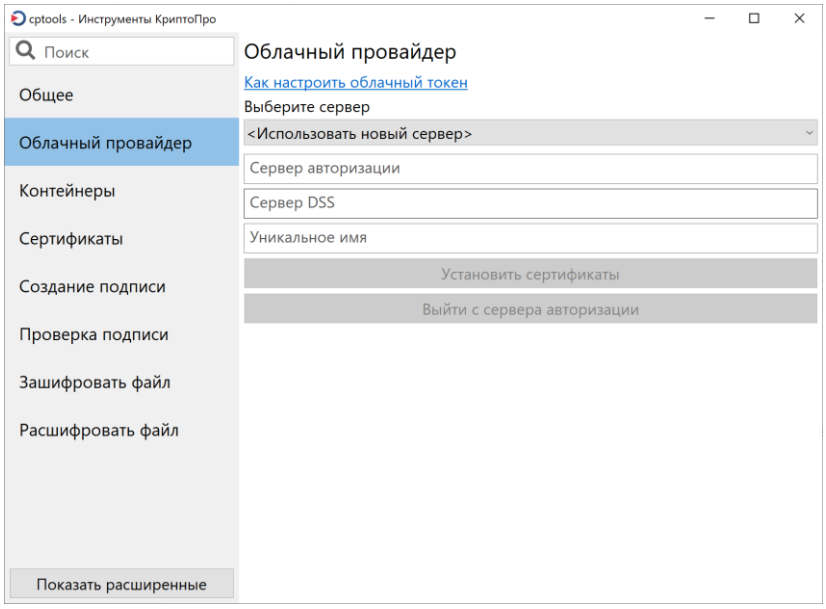

В левом нижнем меню экрана откройте меню **Пуск** и выберите программу **Инструменты КриптоПро,** не закрывая сервис «Документооборот».



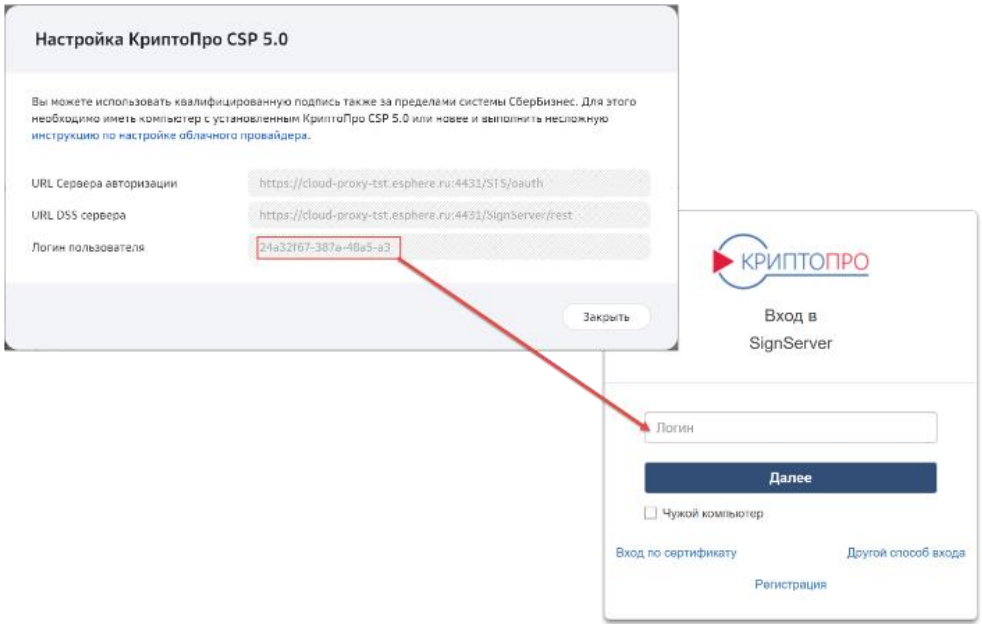

На вкладке **Облачный провайдер** заполните поля формы:

1. В поле **Выберите сервер** выберите значение «Использовать новый сервер».
2. В поле **Сервер авторизации** введите значение: https://cloud-ca.esphere.ru:4431/STS/oauth.
3. В поле **Сервер DSS** введите значение: https://cloud-ca.esphere.ru:4431/SignServer/rest.
4. В поле **Уникальное имя** придумайте и введите уникальное название для созданных настроек. После установки настроек они будут сохранены, и вы сможете выбрать их из списка по заданному имени в поле **Выберите сервер.**

Нажмите кнопку **Установить сертификаты.**

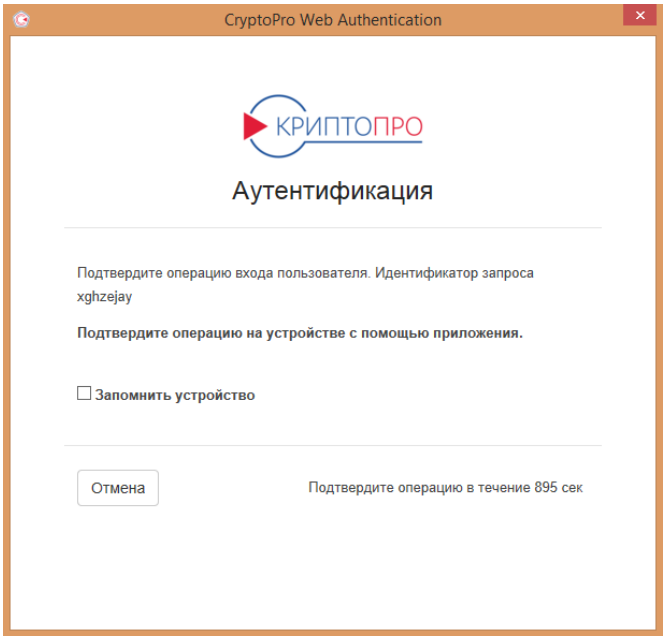


В мобильном приложении СберПодпись Про введите логин, ранее скопированный в поле **Логин пользователя** в сервисе «Документооборот», и нажмите кнопку **Далее**.




Войдите в мобильное приложение СберПодпись Про для подтверждения входа. В разделе **Документы** откройте документ, который необходимо подписать.

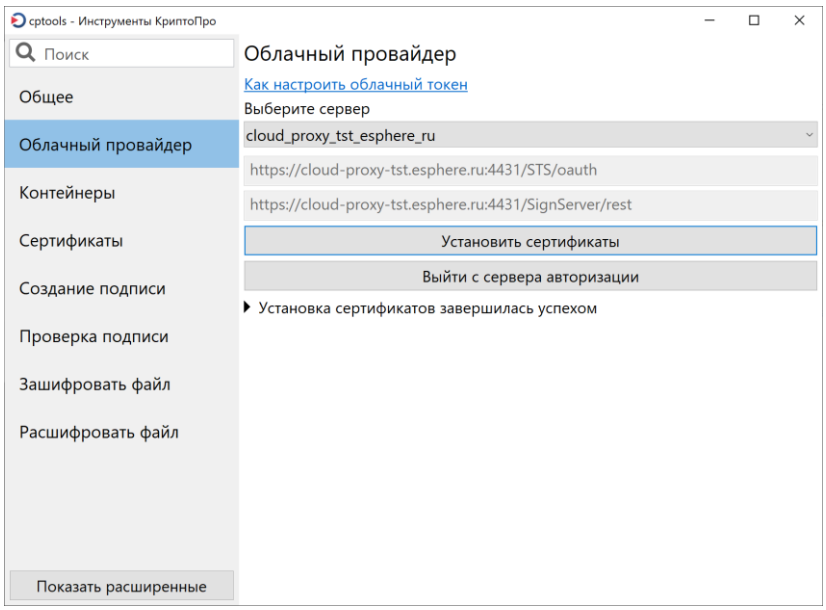

Проверьте идентификатор сессии на компьютере и в мобильном приложении. Если всё верно, нажмите **Подтвердить**.





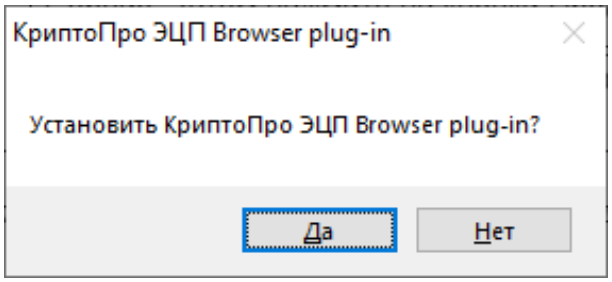
Чтобы подписать документ, введите ПИН-код, который был задан при установке мобильного приложения.


После подтверждения операции начнётся автоматическая установка сертификата на компьютере.

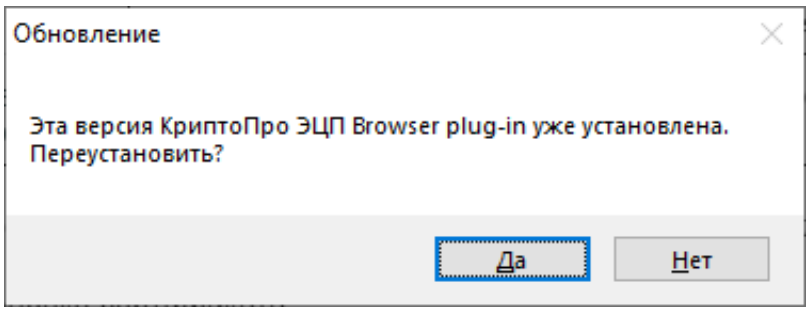



## 3 Установите КриптоПро ЭЦП Browser Plug-in

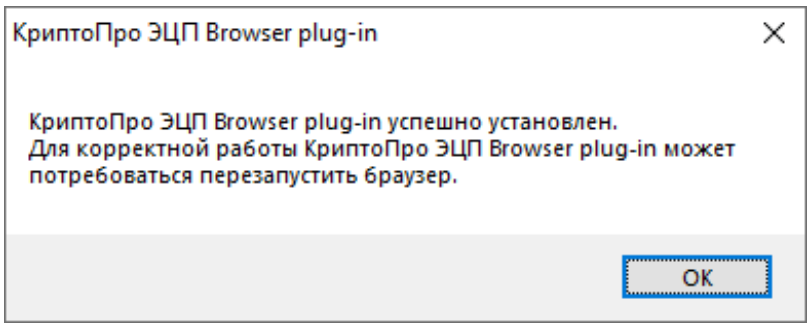
Скачайте КриптоПро ЭЦП Browser Plug-in на ваш компьютер и запустите скачанный файл cadesplugin.exe, нажав **Да.**




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.




## 4 Включите CryptoPro Extension for CAdES Browser Plug-in для браузера

При установке КриптоПро ЭЦП Browser Plug-in установите расширение для любого браузера. Для Internet Explorer данное программное обеспечение недоступно. Убедитесь, что расширение есть и включено.

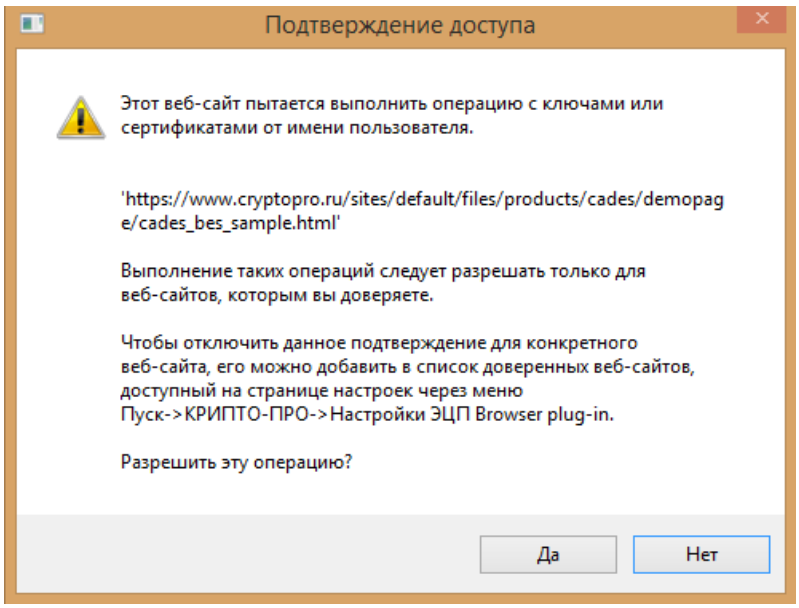
Перейдите в расширения вашего браузера. Для этого в новой вкладке введите соответствующий браузеру адрес и нажмите на кнопку **Enter**:

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

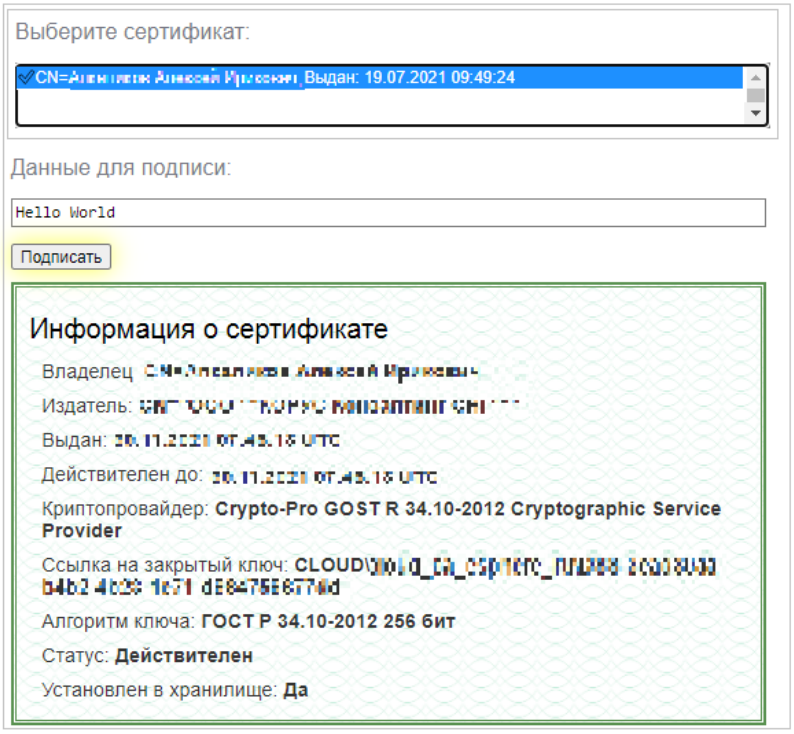
Найдите расширение **CryptoPro Extension for CAdES Browser Plug-in** и убедитесь, что оно включено. Если расширения нет, то перейдите на его страницу и установите расширение для браузера:

- Chrome;
- Firefox;
- Opera;
- Yandex.

Чтобы проверить работу электронной подписи, перейдите на сайт КриптоПро и нажмите кнопку **Да.**



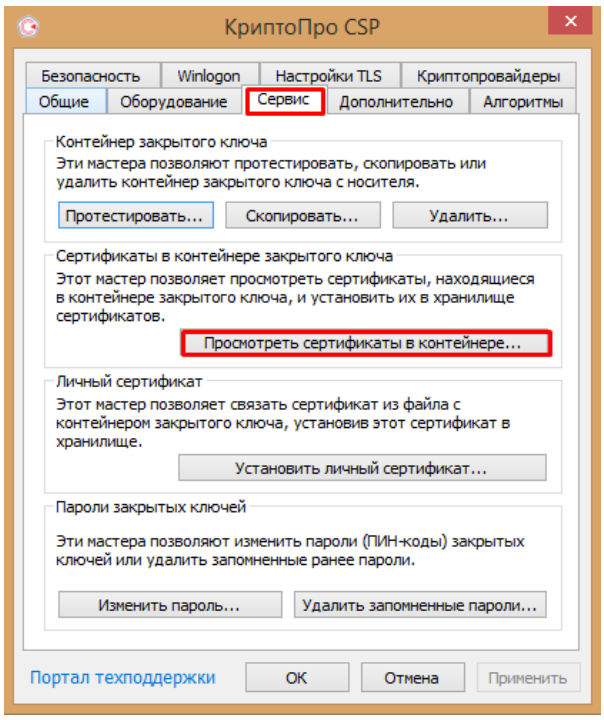

Затем выберите сертификат и нажмите **Подписать**.



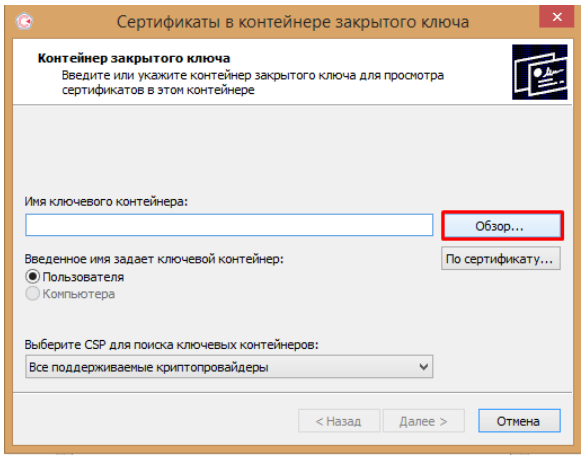

## 5 Экспортируйте сертификат с ключевого носителя для загрузки во внешнюю систему

Если во внешней системе (операторы ЭДО, операторы сдачи отчётности и др.) требуется загрузка сертификата ключа проверки электронной подписи (.cer), то для экспорта сертификата необходимо запустить **КриптоПро CSP.** Для этого перейдите в меню **Пуск,** далее **Панель управления** и выберите **КриптоПро CSP.**

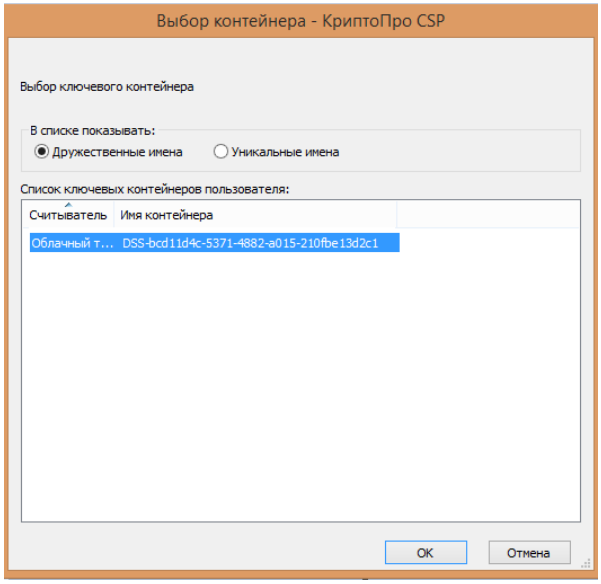
Затем на вкладке **Сервис** нажмите кнопку **Просмотреть сертификаты в контейнере.**



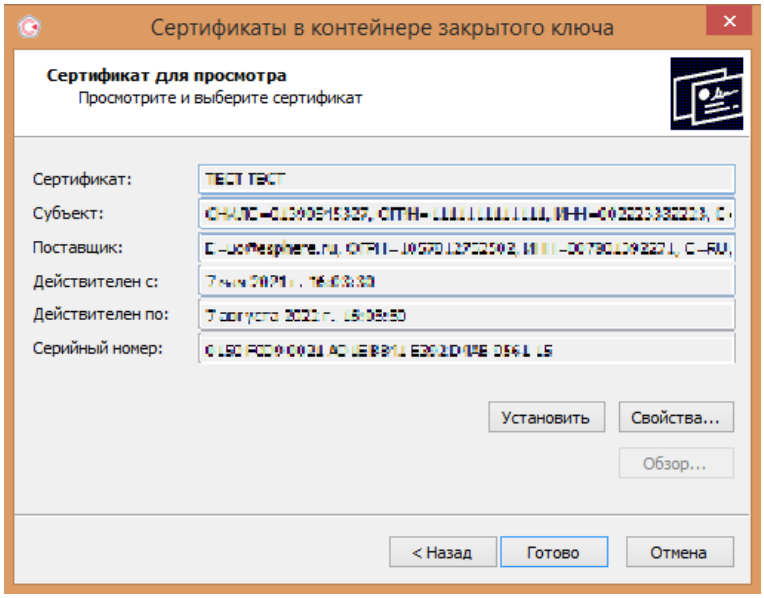

В открывшемся окне нажмите **Обзор.**



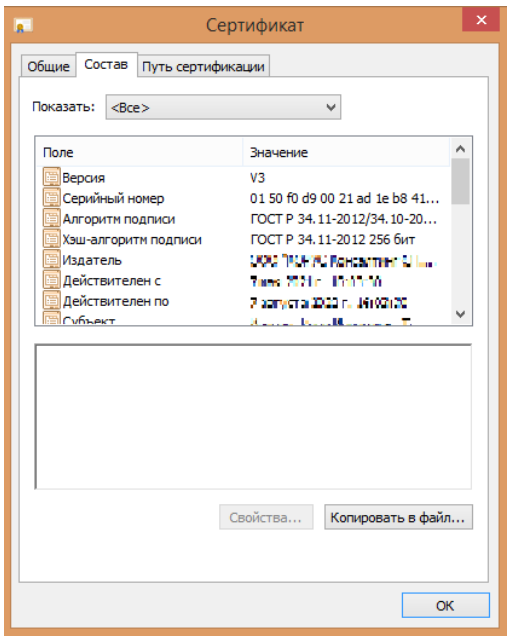

В списке ключевых носителей выберите личный сертификат на считывателе «**Облачный токен**» и нажмите **ОК.**



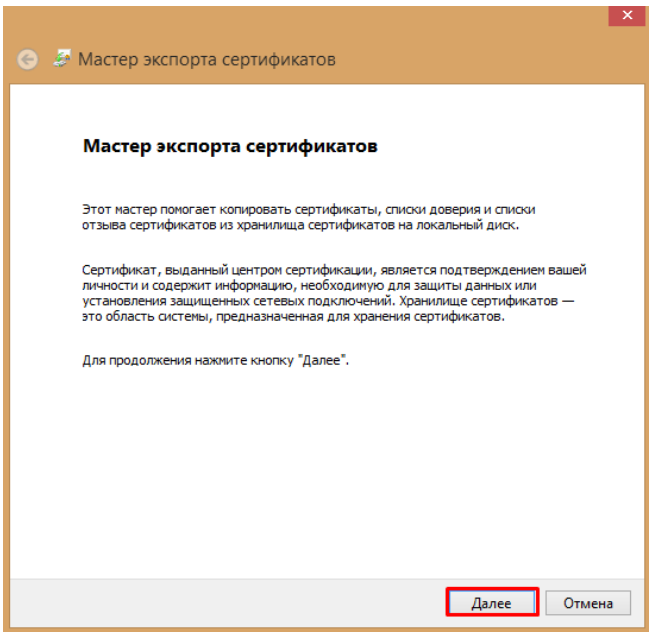
В окне с информацией о выбранном сертификате нажмите кнопку **Свойства.**



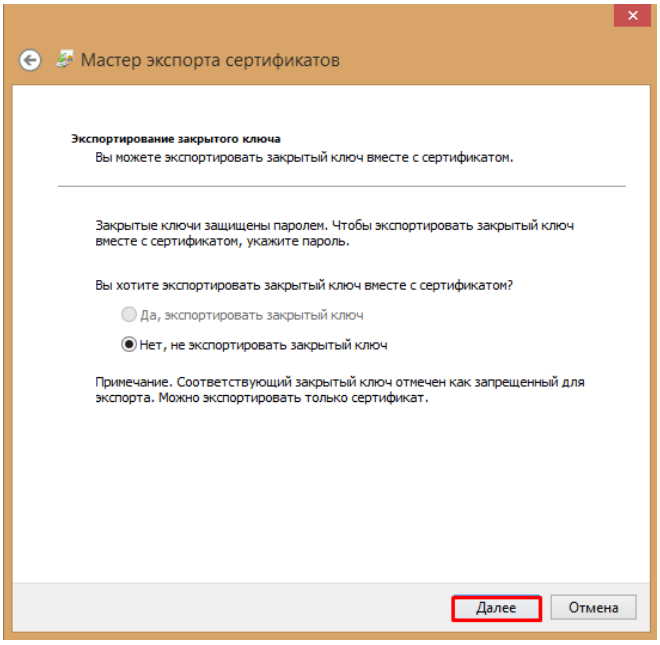

На вкладке **Состав** нажмите кнопку **Копировать в файл.**



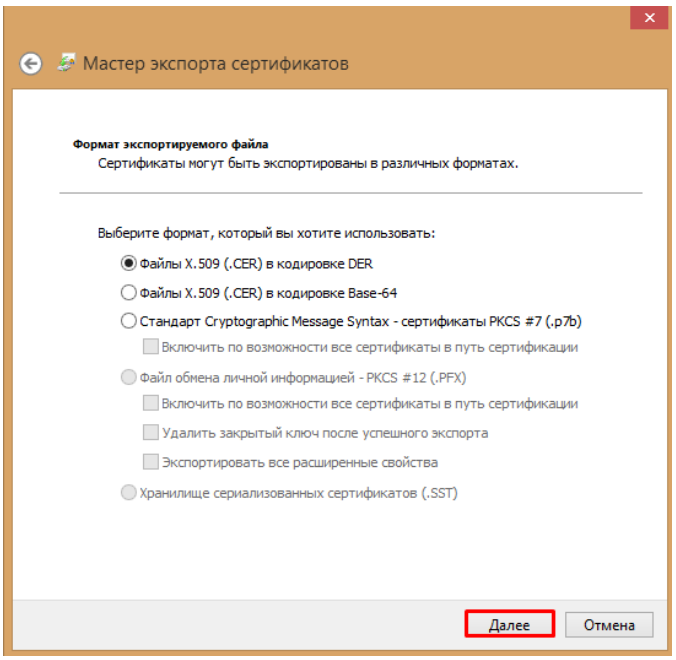

После этого запустится «Мастер экспорта сертификатов». Для продолжения установки нажмите **Далее.**



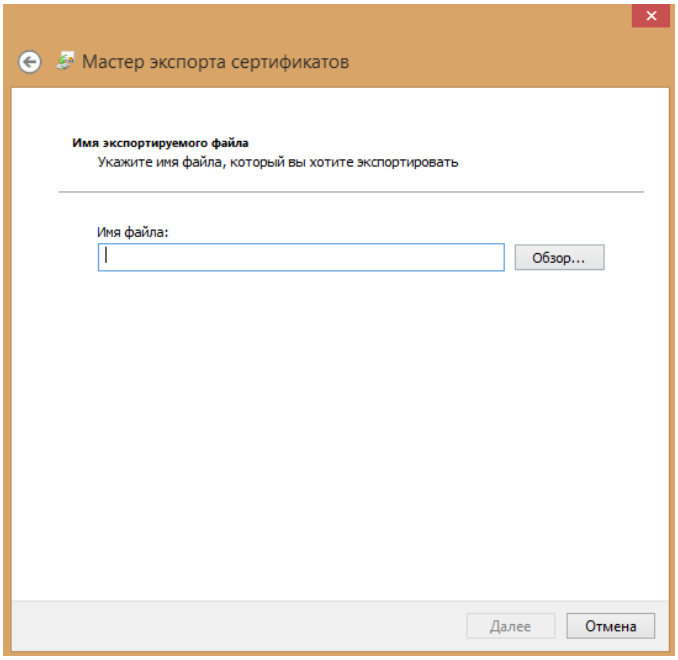

В окне экспортирования закрытого ключа выберите вариант **«Нет, не экспортировать закрытый ключ»** и нажмите **Далее.**



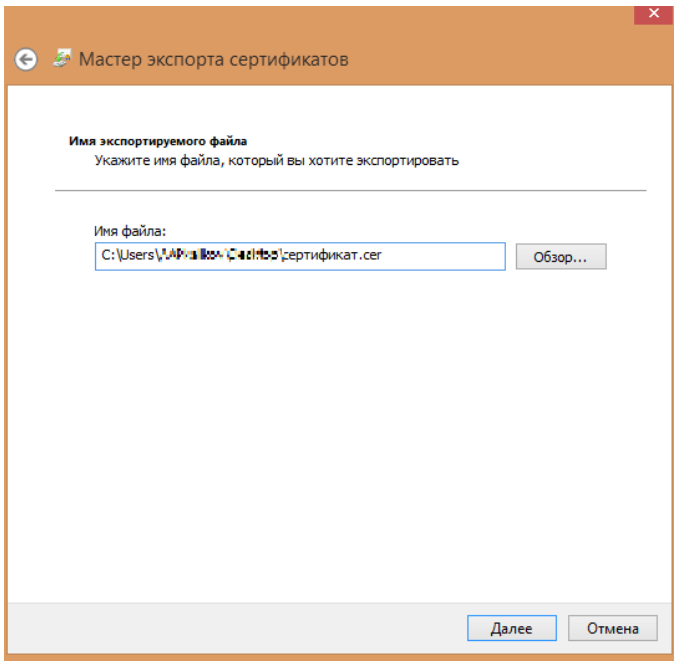

Выберите формат файла сертификата – **Файлы X.509 (.CER) в кодировке DER** – и нажмите **Далее.**



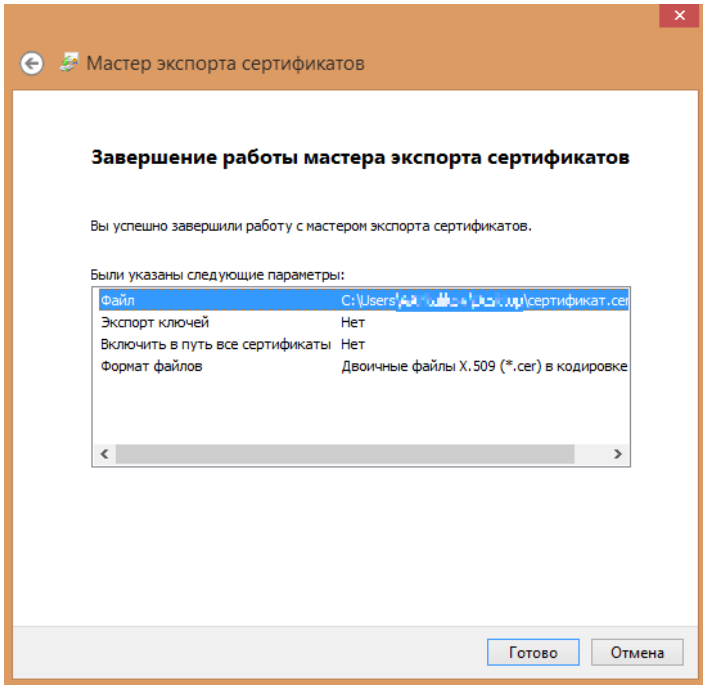

Чтобы добавить место для хранения экспортируемого файла, нажмите **Обзор** и выберите место для хранения. Задайте имя произвольно и нажмите **Сохранить.**




Для продолжения работы мастера нажмите **Далее.**




Завершите работу мастера экспорта сертификатов по клику **Готово.**




Подтвердите завершение экспорта сертификата по клику **ОК.**