

Необходимое программное обеспечение(ПО), которое должно быть установлено на рабочем месте

- драйверы для используемого ключевого носителя (Рутокен, JaCarta и т.д.);
- СКЗИ «КриптоПро CSP» версии 5 и выше;
- плагин КриптоПро ЭЦП Browser Plug-in;
- расширение для браузера;
- корневые сертификаты УЦ;
- личный сертификат ключа электронной подписи, выданный УЦ;
- расширение крипто-плагина для используемого интернет-браузера(если необходимо).

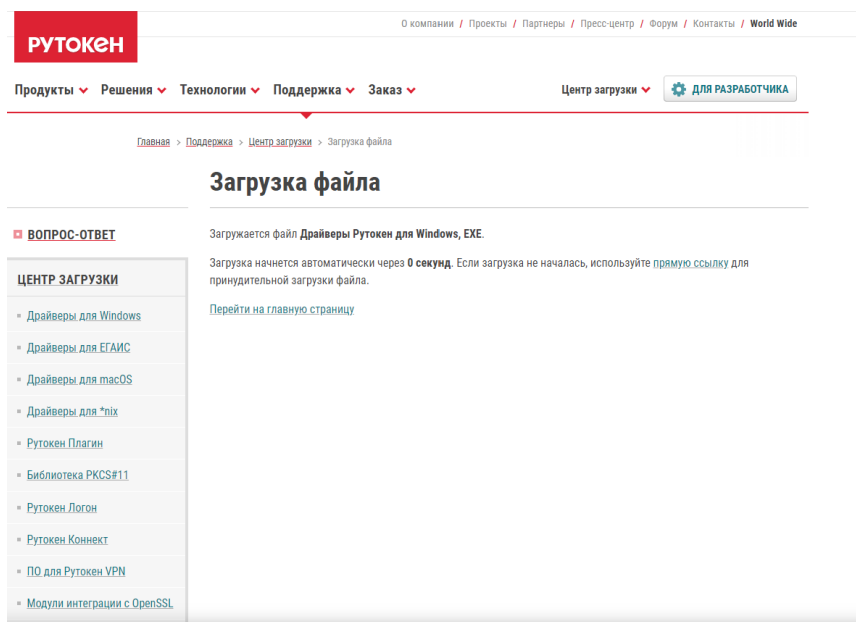
Инструкция для пользователя, на случай, если вышеперечисленные ПО не было установлено на рабочем месте.

Установка драйверов ключевого носителя.

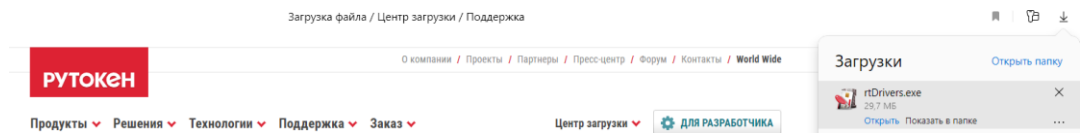
Определите визуально или с помощью имеющихся документов тип носителя, на который записана электронная подпись.

В зависимости от типа носителя скачайте необходимый установочный пакет:

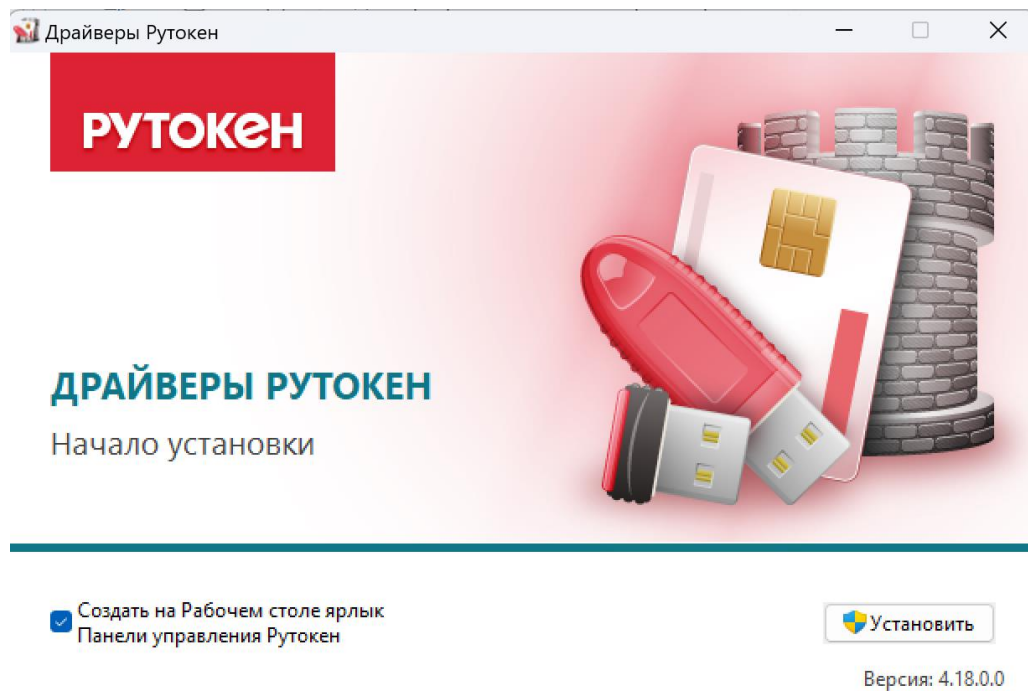
Rutoken – <https://www.rutoken.ru/support/download/get/rtDrivers-exe.html>



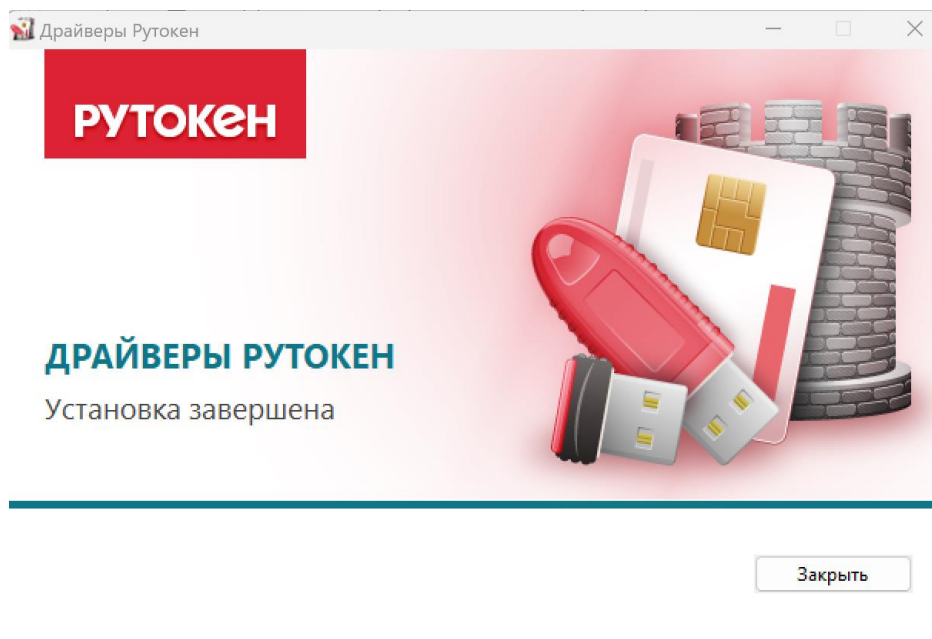
Запустите скачанный установочный пакет драйвера носителя из папки загрузки.



Установите драйвера устройств в режиме по умолчанию, последовательно нажимая кнопки «Установить», «Далее».



Дождитесь завершения установки и нажмите кнопку «Закреть».



Установка КриптоПро CSP 5.0

Скачайте установочный пакет КриптоПро CSP. Для этого перейдите по ссылке: https://cryptopro.ru/fns_experiment

Открывшуюся страницу пролистайте вниз и заполните форму.

Покупка лицензии

Необходимо выбрать подходящий вариант

Введите необходимые сведения и нажмите кнопку «Скачать».

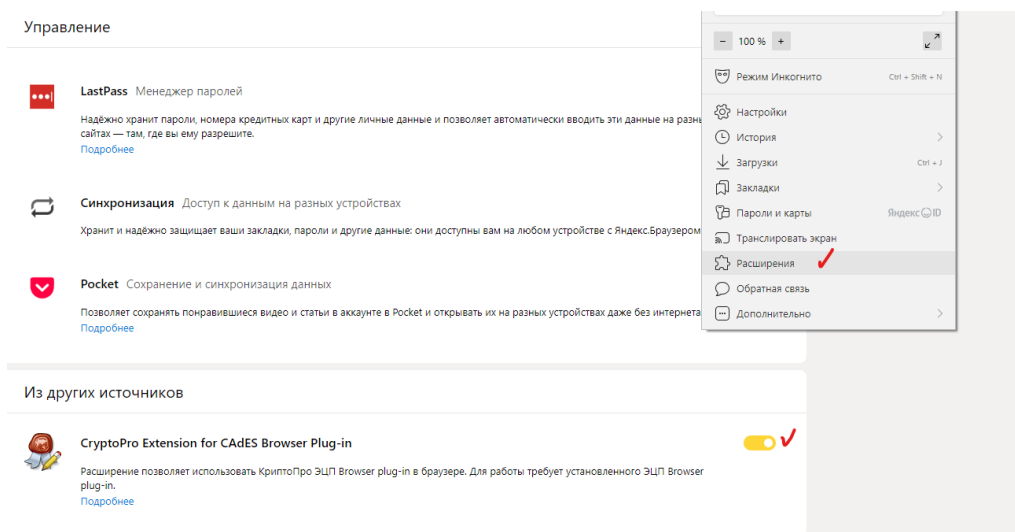
Загруженный пакет включает в себя инсталлятор КриптоПро CSP и плагина КриптоПро ЭЦП Browser Plug-in. Установите КриптоПро CSP и плагин КриптоПро ЭЦП Browser Plug-in.

Плагин КriptoПро ЭЦП Browser Plug-in можно загрузить отдельно по ссылке https://www.cryptopro.ru/products/cades/plugin/get_2_0. В скаченном инсталляционном пакете необходимо запустить файл cadesplugin.exe. После окончания установки КriptoПро ЭЦП Browser plug-in нажмите ОК.

Дальнейшие настройки различаются в зависимости от используемого браузера.

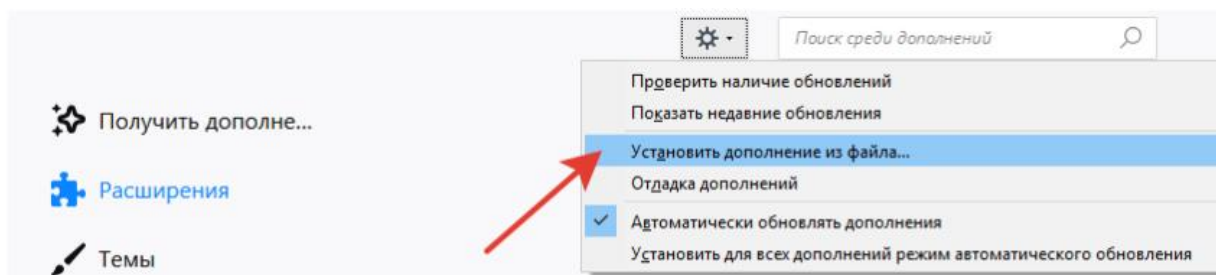
Браузер Chrome: запустите браузер и дождитесь оповещения об установленном расширении "CryptoPro Extension for CAdES Browser Plug-in". Включите это расширение. Если на Вашем компьютере ранее уже выполнялась установка расширения CryptoPro Extension for CAdES Browser Plug-in, а потом оно было удалено, его потребуется установить отдельно. Для этого перейдите по ссылке:

<https://chrome.google.com/webstore/detail/cryptopro-extension-for-cadefhfhfnnmpdbibifmljnfjhpififfog> и установите расширение из интернет-магазина Chrome. Убедитесь, что расширение включено на странице расширений.



Браузер Opera или Яндекс.Браузер: расширение доступно по ссылке: <https://addons.opera.com/ru/extensions/details/cryptopro-extension-for-cades-browser-plugin/>

Браузер Firefox: скачайте расширение по ссылке: https://www.cryptopro.ru/sites/default/files/products/cades/extensions/firefox_cryptopro_extension_latest.xpi и установите в браузер самостоятельно.



Проверьте корректность установки на странице проверки плагина https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html.

Для этого в открывшемся окне подтвердите доступ путем нажатия кнопки "Да".



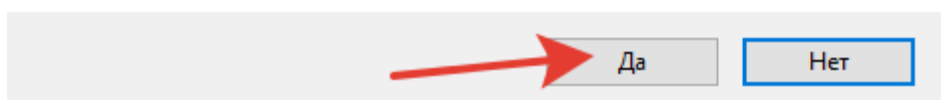
Этот веб-сайт пытается выполнить операцию с ключами или сертификатами от имени пользователя.

'<https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html>'

Выполнение таких операций следует разрешать только для веб-сайтов, которым вы доверяете.

Чтобы отключить данное подтверждение для конкретного веб-сайта, его можно добавить в список доверенных веб-сайтов, доступный на странице настроек через меню Пуск->КРИПТО-ПРО->Настройки ЭЦП Browser plug-in.

Разрешить эту операцию?



Если установка КриптоПро ЭЦП Browser plug-in прошла успешно, появится окно с надписью "Плагин загружен", указанием его версии и используемой Вами версии КриптоПро CSP.

На странице https://cryptopro.ru/fns_experiment также можно скачать руководство по установке вышеперечисленного ПО для различных операционных систем и расширения криптоплагина для интернет-браузеров.

Необходимо обязательно проверить что бы плагин был включен!

Включение плагина (если он ранее был установлен) осуществляется в блоке Настройки - Расширение

Управление расширениями



Включены



Контур.Расширение

Расширение для сервиса Диагностики и выполнения криптографических операций в серв...



CryptoPro Extension for CAdES Browser Plug-in

Расширение позволяет использовать КриптоПро ЭЦП Browser plug-in в браузере. Для ра...



Каталог Opera



КриптоПро ЭЦП [Инструкция по настройке](#)

Позволяет создавать и проверять электронные подписи для торгов, банкинга и подачи отчетности в ФНС, Росстат и другие органы.

[Подробнее](#)



Все расширения



CryptoPro Extension for CAdES Browser Plug-in

Расширение позволяет использовать
КриптоПро ЭЦП Browser plug-in в браузере.
Для работы требует установленного ЭЦП

Сведения

Удалить



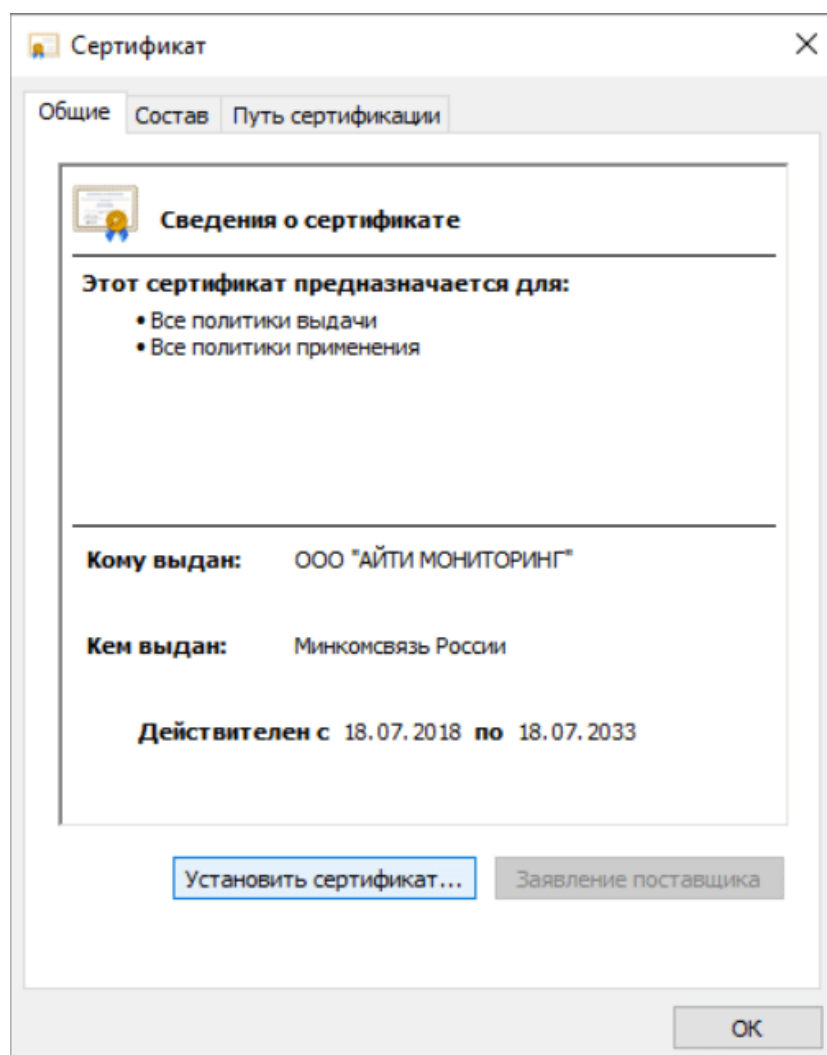
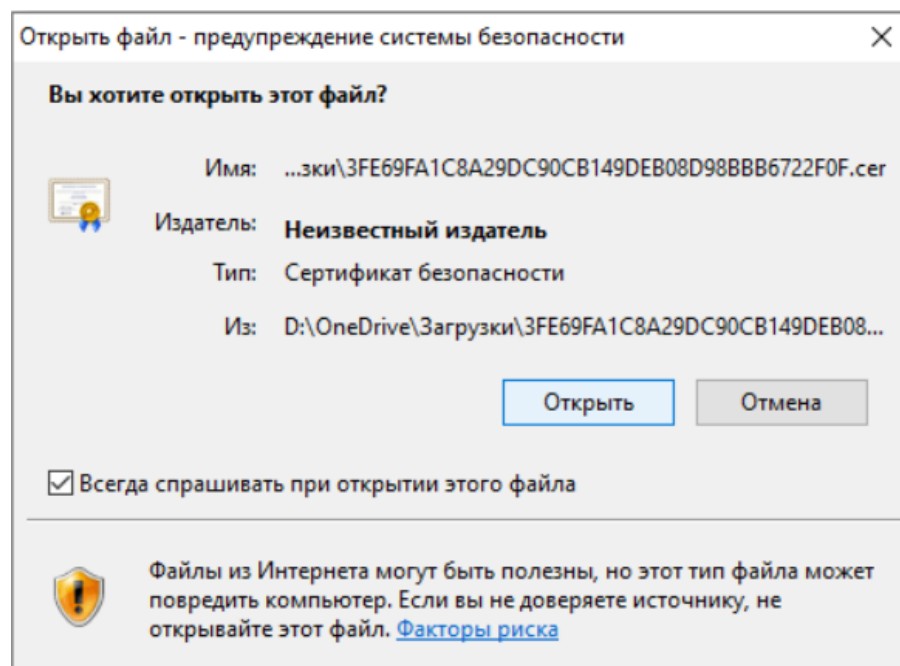
Установка корневых сертификатов

У каждого удостоверяющего центра свой корневой сертификат.

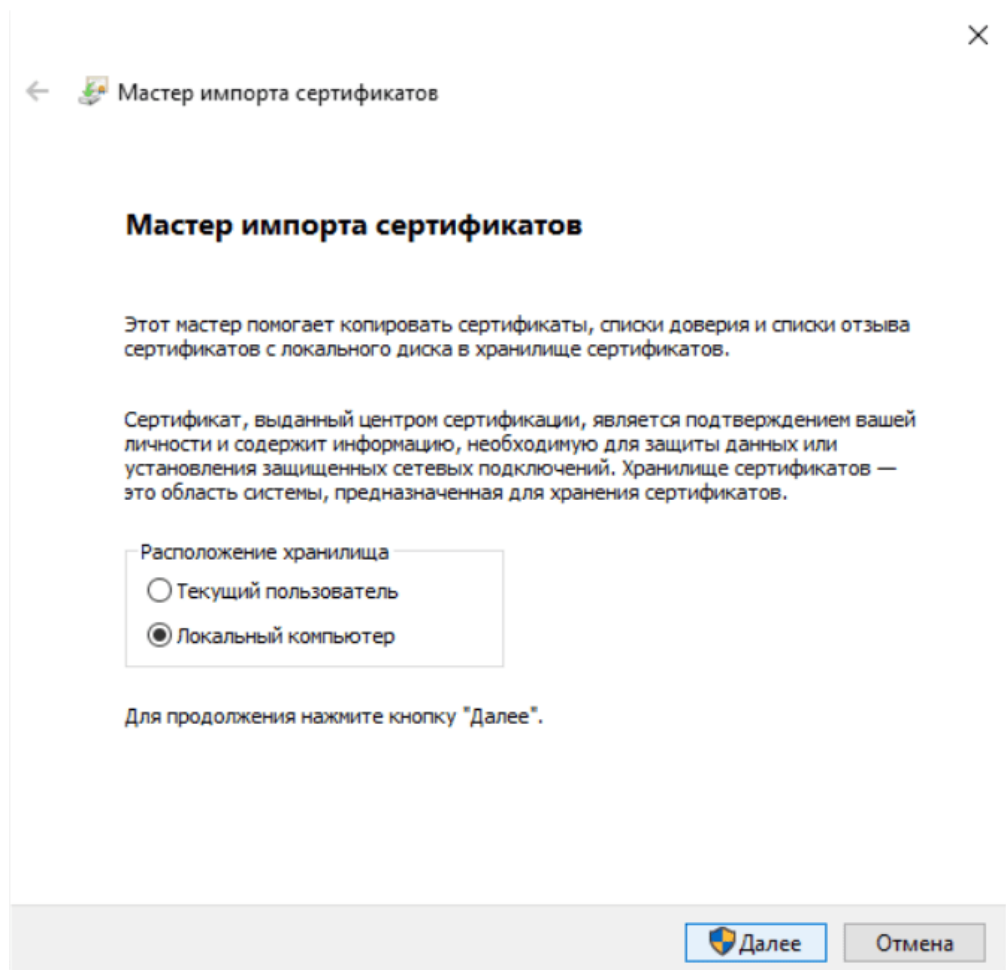
Установка корневого сертификата универсальна для любого удостоверяющего центра:

Скачайте сертификат на официальном сайте удостоверяющего центра.

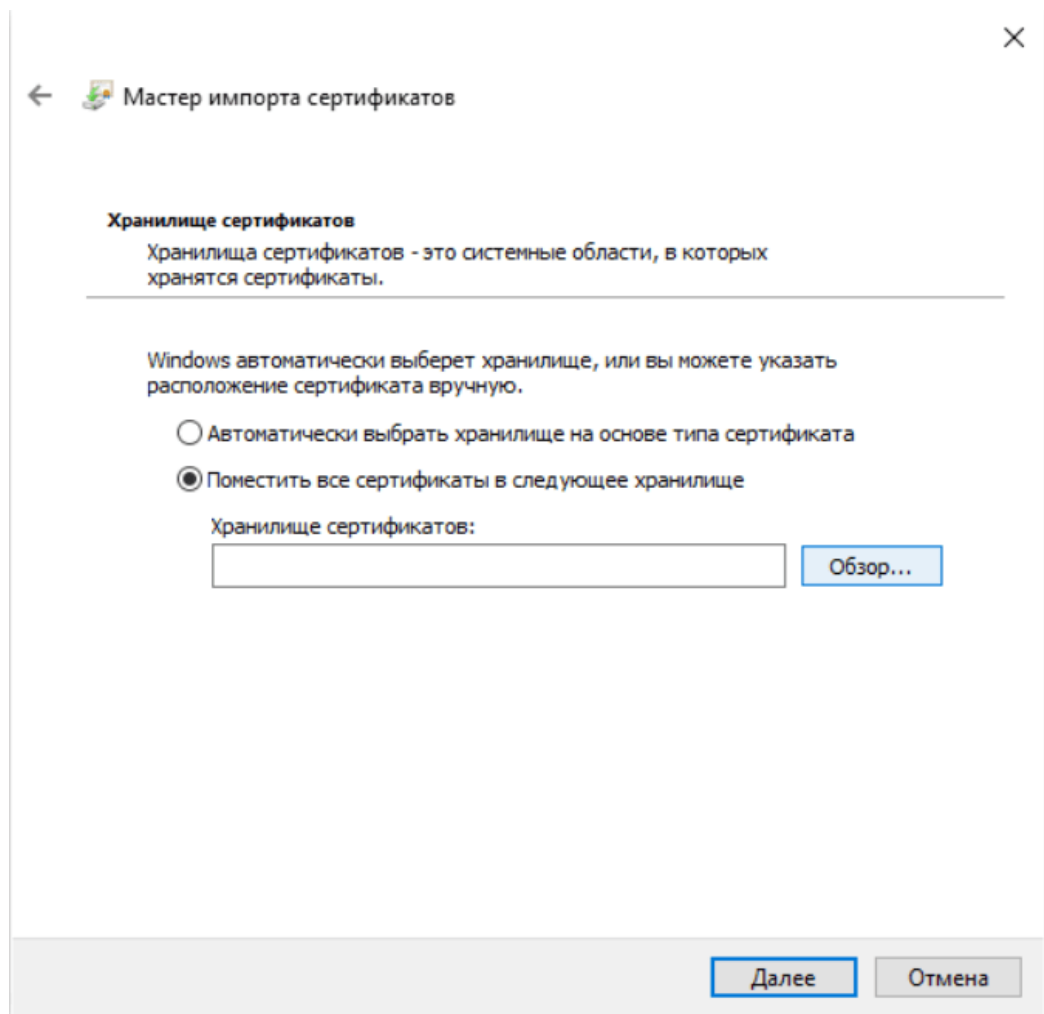
Откройте файл и нажмите «Установить сертификат».



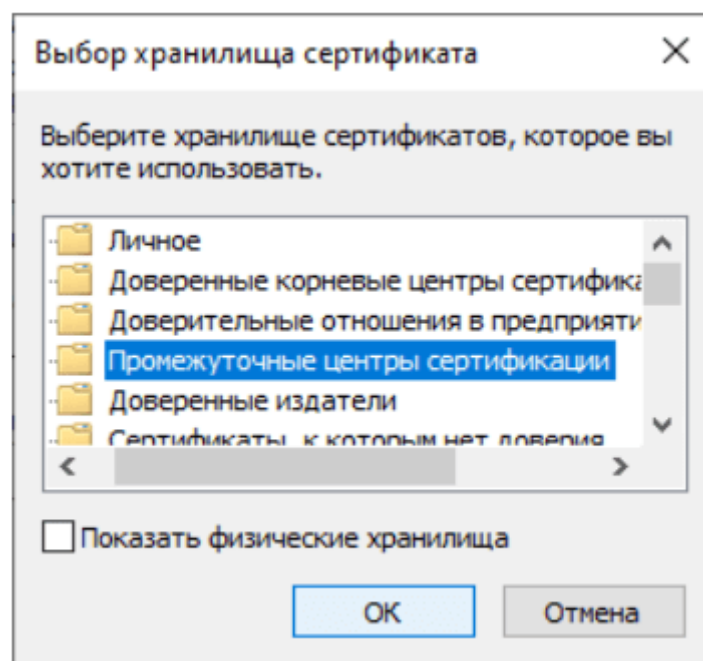
В окне «Мастер импорта сертификатов» выберите расположение хранилища → «Локальный компьютер» и нажмите кнопку «Далее».



Нажмите «Поместить все сертификаты в следующее хранилище» → «Обзор».



Выберите «Промежуточные центры сертификации», затем нажмите кнопку «ОК» → «Далее» → «Готово».





Мастер импорта сертификатов

Хранилище сертификатов

Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

- ☐ Автоматически выбрать хранилище на основе типа сертификата
- ☒ Поместить все сертификаты в следующее хранилище

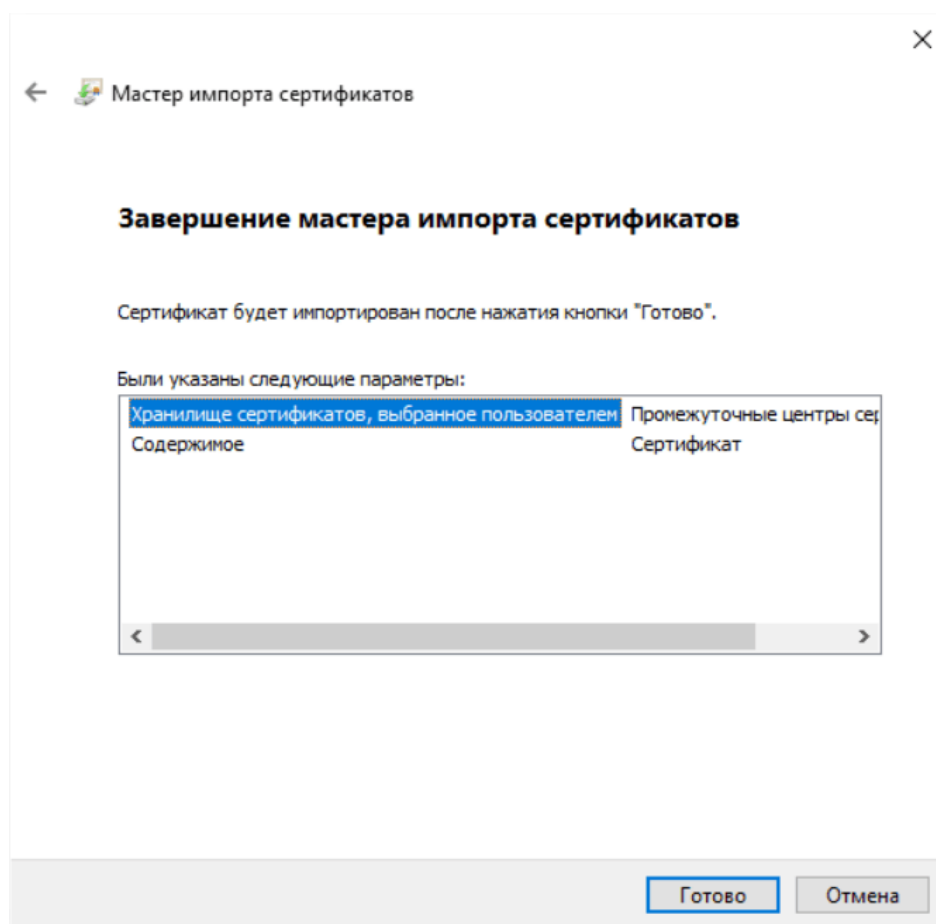
Хранилище сертификатов:

Промежуточные центры сертификации

Обзор...

Далее

Отмена



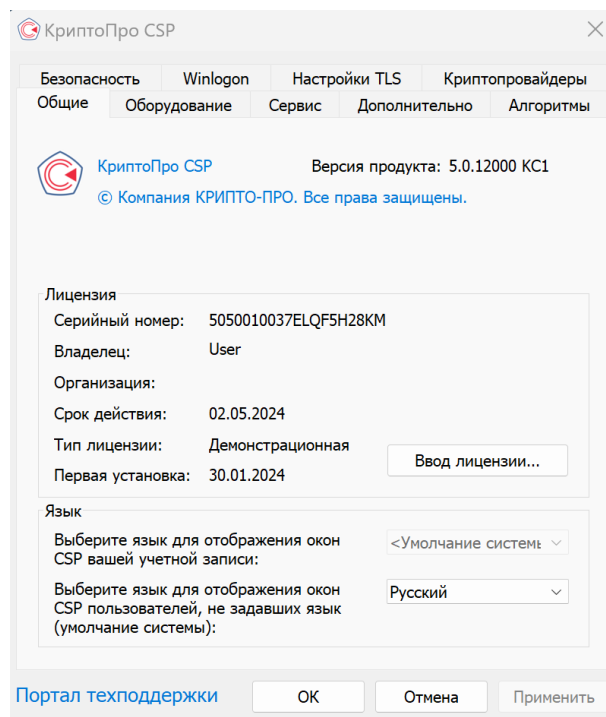
После этих действий корневой сертификат удостоверяющего центра будет установлен.

Подготовка к установке личного сертификата

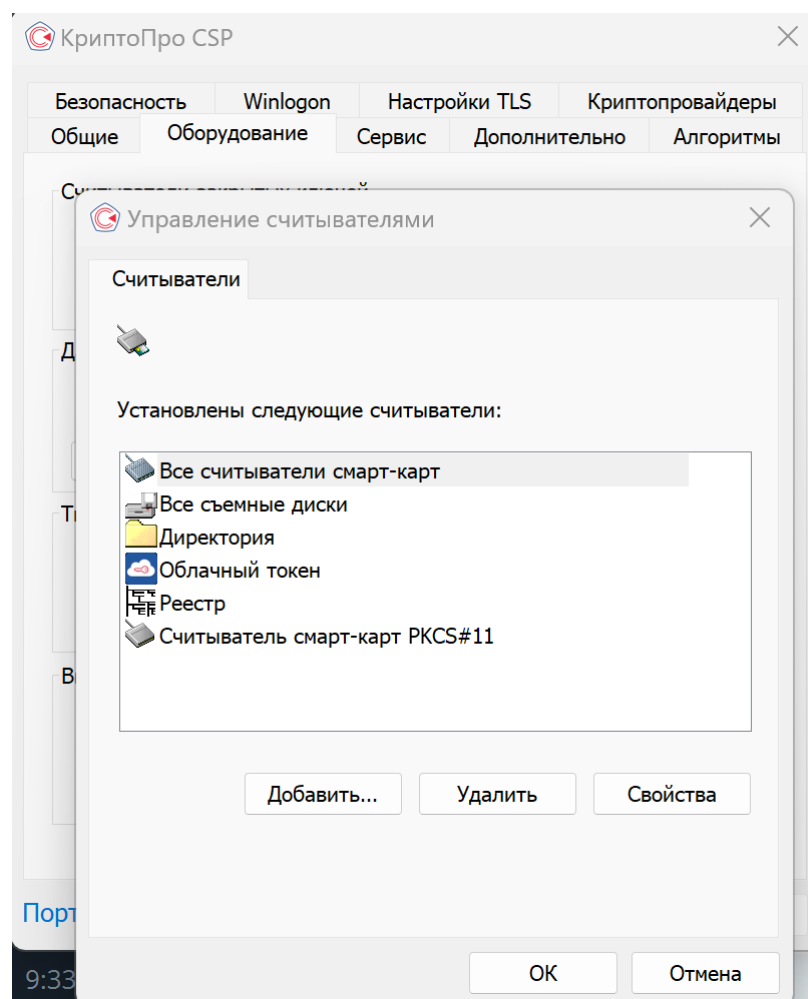
Перед установкой личного сертификата необходимо убедиться в следующем:

1. Вы получили в Удостоверяющем центре личный сертификат электронной подписи и знаете, где он находится.
2. На рабочем месте установлены **корневые сертификаты УЦ и Минцифры.**
3. На рабочем месте **установлен драйвер для ключевого носителя.** Ключевой носитель – отчуждаемый (съёмный) носитель (дискета, флешка, токен), содержащий ключ электронной подписи.
4. **Ключевой носитель подключен к рабочему месту.** Если в качестве ключевого носителя используется флешка или дискета, то они должны отображаться как съёмный диск в «Моем компьютере».
5. На рабочем месте **установлена программа КриптоПро CSP.** В программу КриптоПро CSP введена действующая лицензия.

Ваш ключевой носитель должен быть указан в списке установленных считывателей. Для проверки необходимо запустить КриптоПро CSP (Пуск/Все программы/КРИПТО-ПРО/КриптоПроCSP)



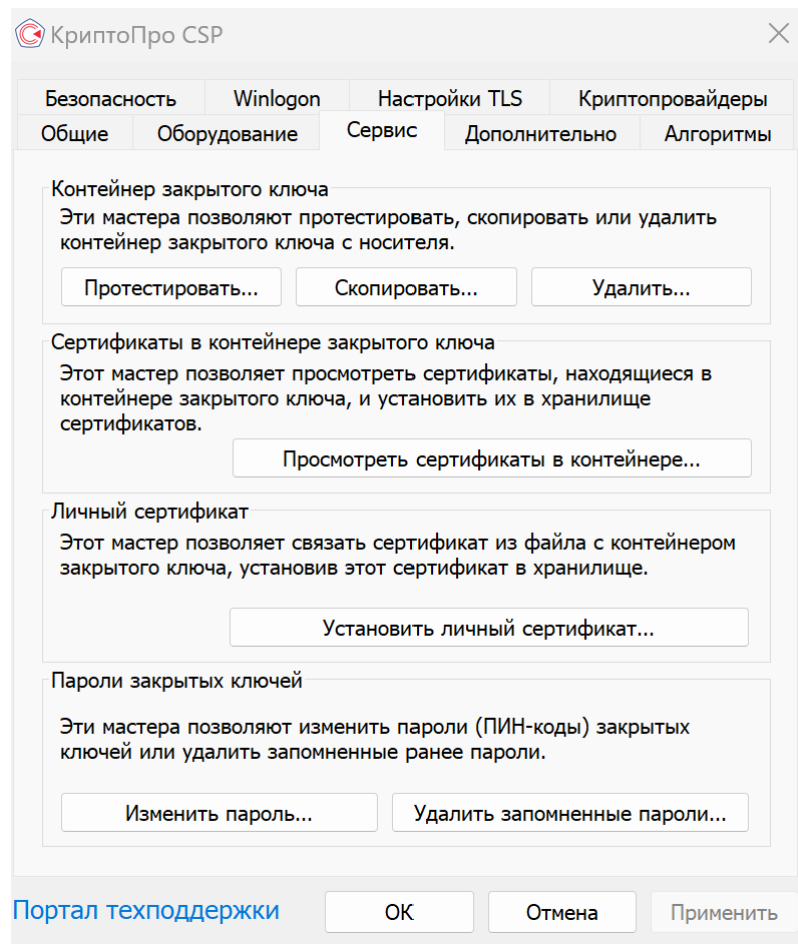
Откройте вкладку «Оборудование», нажмите кнопку «Настроить считыватели...», откроется окно «Управление считывателями».



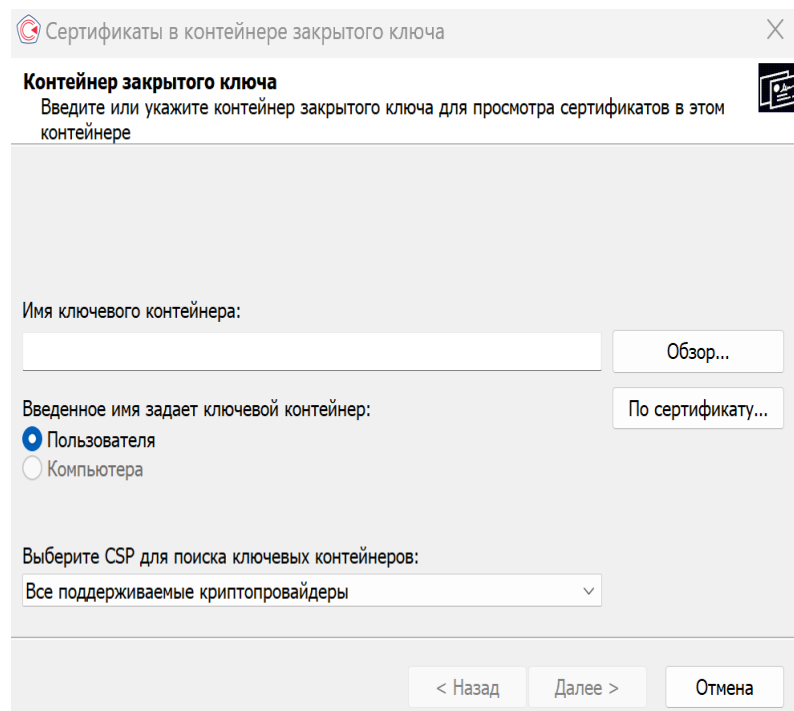
Если ключевым носителем является флешка, в списке должны присутствовать «Все съемные диски». В случае отсутствия в этом списке Вашего ключевого носителя, его необходимо добавить. Кнопка «Добавить» может быть недоступна, если у Вас отсутствуют права администратора.

Установка личного сертификата с ключевого носителя

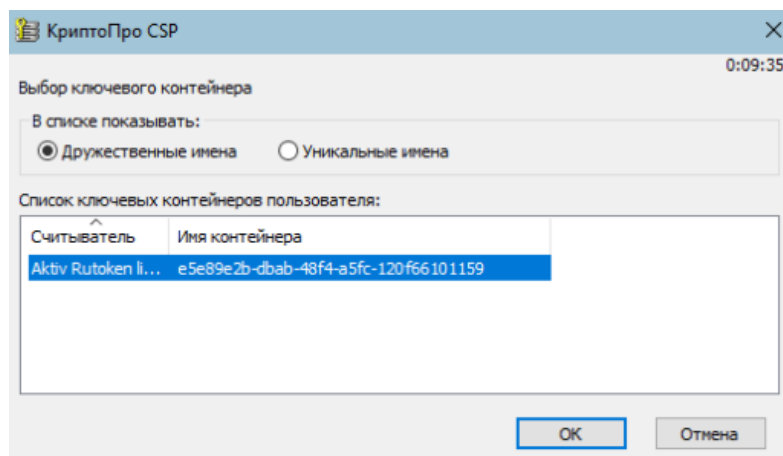
Для установки сертификата необходимо запустить КриптоПро CSP (Пуск/Все программы/КРИПТО-ПРО/КриптоПро CSP), открыть вкладку «Сервис».



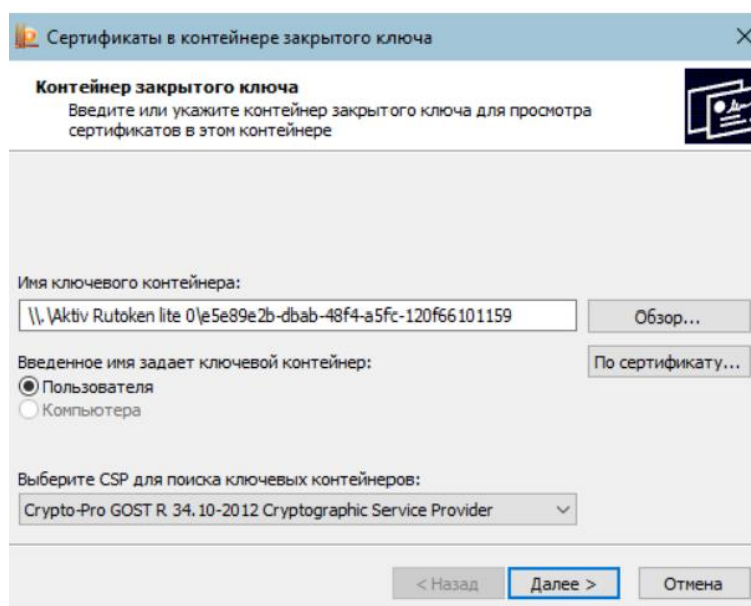
Нажмите кнопку «Просмотреть сертификаты в контейнере...»



В данном окне необходимо нажать кнопку «Обзор...» и выбрать контейнер электронной подписи, полученный в Удостоверяющем центре . После Выбора контейнера сертификата нажать кнопку

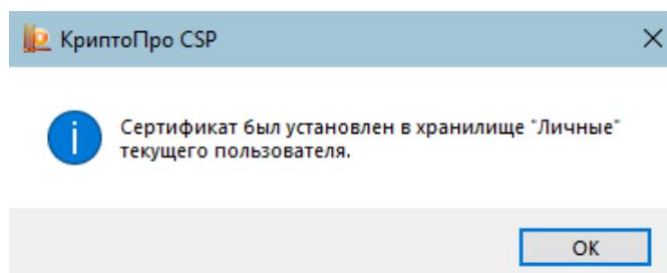


После выбора контейнера нажмите кнопку «Ок».

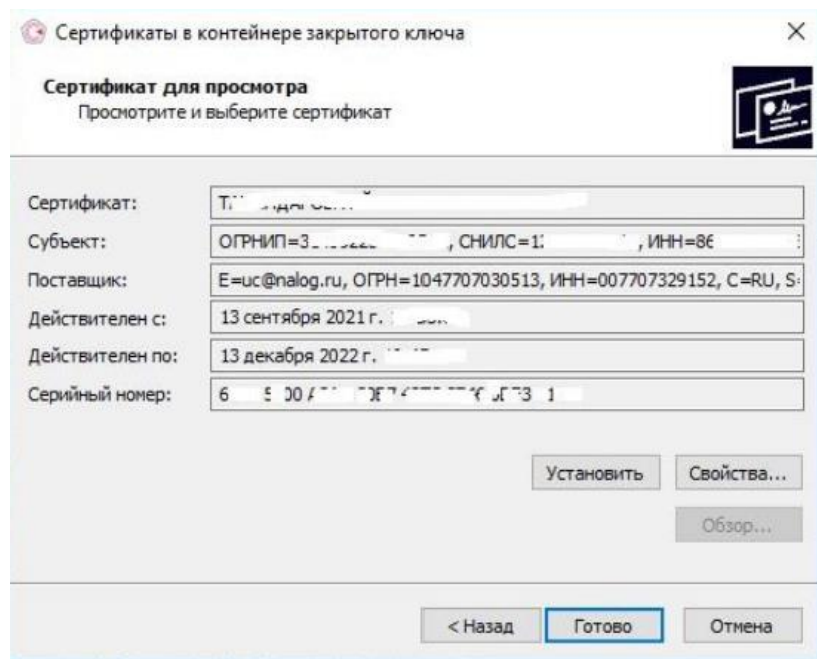


Нажмите кнопку «Далее».

Для завершения установки нажмите кнопки «Установить» и «ОК».



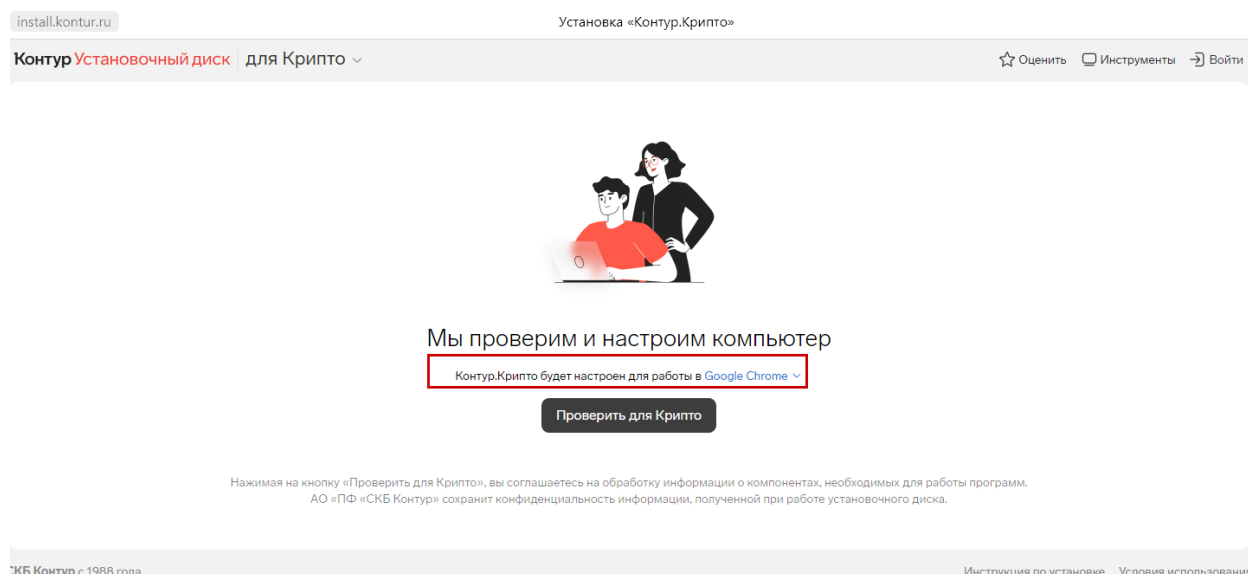
Просмотреть данные установленного сертификата можно в КриптоПро CSP на вкладке «Сервис», нажав кнопку «Обзор» и выбрав «Посмотреть сертификат в контейнере».



Необходимое программное обеспечение для работы с электронной подписью установлено и готово к использованию.

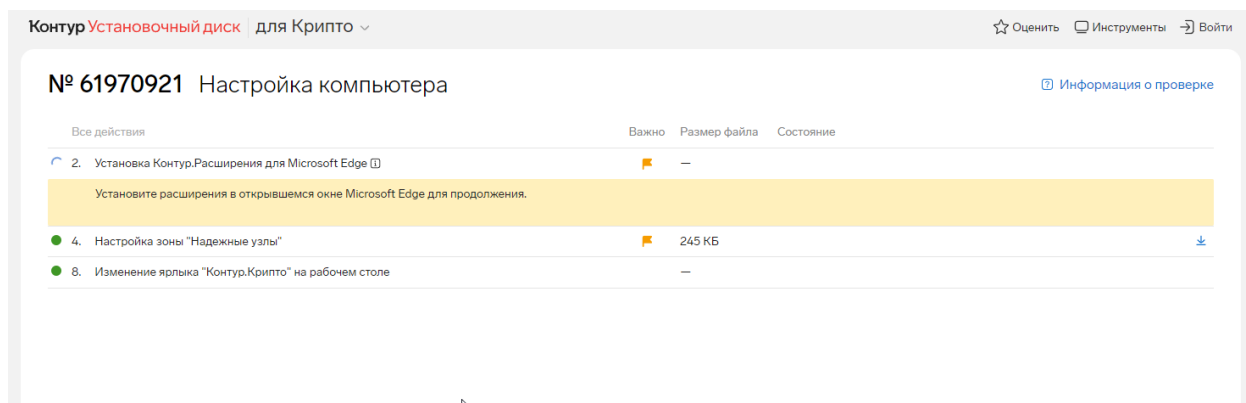
Установка расширения для браузера

Перейти на сайт <https://install.kontur.ru/crypto>

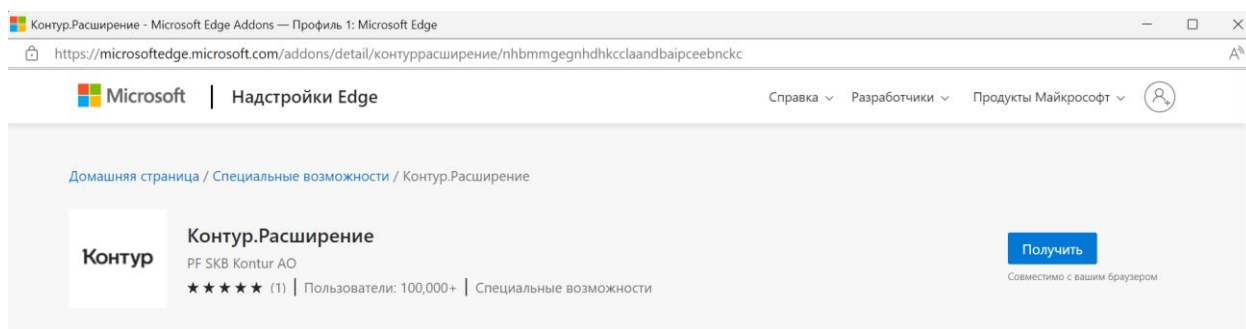
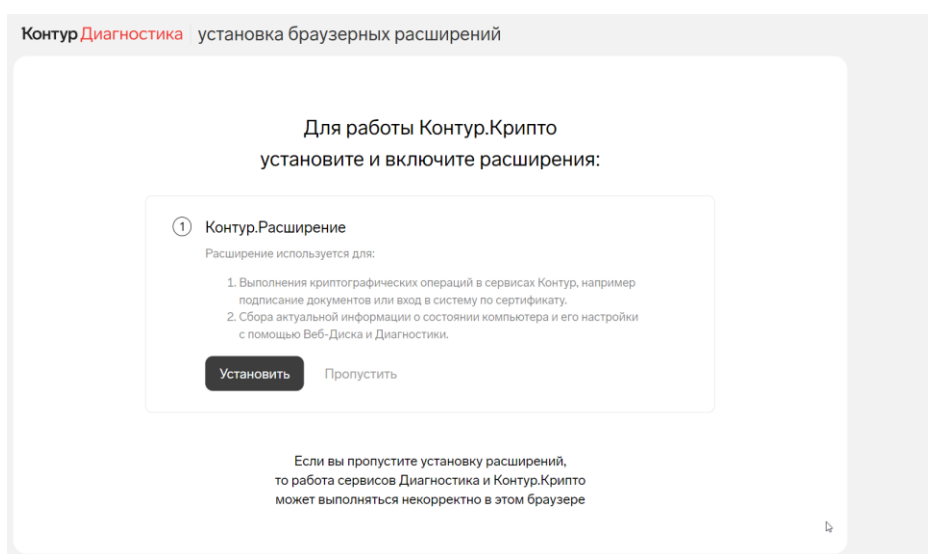


Нажать клавишу «Проверить для Криптопро»

Далее откроется окно диагностики компьютера для работы с ЭП



Если для используемого браузера не было установлено расширение, то будет предложено его установить из магазина приложений



Когда расширение будет установлено и закончится диагностика компьютера, то на экране появится сообщение об успешной настройке и возможности использовать ЭП.



№ 61971637

Компьютер готов к работе

Для входа в систему нужен сертификат

Войти в Контур.Крипто

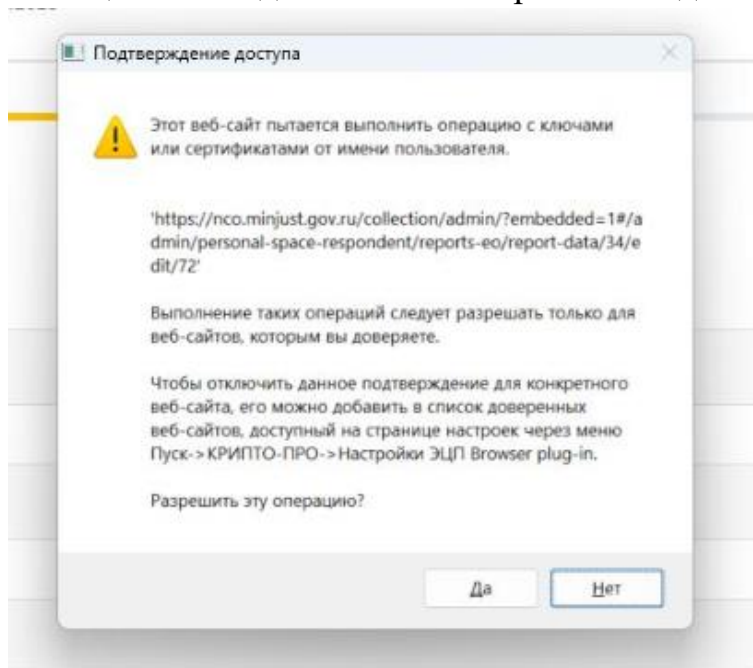
Получить сертификат

> Что еще можно сделать?

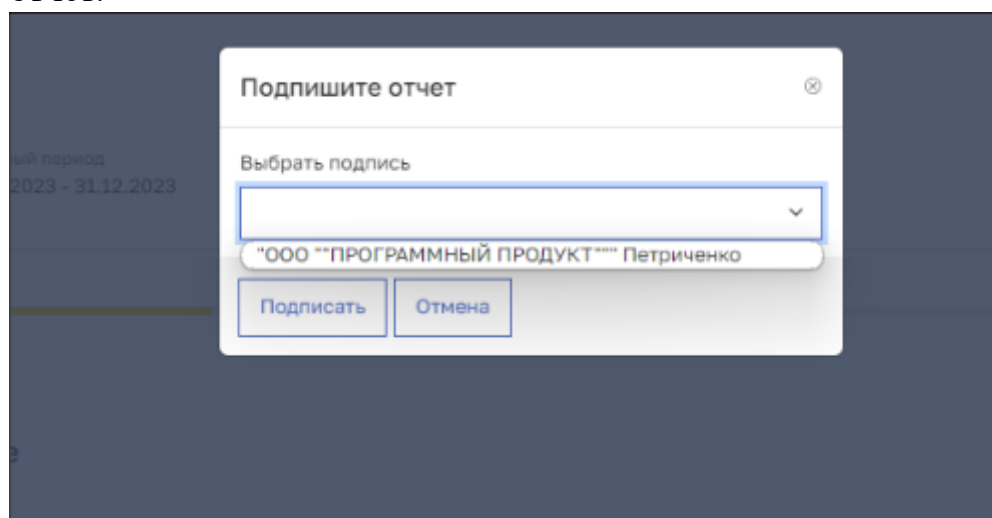
Подписание отчета

После выполнения всех подготовительных мероприятий вы можете приступить к подписанию отчета. Для этого необходимо выполнить следующие действия:

1. Заполните отчет
2. Вставьте Ключ с ЭП в USB порт
3. При нажатии на клавишу «Подписать и отправить» будет выведено сообщение о подписании Электронной подписью.



4. В сообщении нажать «ДА». В открывшемся окне выбора подписи выбрать сертификат электронной подписи, которой будет подписан отчет.



5. И нажать клавишу «Подписать». После чего отобразится сообщение об успешной отправке отчета

Найдено записей: 7


Отчет успешно отправлен
✕
0

Статус	Наименование формы	▼ Дата сдачи	Период	Дата изменения	
К заполнению	Отчетная форма о деятельности НКО	29.12.2023	01.01.2022 - 31.12.2022	28.12.2023 20:50:03	⋮
Отправлено	Отчетная форма о деятельности НКО	29.12.2023	01.01.2022 - 31.12.2022	28.12.2023 13:34:48	⌵ ⋮
Просрочено	Отчет о деятельности НКО	22.11.2023	01.10.2023 - 31.10.2023	27.12.2023 08:54:03	⋮
Просрочено	Отчет о деятельности НКО в отчетном периоде	22.11.2023	01.10.2023 - 31.10.2023	27.12.2023 08:54:03	⋮
Просрочено	НКО Сбор отчетности	22.11.2023	01.10.2023 - 31.10.2023	27.12.2023 08:54:03	⋮
Просрочено	Отчетность по приказу 185 в части НКО	22.11.2023	01.10.2022 - 31.10.2023	27.12.2023 08:54:03	⋮
Отправлено	Отчетность НКО	22.11.2023	01.11.2023 - 30.11.2023	28.12.2023 21:08:46	⌵ ⋮

< 1 >

Ошибки и варианты решения

Ошибка: "Не удастся построить цепочку сертификатов для доверенного корневого центра. (0x800B010A)".

Это означает, что у Вас на машине не установлены необходимые промежуточные/корневые сертификаты для проверки создания подписи.

Для решения проблемы необходимо скачать с сайта Удостоверяющего центра, выдавшего Вам сертификат, промежуточные и корневой сертификаты и установить их в соответствующие хранилища, как описано в п. Установка корневых сертификатов настоящей инструкции.

Не удастся найти сертификат и закрытый ключ для расшифровки (0x8009200B)

Если система не смогла обнаружить соответствующий ключ на носителе. Для решения проблемы необходимо бывает достаточно произвести корректную ручную переустановку сертификата.

Не найден автор исходной подписи (0x8009100E)

Если система не смогла обнаружить автора исходной подписи. Для решения проблемы необходимо бывает достаточно произвести корректную ручную переустановку сертификата.

Цепочка сертификатов обработана, но обработка прервана на корневом сертификате, у которого отсутствует отношение доверия с поставщиком доверия (0x800B0109)

Для решения проблемы необходимо установить корневые сертификаты в доверительные корневые центры. Как описано в п. Установка корневых сертификатов.

Ошибка исполнения функции (0x8007065B)

Причина возникновения подобной ошибки - истекшая лицензия КристоПро CSP.

Для решения проблемы необходимо приобрести и активировать лицензию КристоПро CSP (рекомендуется сразу приобретать лицензию и переходить на версию 5.0).