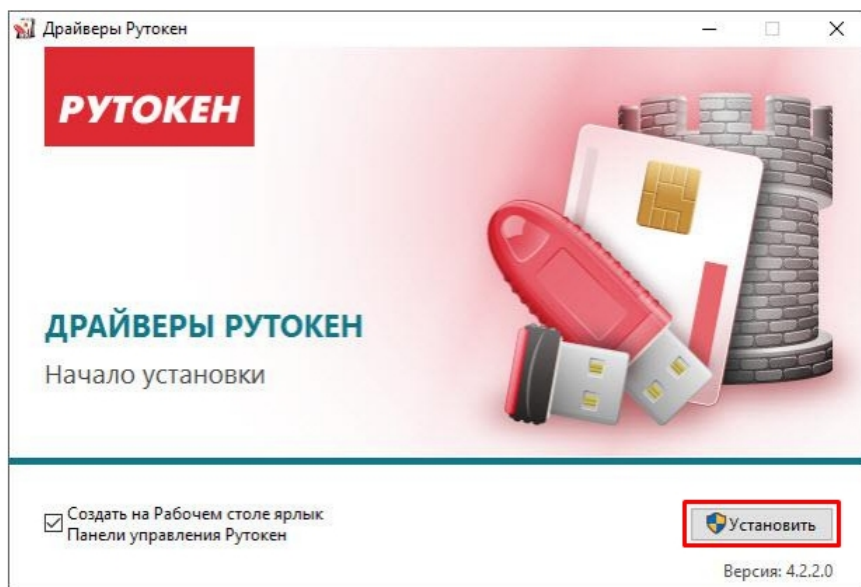


# Установка необходимых драйверов и утилит для работы с носителями ЭП

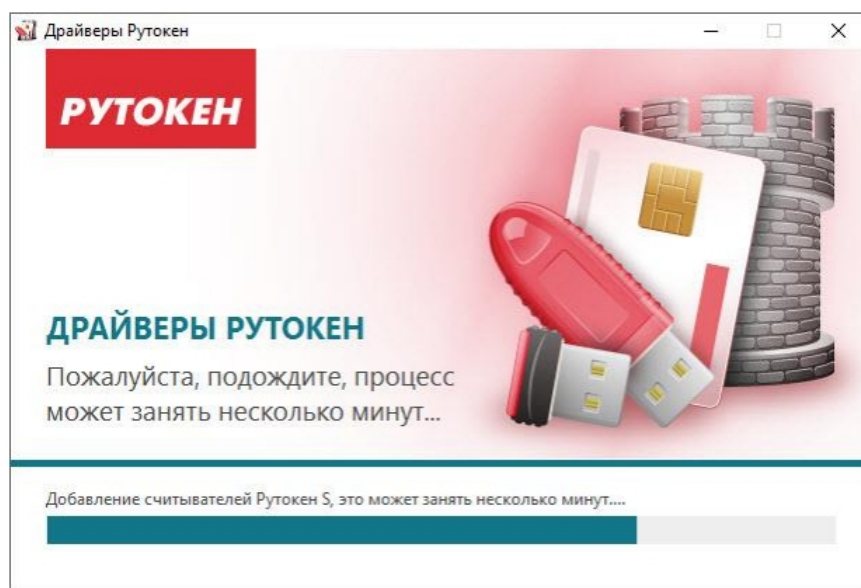
Последние изменения: 2024-03-26

## Драйверы Рутокен для Windows

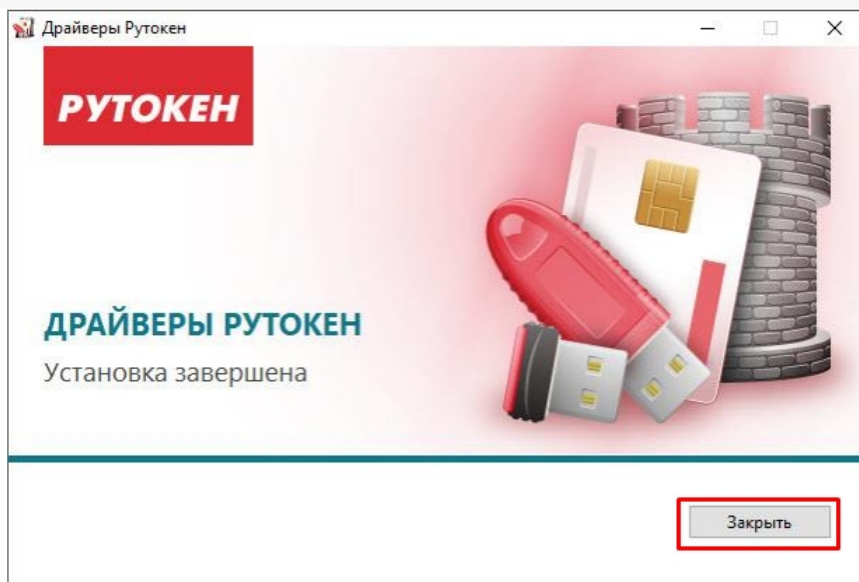
- **Скачайте** актуальную версию комплекта «Драйверы Рутокен для Windows».
- Запустите программу установки комплекта драйверов для Windows и нажмите на кнопку «Установить».



- В окне с запросом на разрешение изменений на компьютере нажмите на кнопку «Да». В результате запустится процесс установки комплекта драйверов.



- После завершения процесса установки нажмите на кнопку «Заккрыть».



- Подключите устройство Рутокен к компьютеру.

## Рутокен Плагин в Windows

В Windows Рутокен Плагин работает в следующих браузерах:

- Google Chrome.
- Mozilla Firefox.
- Яндекс Браузер.
- Internet Explorer.
- Opera.

Скачать актуальную версию плагина можно [здесь](#).

Не нашли что искали?



Задать вопрос в техническую поддержку

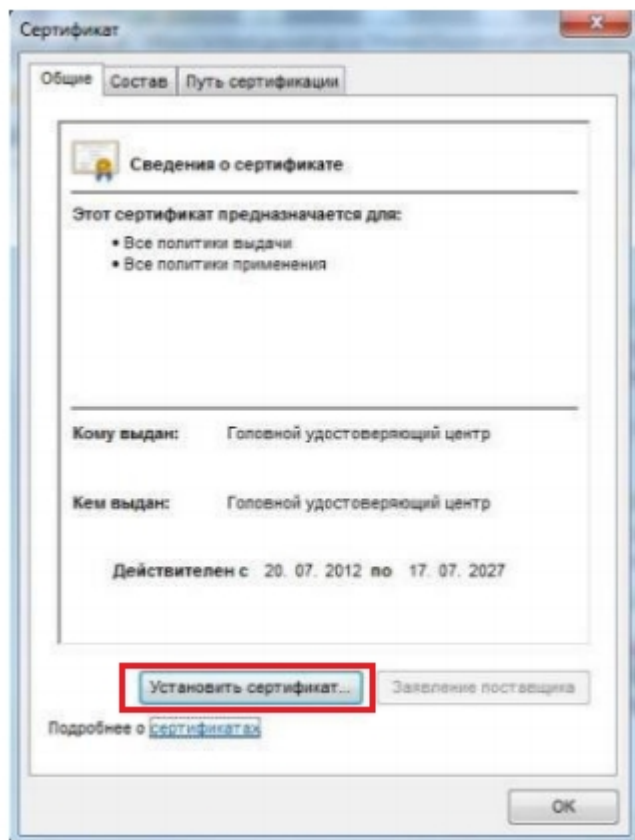
# Установка корневых сертификатов в хранилища

Последние изменения: 2024-03-26

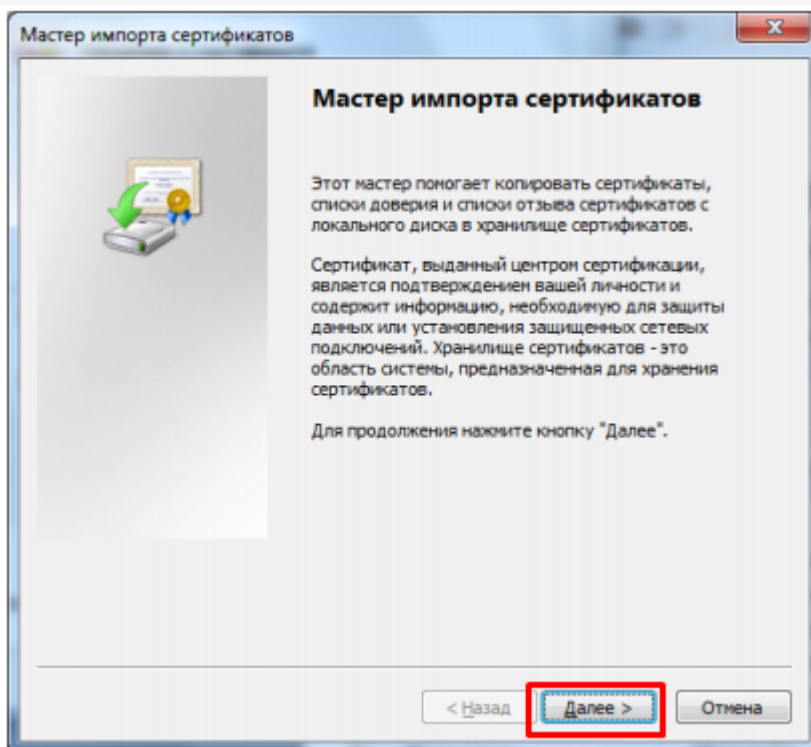
## Корневой сертификат Головного Удостоверяющего Центра

Для установки сертификата вам потребуется перейти по [ссылке](#) и открыть скачанный сертификат.

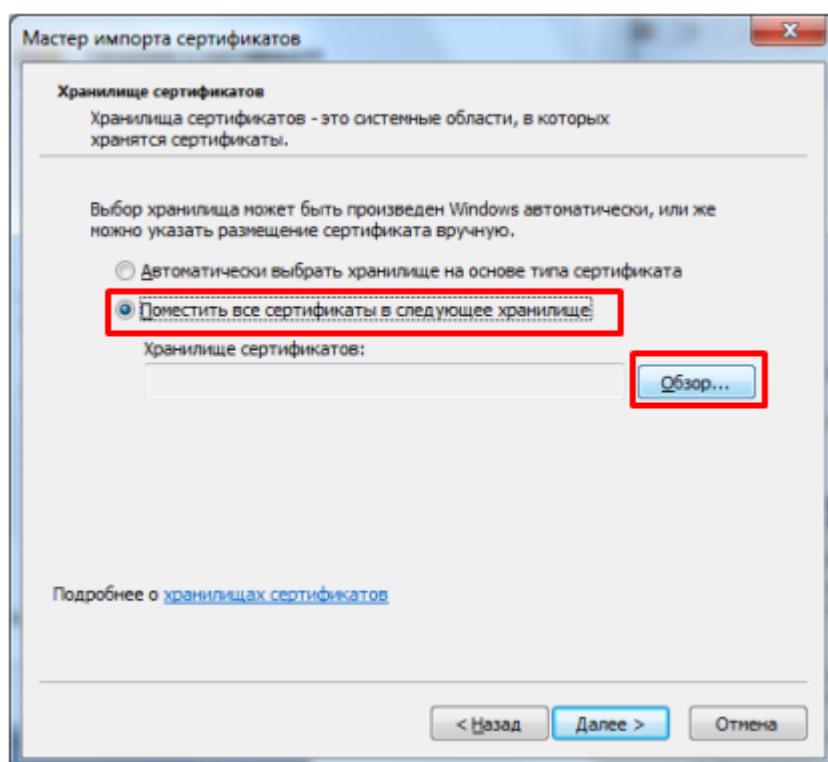
- Нажмите «Установить сертификат».



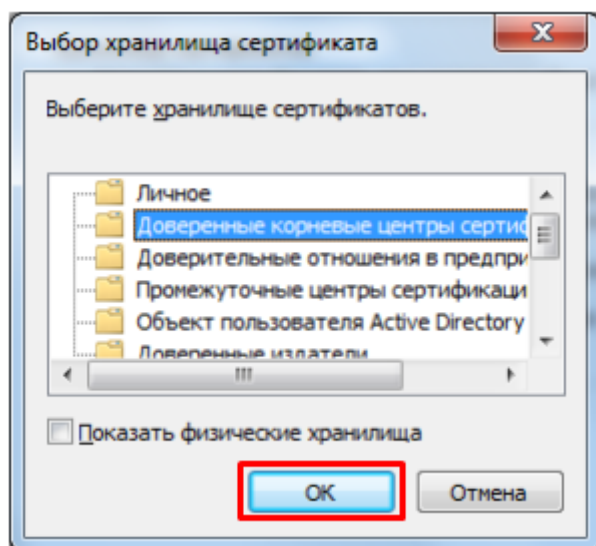
- В открывшемся окне мастера импорта сертификатов нажмите «Далее».



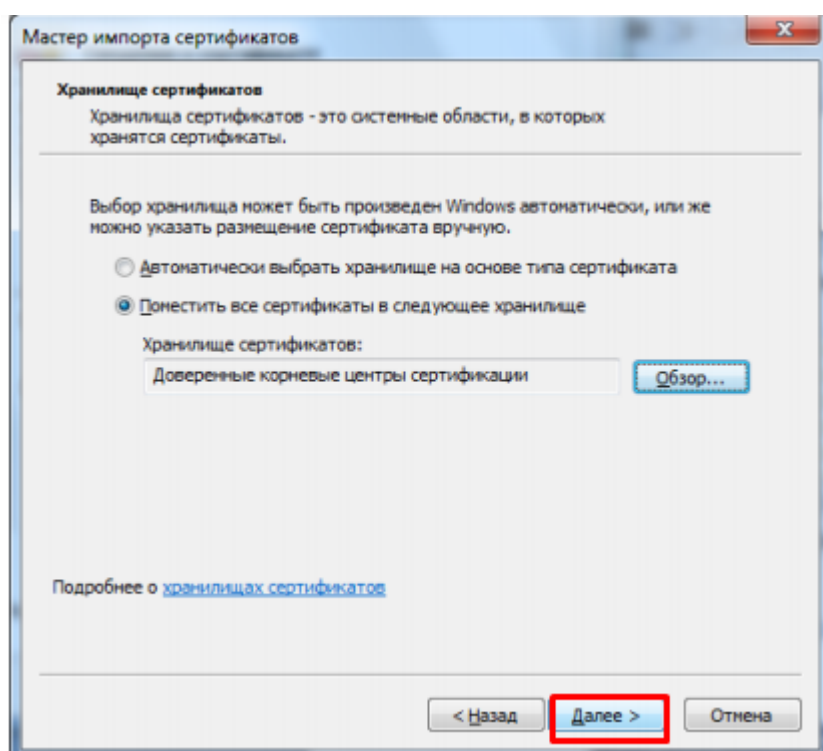
- Выберите «Поместить все сертификаты в следующее хранилище», после чего нажмите «Обзор...».



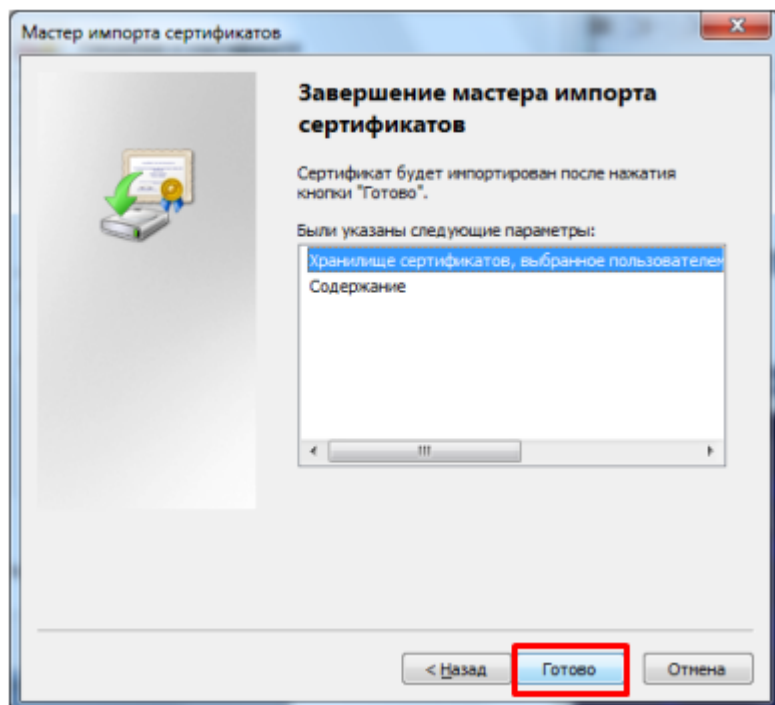
- Укажите «Доверенные корневые центры сертификации», нажмите «ОК».



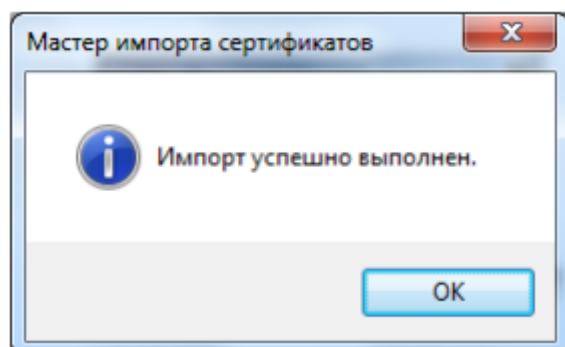
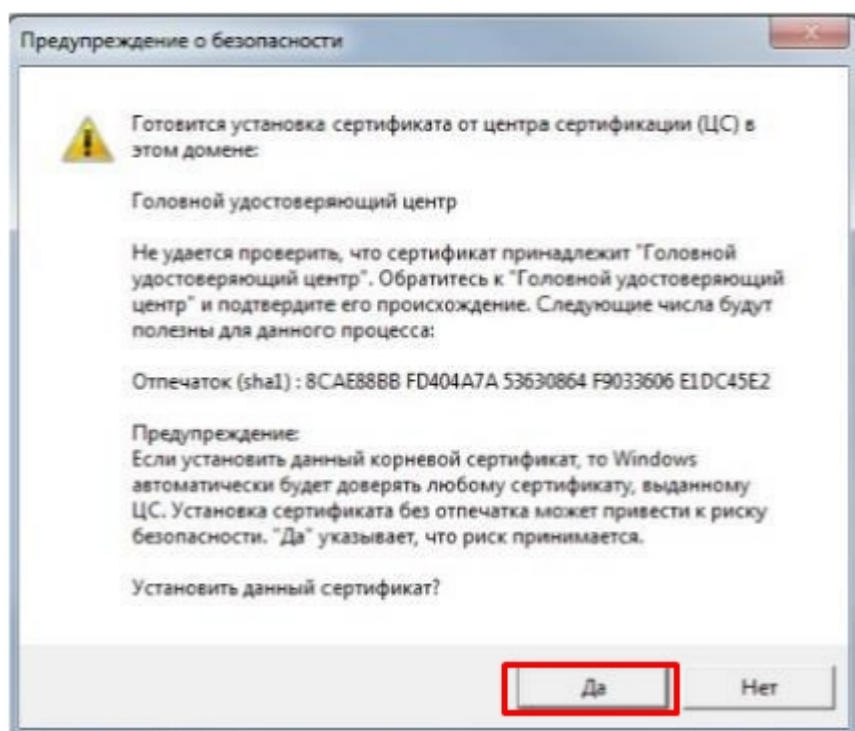
- Нажмите «Далее».



- Для завершения работы мастера импорта сертификатов нажмите «Готово».



- Если вы переходите с тестового сертификата на рабочий или обратно, появится следующее предупреждение, где необходимо подтвердить установку сертификата, нажав кнопку «Да».



## Корневой сертификат Минкомсвязи России

Произведите установку корневого сертификата Минкомсвязи России аналогично установке корневого сертификата Головного Удостоверяющего Центра. Для установки сертификата вам потребуется перейти по [ссылке](#) и открыть скачанный сертификат.

## Корневой сертификат Удостоверяющего Центра

Произведите установку корневого сертификата Удостоверяющего Центра, выдавшего вашу электронную подпись, аналогично установке корневого сертификата Головного Удостоверяющего Центра. За сертификатом следует обратиться на [сайт УЦ](#).

Не нашли что искали?



Задать вопрос в техническую поддержку

# Установка криптопровайдера КriptoПро CSP

Последние изменения: 2024-03-26

## Установка КriptoПро CSP

Пройдите процедуру регистрации и [загрузите](#) дистрибутив КriptoПро CSP с официального сайта разработчика.

Установка дистрибутива СКЗИ КriptoПро CSP должна производиться пользователем, имеющим права администратора.

При установке КriptoПро CSP следуйте инструкциям мастера установки:



Благодарим за выбор КriptoПро CSP.

Продолжая установку, вы принимаете условия Лицензионного соглашения.  
Продукт будет установлен с временной лицензией на 3 месяца.

<http://www.cryptopro.ru>

→ Установить (рекомендуется)

Продукт будет установлен в конфигурации КС1 и языком операционной системы с настройками по умолчанию.

→ Дополнительные опции

Позволяет выбрать конфигурацию КС и язык.

☒ Установить корневые сертификаты

Рекомендуется устанавливать КriptoПро CSP с автоматическими настройками, но вы можете установить язык и конфигурацию уровня безопасности самостоятельно (с помощью кнопки «Дополнительные опции»).



Благодарим за выбор КристоПро CSP.

Язык установки:

- ☒ Русский  
☐ English

Уровень безопасности:

- ☐ KC1  
☒ KC2  
☐ KC3

→ **Установить**  
Установить с выбранными KC-уровнем и языком.

После завершения установки перезагрузите браузер.

КристоПро CSP

✕

КристоПро CSP успешно установлен.  
Для корректной работы КристоПро CSP может потребоваться  
перезапустить браузер.

ОК

## Установка контейнера закрытого ключа

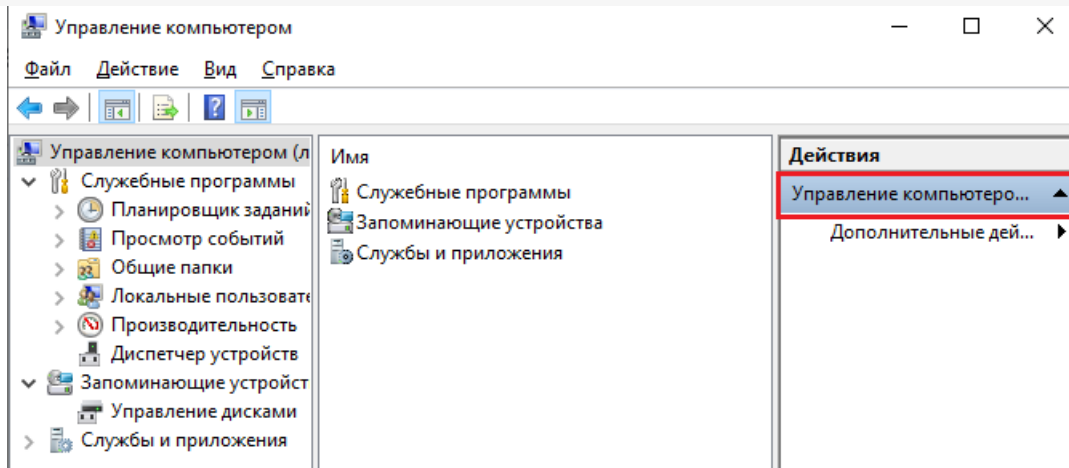
Контейнер закрытого ключа может быть установлен на одном из носителей:

- реестр (для установки в реестр);
- директория;
- съемный диск для хранения ключей (usb-ключ, pfc-карта, виртуальный жесткий диск).

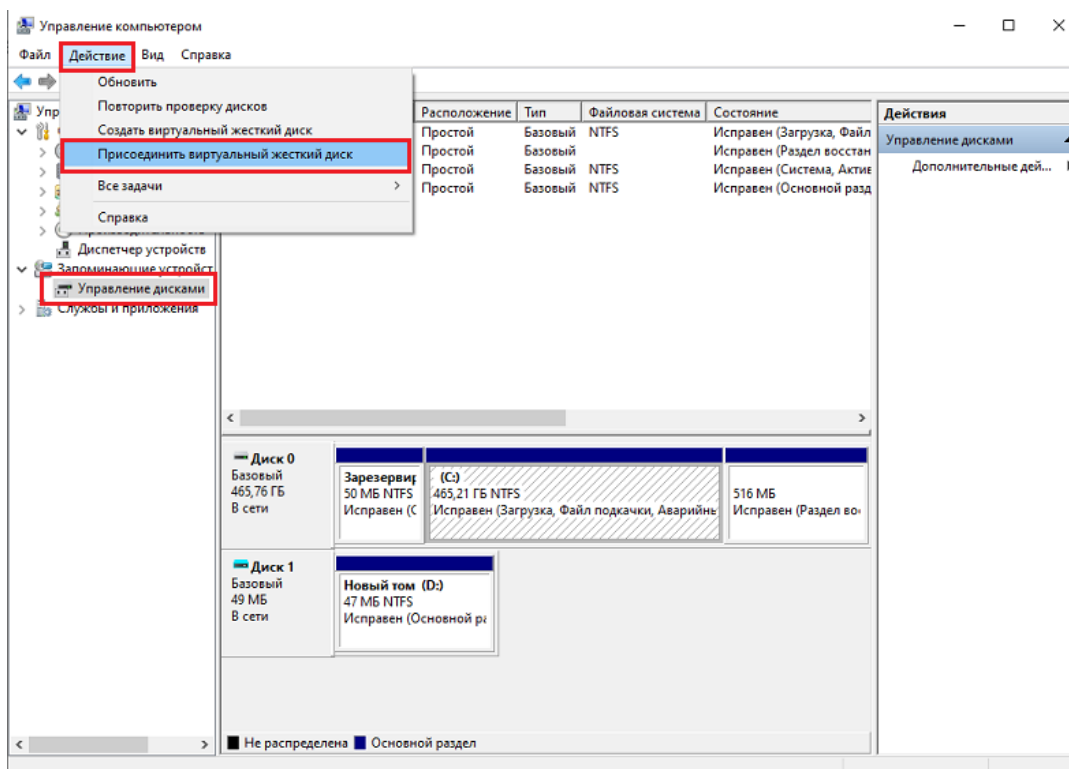
При установке контейнера в реестр или директорию нужно удостовериться, что предоставлены необходимые права на ветку реестра или на папку, в которую устанавливается контейнер.

При установке контейнера на виртуальный жесткий диск, необходимо подключить его следующим путем:

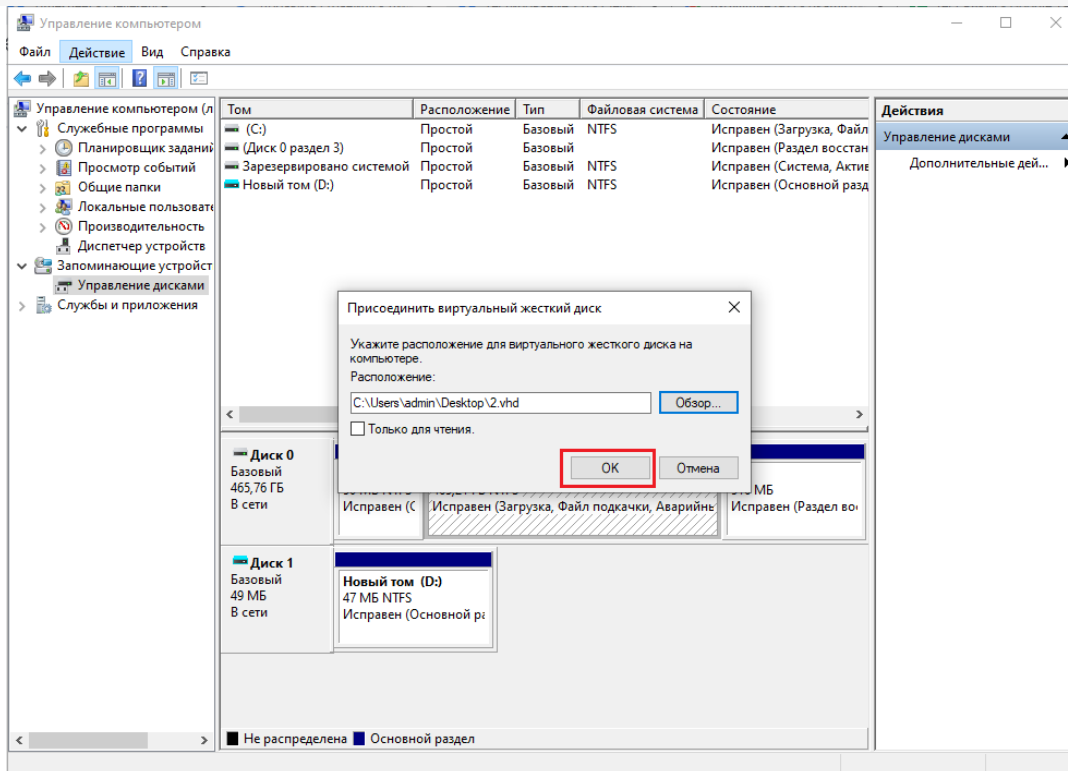
- ПУСК → «Средства администрирования» → «Управление компьютером».



- Открыть вкладку «Управление дисками», нажать «Действие» → «Присоединить виртуальный жесткий диск».



- Выбрать загруженный ранее контейнер, нажать «ОК».



- После этого новый диск будет добавлен.

Том	Расположение	Тип	Файловая система	Состояние	Емкость	Свободно	Свободно %
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Аварийный дамп памяти, Основной раздел)	49,40 ГБ	18,63 ГБ	38 %
Диск 0 раздел 1)	Простой	Базовый		Исправен (Раздел восстановления)	499 МБ	499 МБ	100 %
Диск 0 раздел 2)	Простой	Базовый		Исправен (Шифрованный (EFI) системный раздел)	99 МБ	99 МБ	100 %
Новый том (D:)	Простой	Базовый	NTFS	Исправен (Основной раздел)	47 МБ	32 МБ	68 %

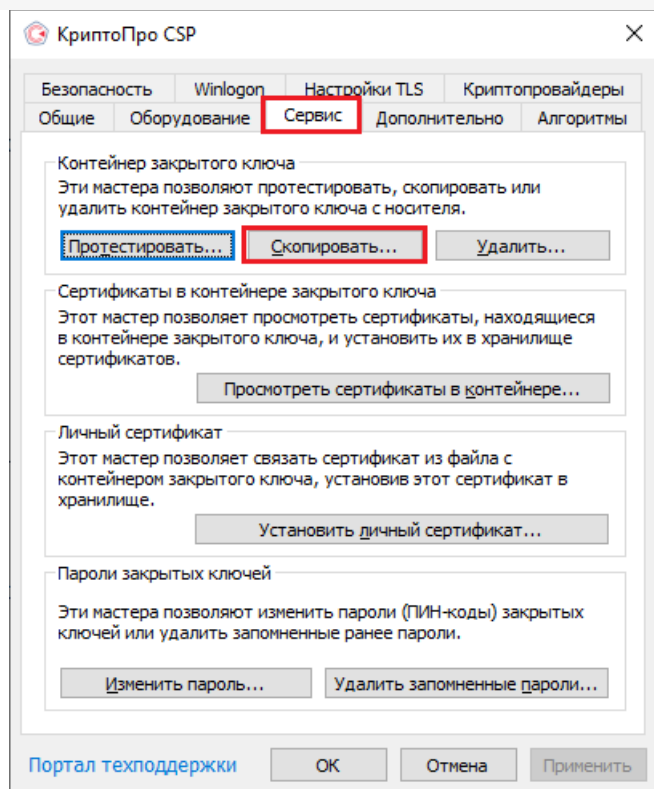
Диск 0	Базовый	499,98 ГБ	В сети	499 МБ	Исправен (Раздел восстановления)	99 МБ	Исправен (Шифрованный (EFI) системный)	(C:)	49,40 ГБ NTFS	Исправен (Загрузка, Аварийный дамп памяти, Основной раздел)
--------	---------	-----------	--------	--------	----------------------------------	-------	--	------	---------------	---

Диск 1	Базовый	49 МБ	В сети	Новый том (D:)	47 МБ NTFS	Исправен (Основной раздел)			
--------	---------	-------	--------	----------------	------------	----------------------------	--	--	--

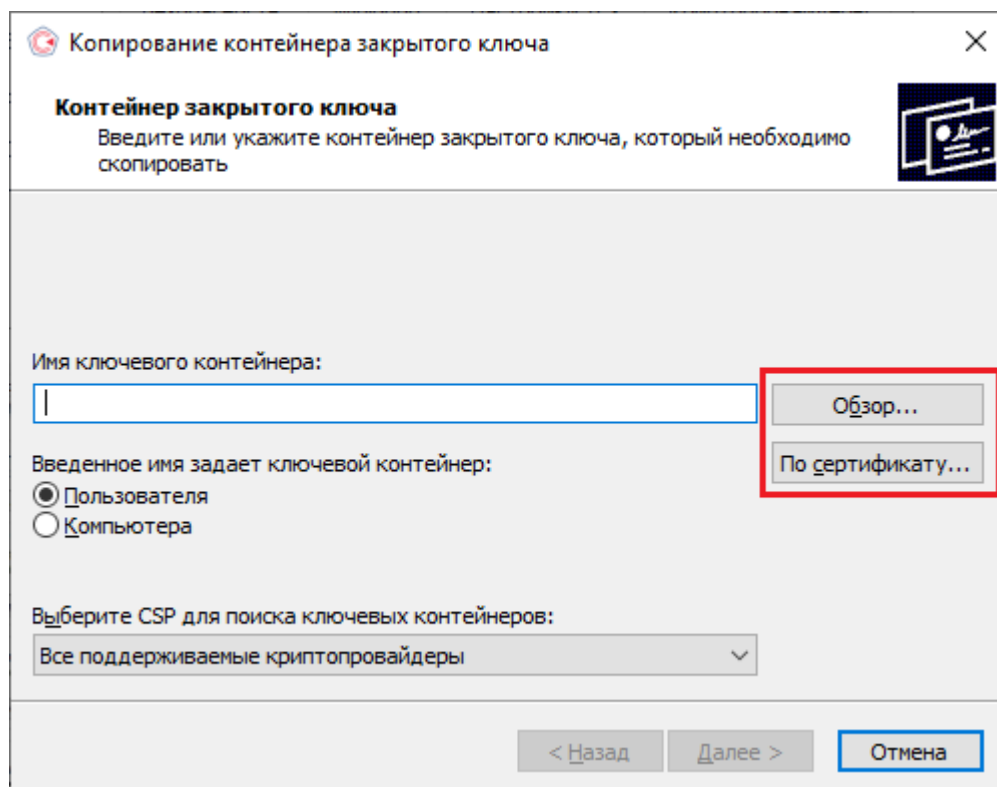
Диск 2	Базовый	49 МБ	Вне сети	47 МБ					
--------	---------	-------	----------	-------	--	--	--	--	--

Если хранить контейнер на виртуальном жестком диске, то после перезагрузки ПК этот жесткий диск потребует подключения заново. Поэтому рекомендуем скопировать контейнер на любой из доступных носителей с помощью программы КриптоПро CSP. Для этого:

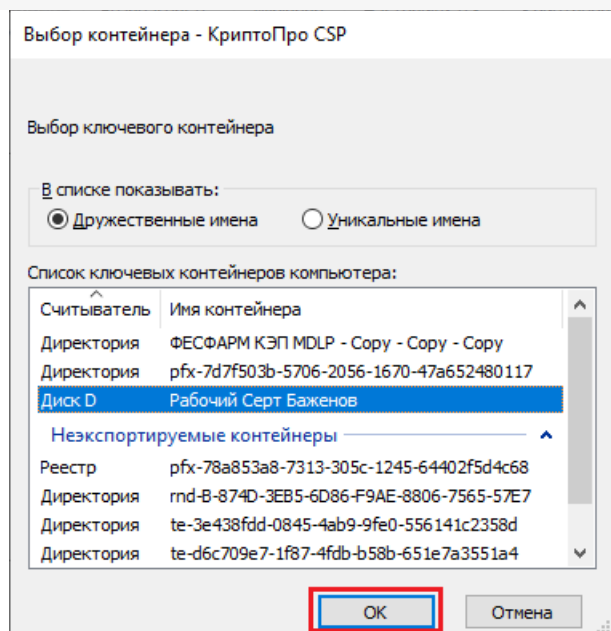
Запустите КриптоПро CSP от имени администратора, откройте вкладку «Сервис» и нажмите на кнопку «Скопировать».



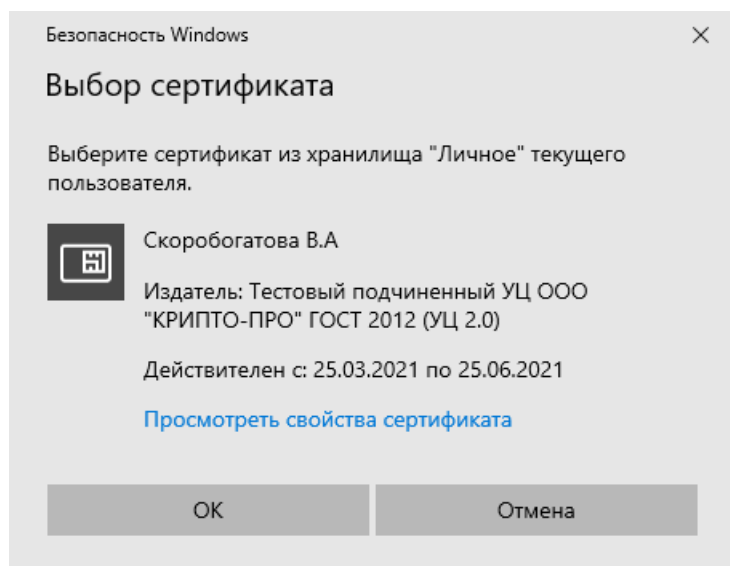
В открывшемся окне необходимо выбрать, где будет располагаться ключевой контейнер (пользователь или компьютер) с помощью кнопки «Обзор» или «По сертификату».



При нажатии на кнопку «Обзор», потребуется выбрать контейнер из списка:



При нажатии на кнопку «По сертификату» потребуется выбрать нужный сертификат.



После того как выбран нужный контейнер, выберите имя и доступ сертификата. Нажмите кнопку «Готово».

Копирование контейнера закрытого ключа

**Контейнер закрытого ключа**  
Введите имя контейнера закрытого ключа, на который необходимо скопировать

Введите имя для создаваемого ключевого контейнера:  
Рабочий Серт Баженов - Сору

Введенное имя задает ключевой контейнер:  
☐ Пользователя  
☒ Компьютера

Выберите CSP для поиска ключевых контейнеров:  
Crypto-Pro GOST R. 34.10-2012 Cryptographic Service Provider

< Назад   Готово   Отмена

После этого откроется окно выбора ключевого носителя, на который будет копироваться контейнер. укажите нужный и нажмите «ОК».

Выбор ключевого носителя - КриптоПро CSP

Выберите носитель для создания контейнера Рабочий Серт Баженов - Сору

Реестр  
Директория  
Диск D  
Недоступны для данной операции  
Аktiv Co. ruToken 2  
Аktiv Co. ruToken 1

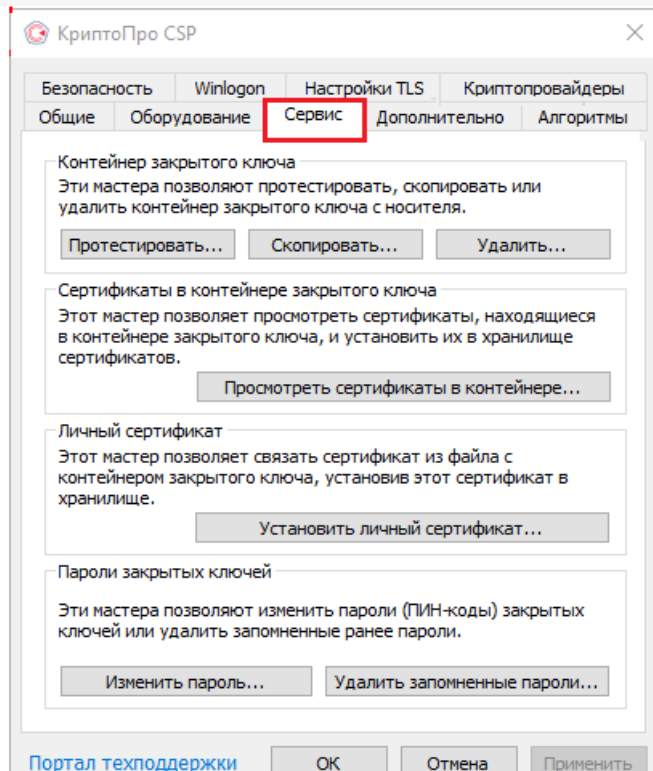
Тип приложения  
CSP

Описание:  
Использовать в качестве хранилища ключей реестр Windows.

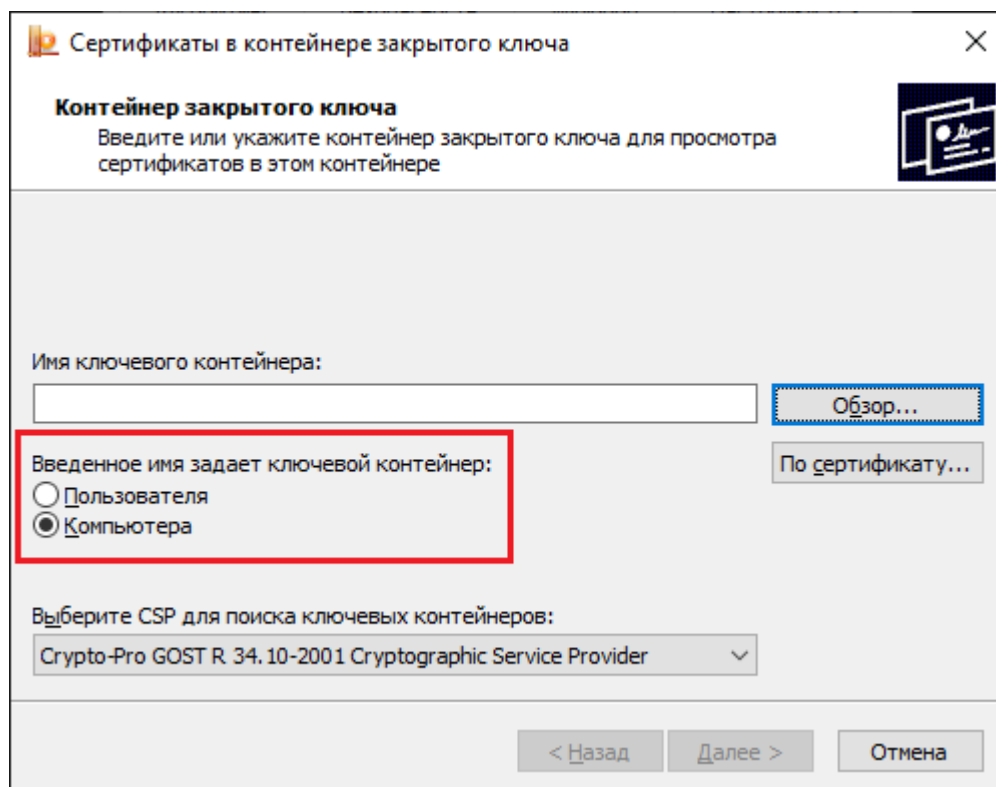
ОК   Отмена

После выбора ключевого носителя создайте пароль на контейнер. Нажмите «ОК».





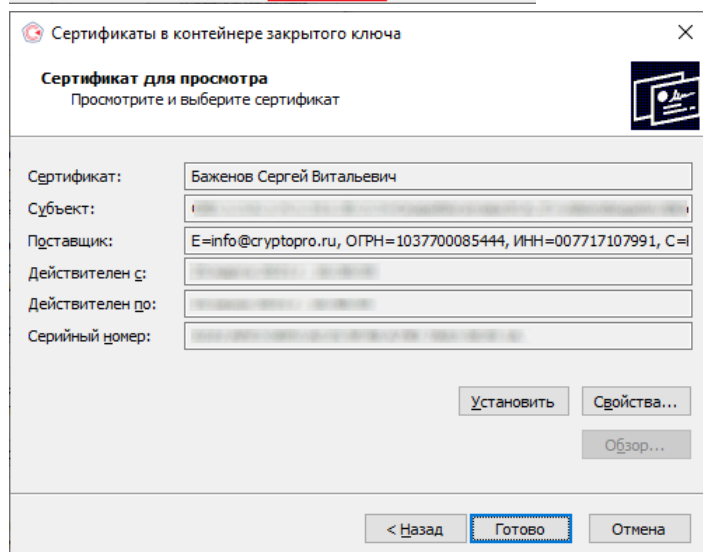
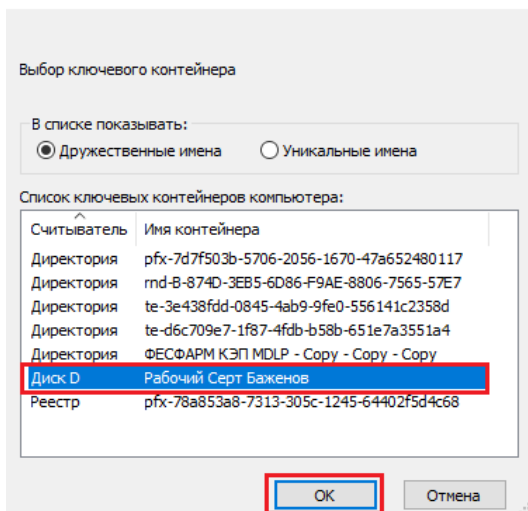
- Нажмите кнопку «Просмотреть сертификаты в контейнере». Откроется окно «Сертификаты в контейнере закрытого ключа». На этой форме в пункте «Введенное имя задает ключевой контейнер» необходимо установить флаг в пункте «Компьютера» (возможно только в случае если вы открыли КриптоПро CSP от имени администратора).



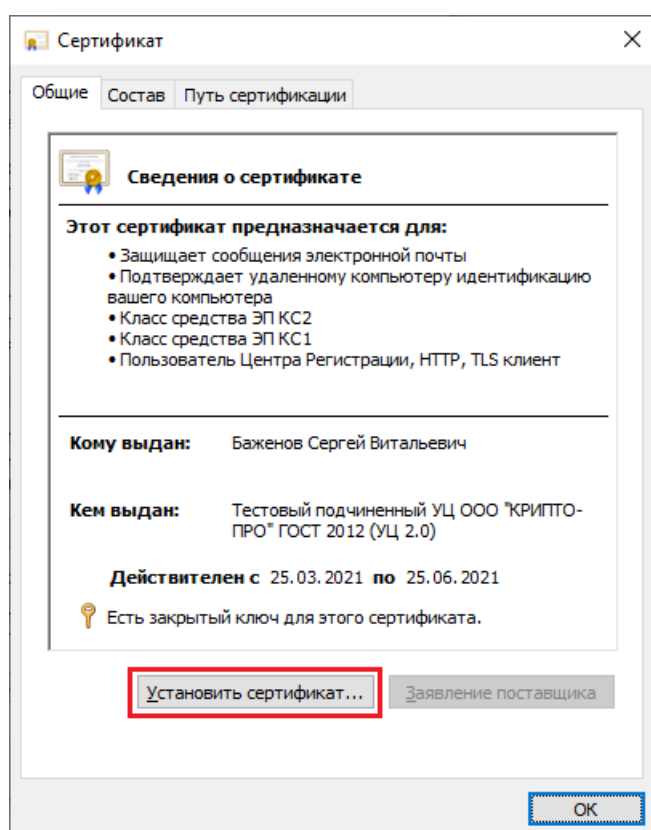
- Далее необходимо заполнить поле «Имя ключевого контейнера». Оно может быть введено вручную или найдено в списках контейнеров (кнопка «Обзор») или сертификатов (кнопка «По сертификату»). Если сертификат в выбранном контейнере имеется, откроется окно «Сертификат для просмотра».



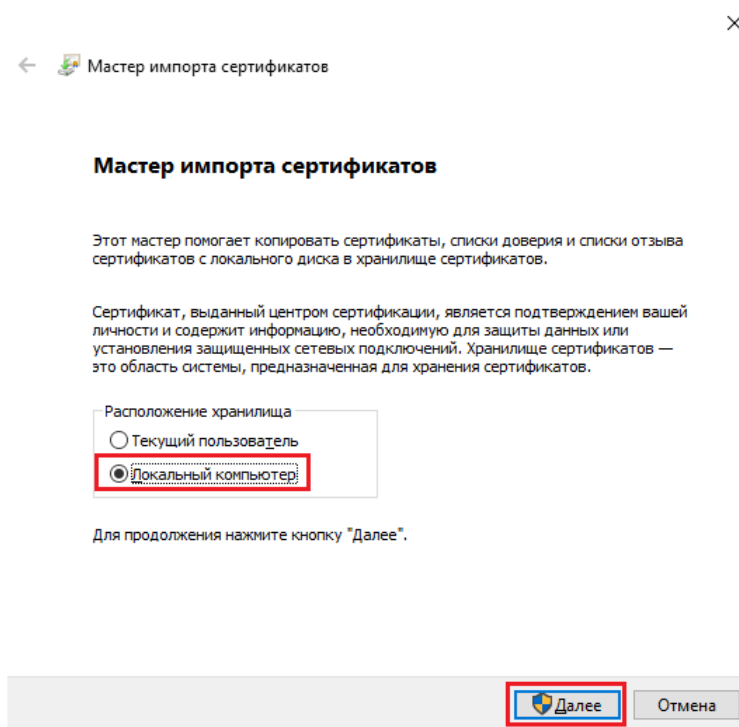
## Выбор контейнера - КриптоПро CSP



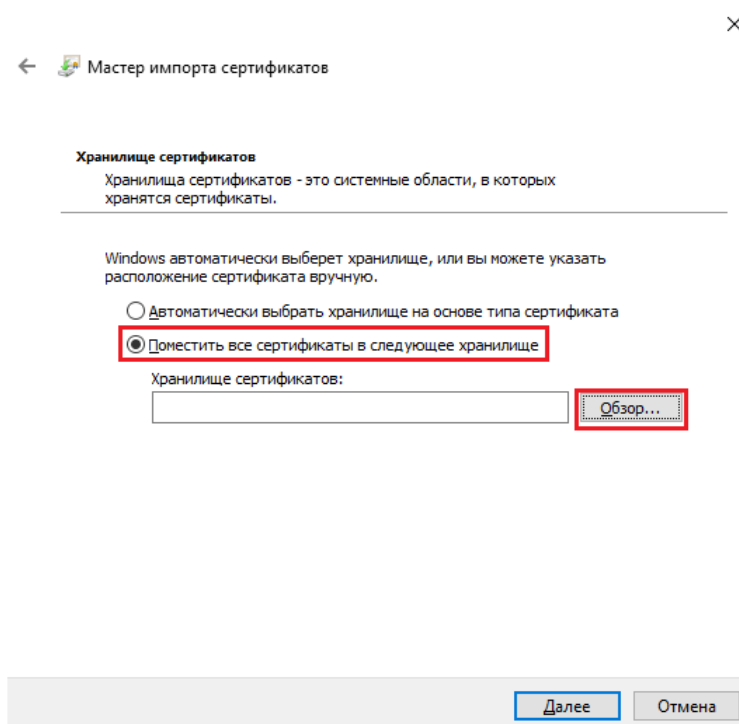
- В окне «Сертификаты в контейнере закрытого ключа» нажмите кнопку «Установить» (для связи сертификата и закрытого ключа). После этого установите сертификат в личное хранилище («Свойства» → «Установить сертификат»).

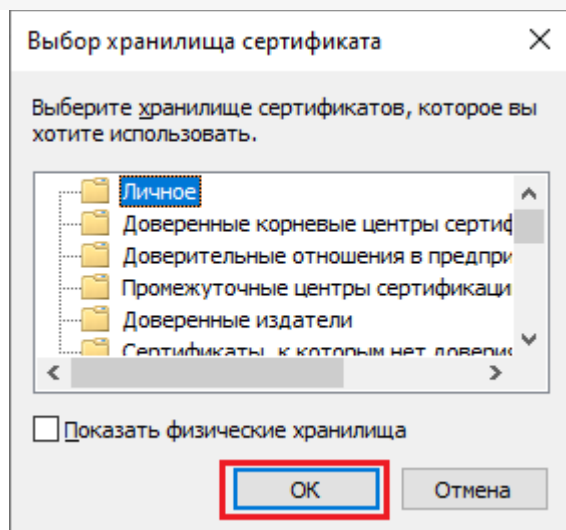


- В качестве расположения хранилища выберите «Локальный компьютер» и нажмите кнопку «Далее».



- В следующем окне выберите пункт «Поместить все сертификаты в следующее хранилище», нажмите кнопку «Обзор» и из списка хранилищ выберите «Личное».



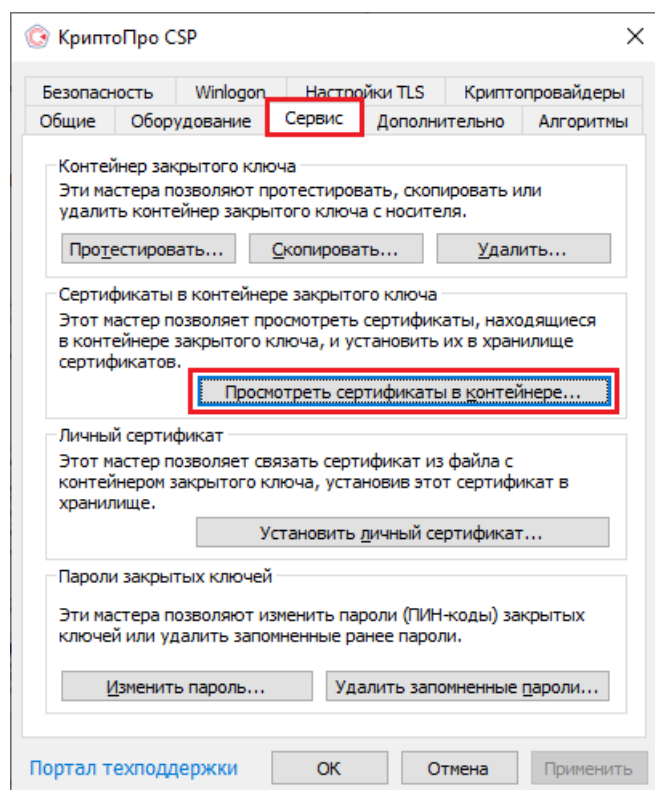


- Нажмите «ОК» → «Далее» → «Готово».

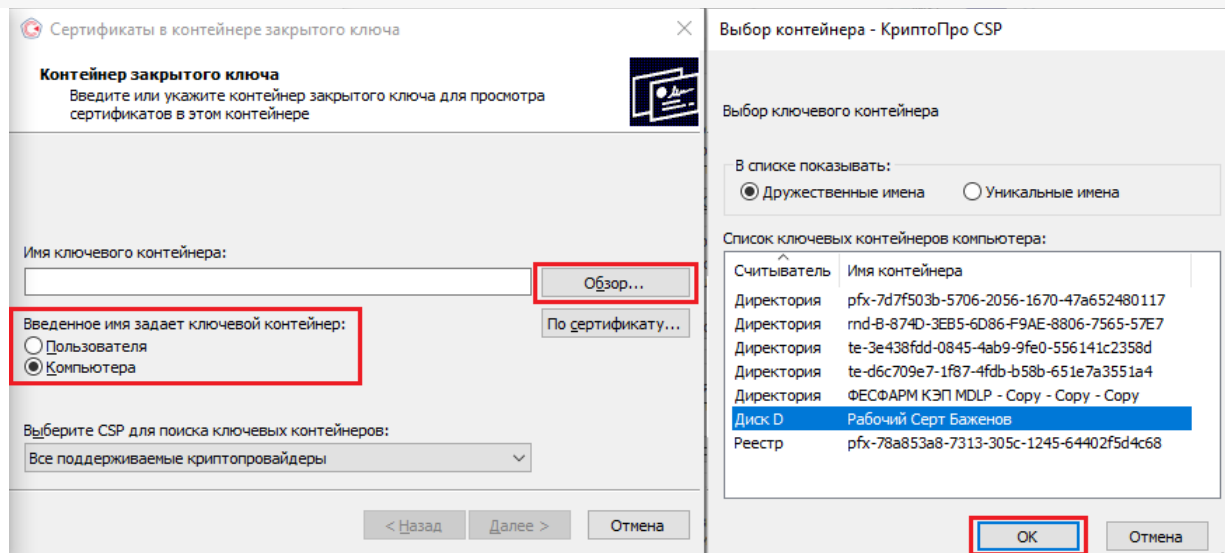
## Проверка и сопоставление текущего личного сертификата и сертификата в контейнере

Данное действие можно выполнить двумя способами.

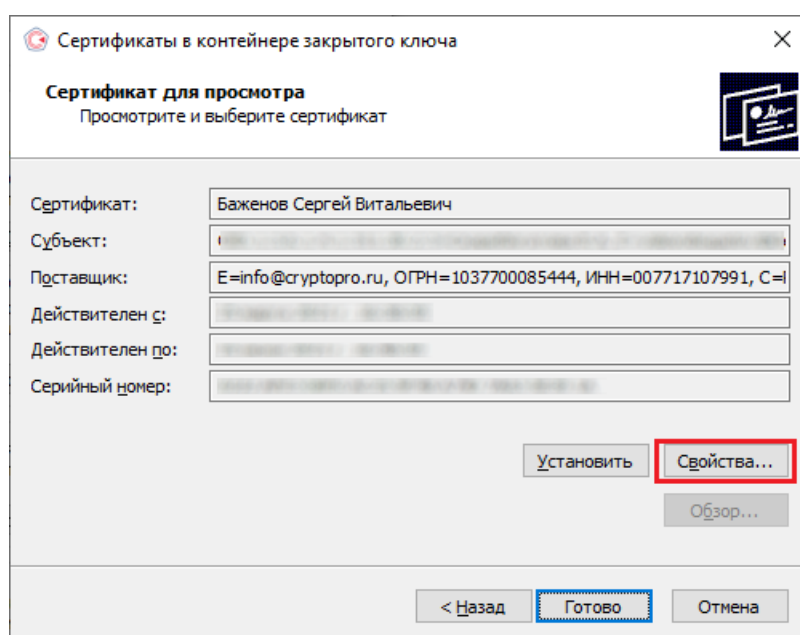
**Способ 1.** Сравнить отпечатки сертификата в контейнере и сертификата, установленного на ПК. Для проверки сертификата в контейнере нужно запустить КриптоПРО CSP от имени администратора, перейти во вкладку «Сервис» и нажать на кнопку «Просмотреть сертификаты в контейнере».



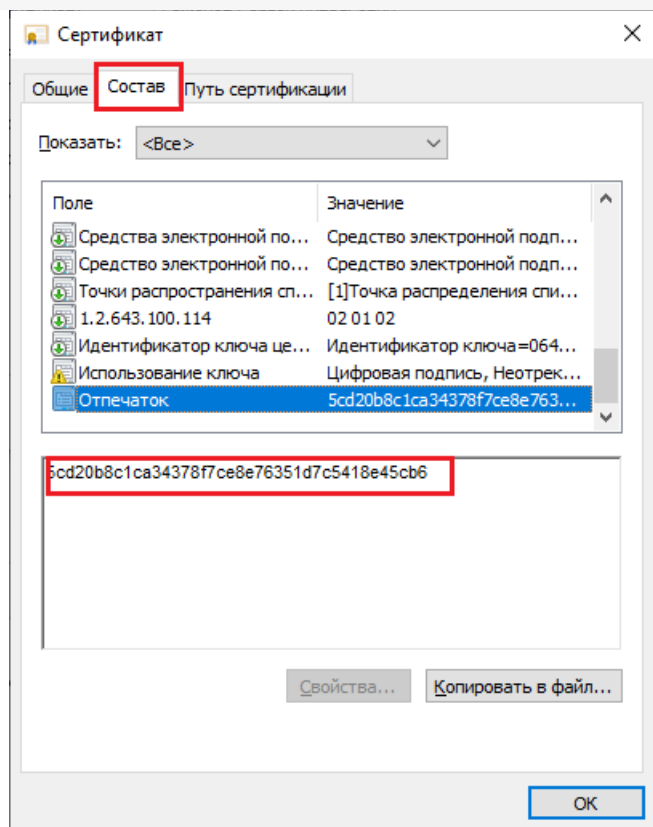
В открывшемся окне нужно выбрать «Введенное имя задает ключевой контейнер» — «Компьютер», далее нажать на кнопку «Обзор», выбрать контейнер из списка и нажать «ОК».



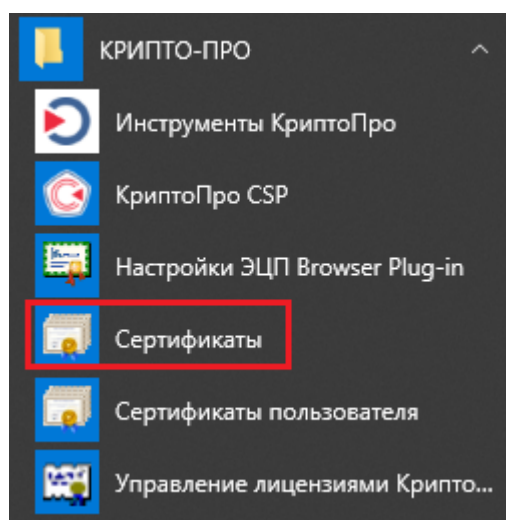
Откроется окно с информацией о сертификате, в котором необходимо нажать на кнопку «Свойства».



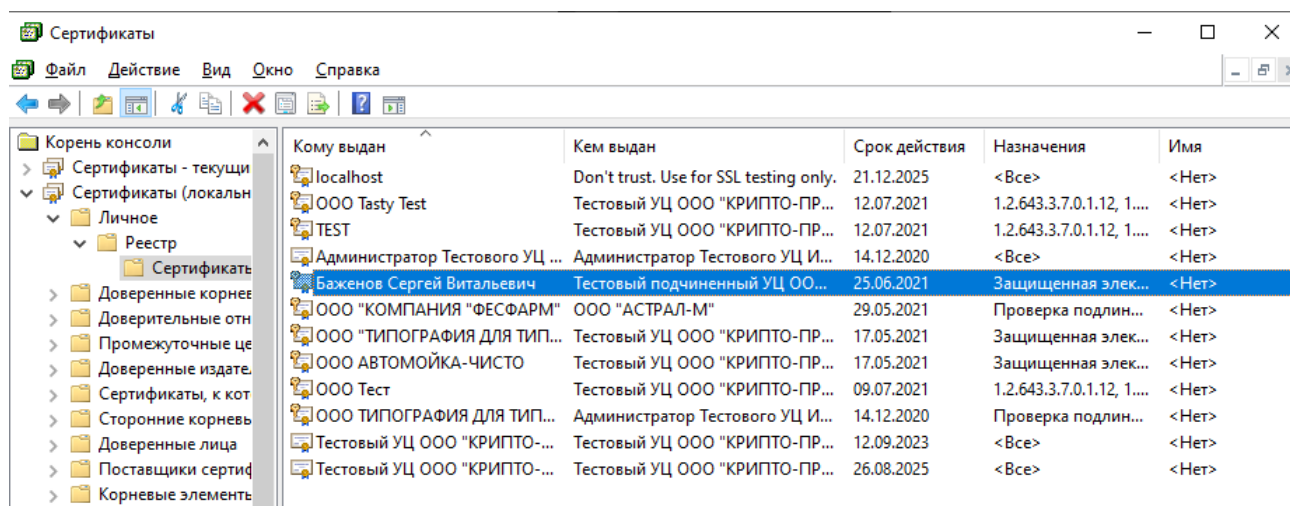
В открывшемся окне перейдите на вкладку «Состав». Вам нужна строка-отпечаток, которую вы можете сравнить наглядно со строкой-отпечатком, установленным на ПК.



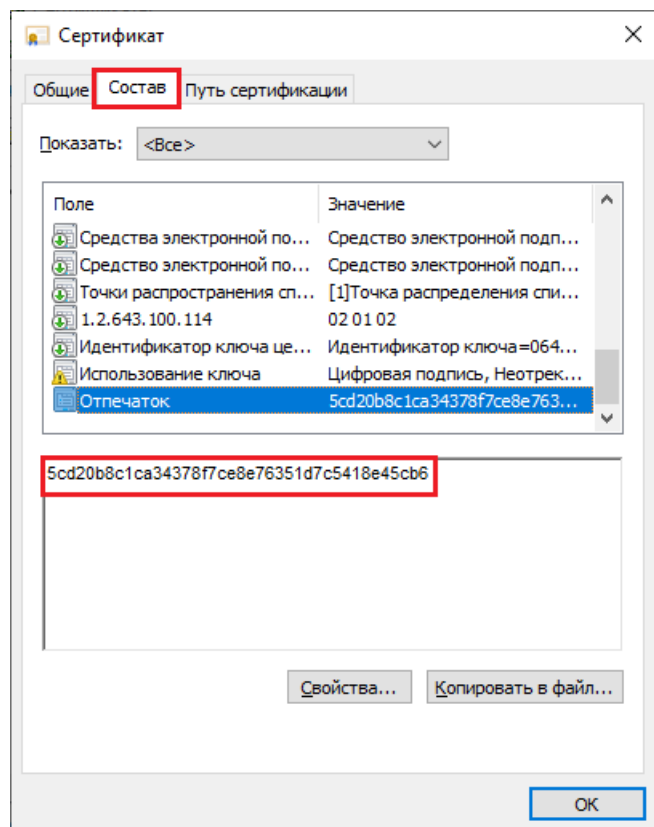
Для того чтобы сверить данный отпечаток с сертификатом, установленным на ПК, необходимо открыть ПУСК → КРИПТО-ПРО → Сертификаты.



В открывшемся окне сертификатов выберите «Сертификаты (локальный компьютер)» → «Личное» → «Реестр» → «Сертификаты», и выберите нужный вам сертификат.

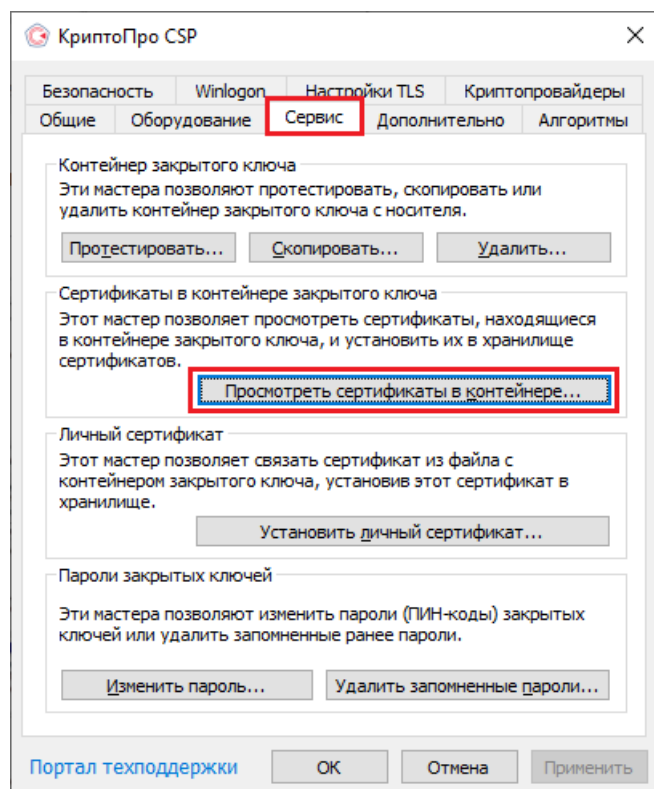


В окне сертификата перейдите на вкладку «Состав», где будет указана строка-отпечаток.

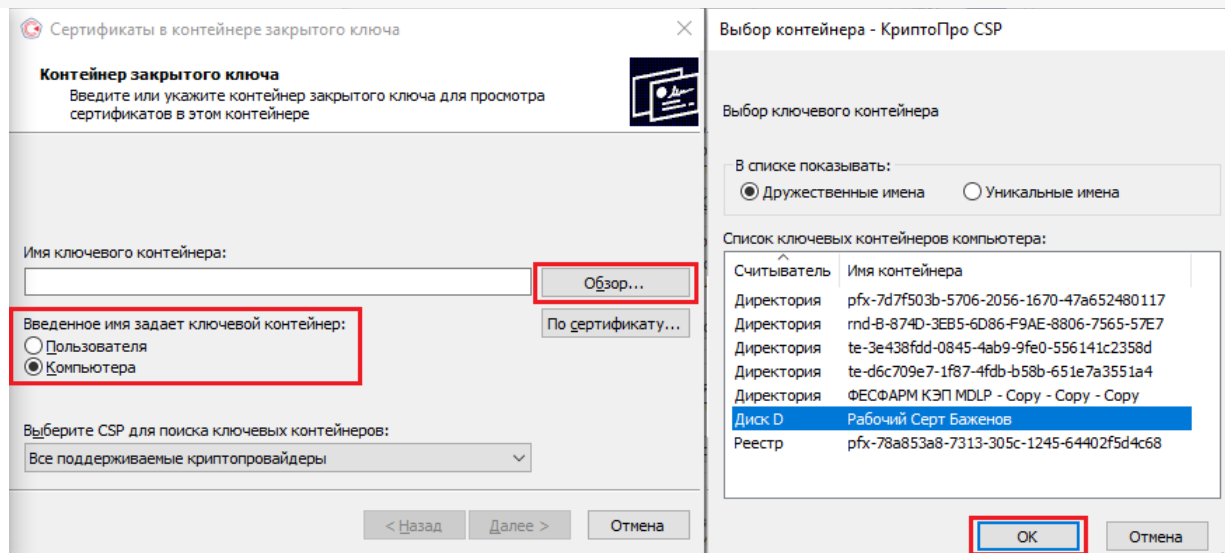


После этого вы можете сравнить два отпечатка.

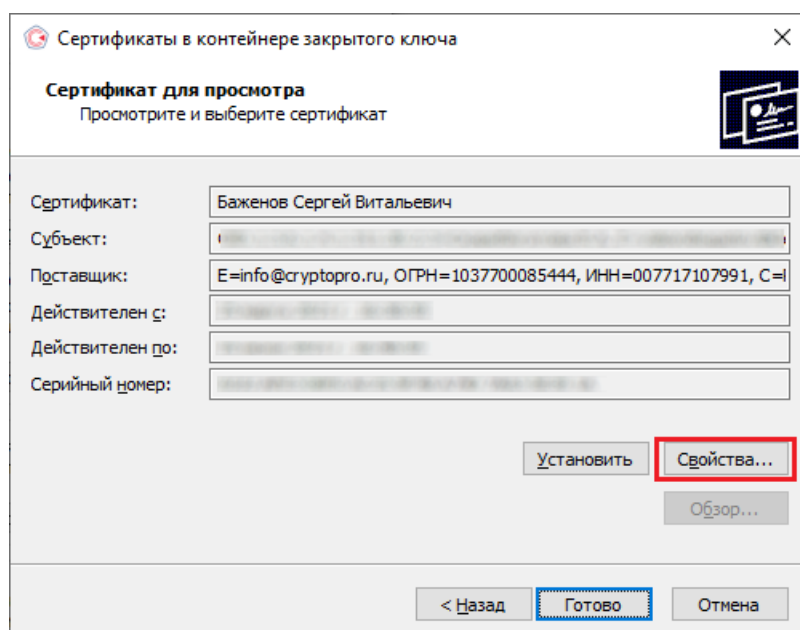
**Способ 2.** Переустановить сертификат на ПК из контейнера. Для этого запустите КриптоПРО CSP от имени администратора, перейдите во вкладку «Сервис» и нажмите на кнопку «Просмотреть сертификаты в контейнере».



В открывшемся окне нужно выбрать «Введенное имя задает ключевой контейнер» — «Компьютер», далее нажать на кнопку «Обзор», выбрать контейнер из списка и нажать «ОК».



Откроется окно с информацией о сертификате, в котором необходимо нажать на «Свойства» → «Установить сертификат».



В качестве хранилища сертификата необходимо выбрать «Локальный компьютер».

## Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

☐ Текущий пользователь

☒ Локальный компьютер

Для продолжения нажмите кнопку "Далее".

Далее

Отмена

В следующем окне необходимо выбрать «Поместить все сертификаты в следующее хранилище» → «Обзор» → «Личное».

### 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:

Обзор...

Далее

Отмена

Нажмите «Далее» → «Готово». После этого импорт сертификата будет успешно выполнен.



Не нашли что искали?



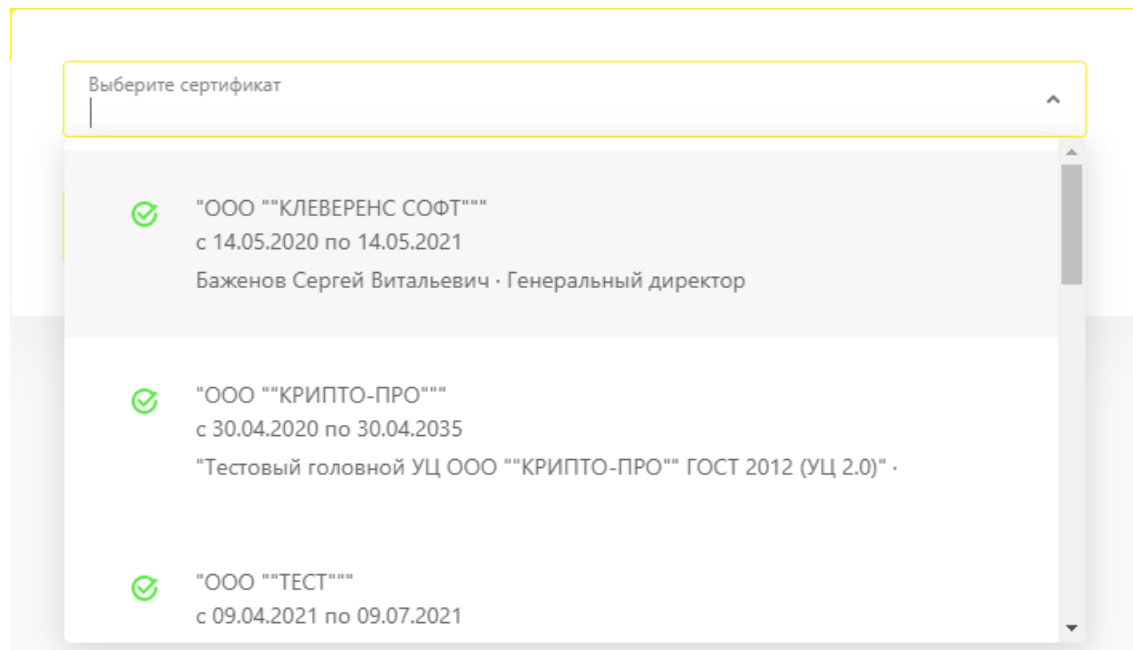
Задать вопрос в техническую поддержку

# Подключение к станции управления заказами

Последние изменения: 2024-03-26

Для подключения к СУЗ потребуется [установить контейнер закрытого ключа](#) на пользователя. После этого появится возможность подключиться к portalу СУЗ (демонстрационный режим для тестирования).

После установки контейнера на пользователя он будет доступен для выбора на сайте СУЗ.



Не нашли что искали?



Задать вопрос в техническую поддержку

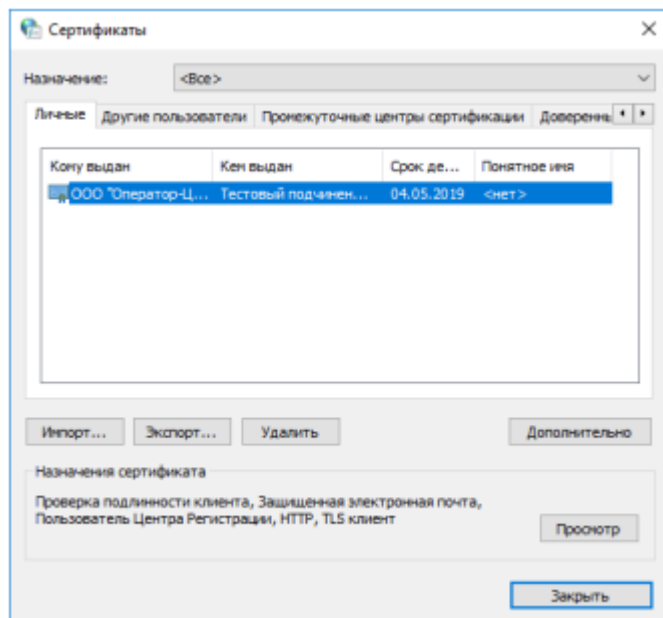
# Построение цепочки доверия КСКПЭП

Последние изменения: 2024-03-26

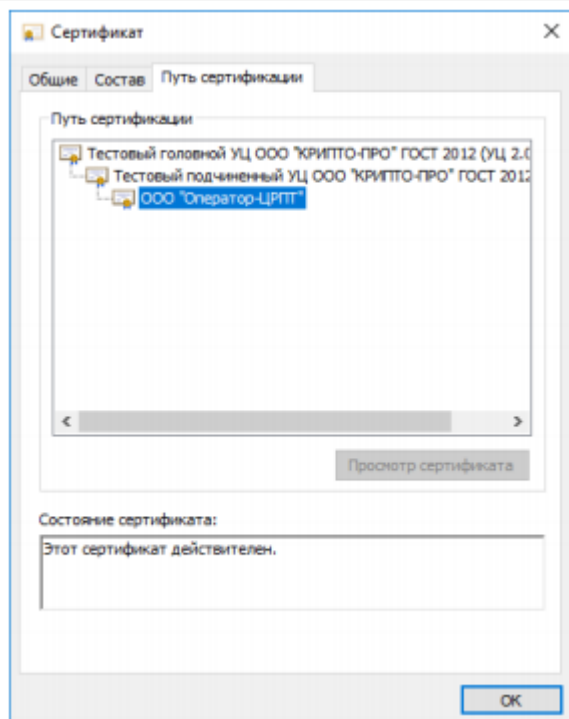
Для того чтобы выстроить цепочку доверия КСКПЭП, необходимо:

- В меню «Пуск» выберите «Панель управления» → «Свойства браузера» → вкладка «Содержание» → «Сертификаты». Откройте вкладку «Личные»:

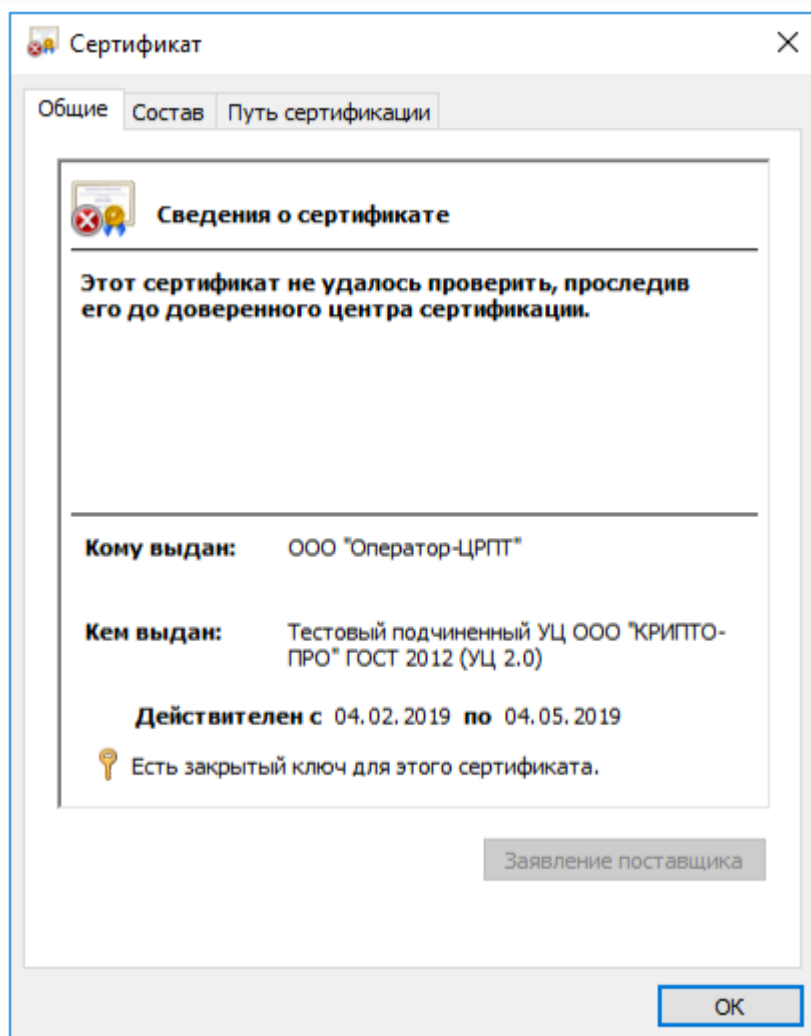
Если в данном окне не отображаются сертификаты, это значит, что ранее не был произведен импорт сертификатов на пользователя. Чтобы сертификаты отображались во вкладке «Личные», необходимо **после их установки** прописать их и на локальный компьютер, и на текущего пользователя. Если после этих действий сертификаты все равно не отображаются, а работа происходит в тестовой среде, то следует **скачать и установить промежуточный сертификат тестового удостоверяющего центра**, импортировать их и на локальный компьютер, и на пользователя, а затем вновь открыть вкладку с сертификатами.



- Выберите установленный сертификат, кликнув по нему два раза левой кнопкой мыши. Перейдите на вкладку «Путь сертификации»:

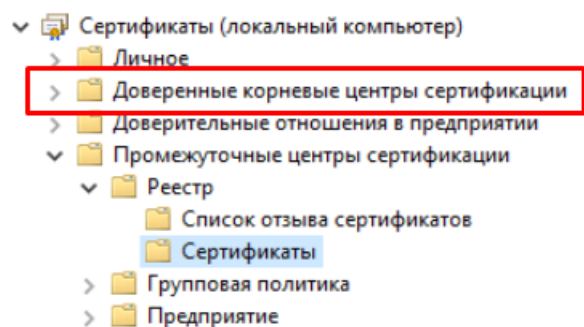


- На вкладке «Путь сертификации» должна отображаться цепочка сертификатов, с помощью которых устанавливается доверие. Если цепочка не сформирована, потребуется добавить сертификаты самостоятельно (см. ниже). Если какой-то из этих сертификатов не будет установлен, то при подключении к СУЗ будут появляться ошибки. В поле «Состояние сертификата» должно отображаться сообщение о действительности сертификата. В случае если во вкладке «Общие» → «Сведения о сертификате» отображается «Этот сертификат не удалось проверить, проследив его до доверенного центра сертификации» — необходимо установить корневой сертификат ГУЦ и удостоверяющего центра, выдавшего вашу электронную подпись (как это сделать с помощью мастера импорта сертификатов, смотрите пункт 3).











У демонстрационного и рабочего сертификата разные цепочки сертификации, поэтому если будет установлены данные частично от одного и от другого сертификата, ничего работать не будет.

Сертификат Головного Удостоверяющего Центра и удостоверяющего центра, выдавшего КСКПЭП юридическому лицу, будут размещаться в хранилище сертификатов «Доверенные корневые центры сертификации».



Остальные сертификаты цепочки будут размещаться в хранилище сертификатов «Промежуточные центры сертификации». Как их туда добавить самостоятельно с помощью мастера импорта сертификатов, описано в пункте 3, с отличием в том, что при выборе хранилища сертификатов указываются «Промежуточные центры сертификации».

- ▼  Сертификаты (локальный компьютер)
  - >  Личное
  - >  Доверенные корневые центры сертификации
  - >  Доверительные отношения в предприятии
  - ▼  Промежуточные центры сертификации
    - ▼  Реестр
      -  Список отзыва сертификатов
      -  Сертификаты

Не нашли что искали?



[Задать вопрос в техническую поддержку](#)

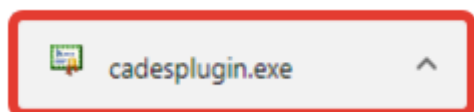
# Установка КриптоПро ЭЦП Browser plug-in

Последние изменения: 2024-03-26

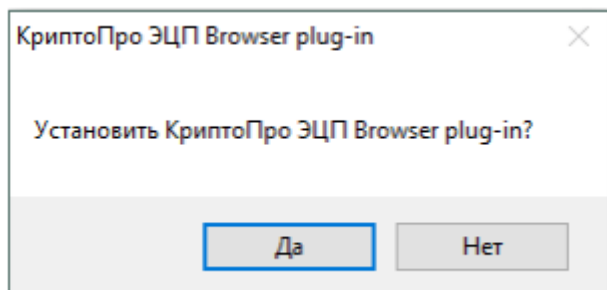
Для корректного функционирования веб-страниц, использующих КриптоПро ЭЦП Browser plug-in, недостаточно расширения для браузера. Сначала необходимо скачать установочный файл и установить его.

Для работы плагина требуется установленный КриптоПро CSP версии 3.6 R4 и выше. Дистрибутив и инструкцию по установке можно получить по [ссылке](#).

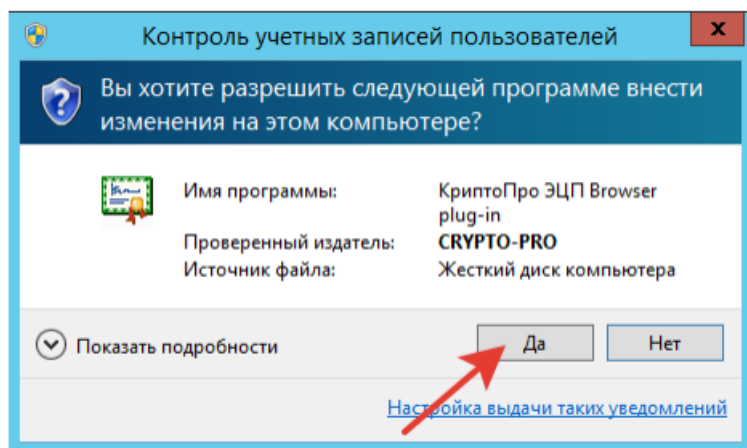
- Скачайте программу установки. КриптоПро ЭЦП Browser plug-in доступен по [ссылке](#).
- Запустите исполняемый файл cadesplugin.exe.



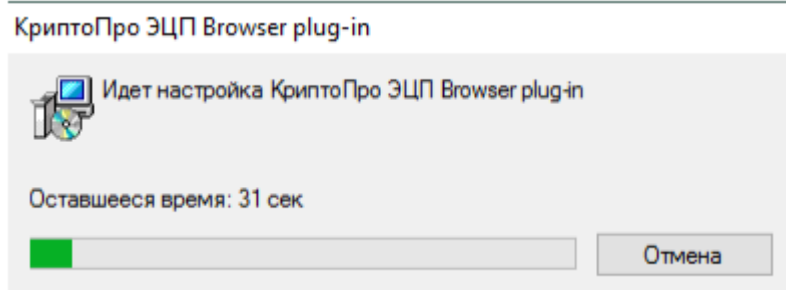
- Подтвердите установку КриптоПро ЭЦП Browser plug-in.



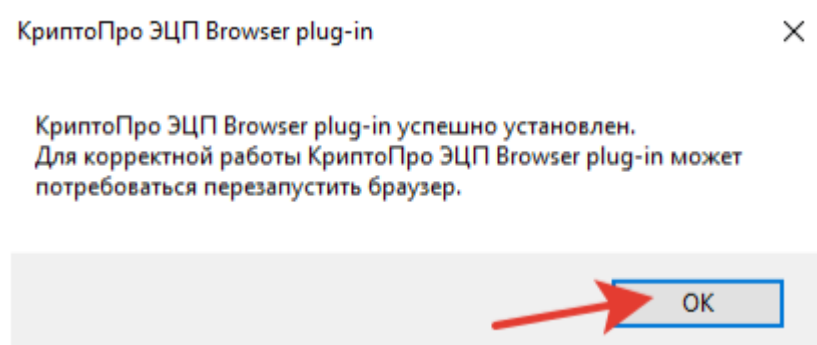
- Если потребуется, разрешите КриптоПро ЭЦП Browser plug-in внести изменения путем нажатия кнопки «Да».



- Дождитесь окончания установки КриптоПро ЭЦП Browser plug-in.

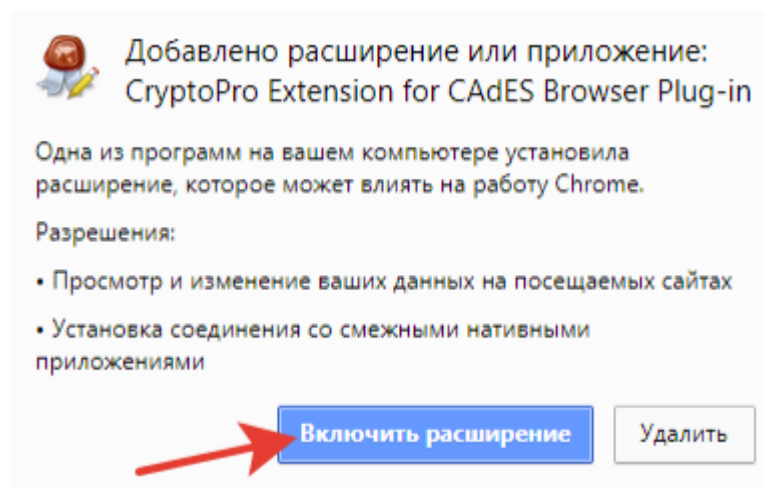


- После окончания установки КриптоПро ЭЦП Browser plug-in нажмите ОК.



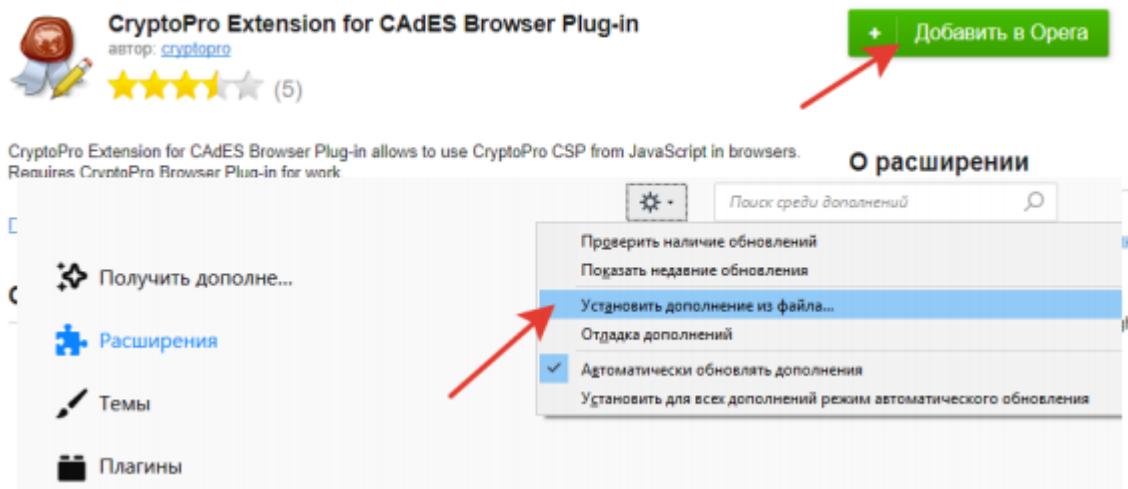
- Дальнейшие настройки различаются в зависимости от используемого браузера.

**Браузер Chrome:** запустите Chrome и дождитесь оповещения об установленном расширении «CryptoPro Extension for CAdES Browser Plug-in». Включите это расширение. Если на Вашем компьютере ранее уже выполнялась установка КриптоПро ЭЦП Browser plug-in, а потом он был удален, потребуется отдельно установить расширение. Для этого перейдите по [ссылке](#) и установите расширение из интернет-магазина Chrome.



**Браузер Opera или Яндекс.Браузер:** расширение доступно по [ссылке](#).

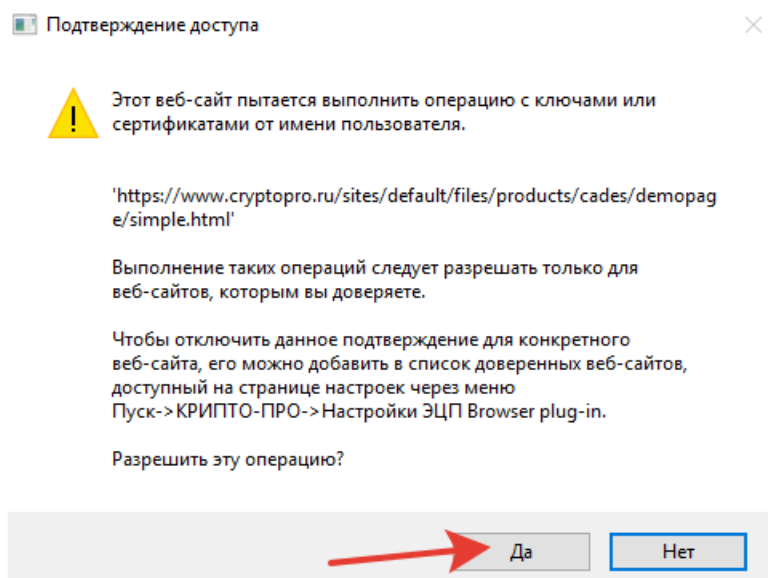




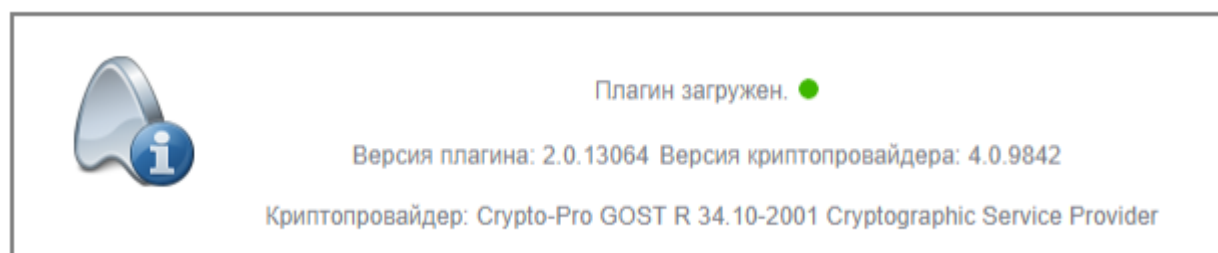
Браузер Firefox: скачайте расширение по [ссылке](#) и установите в браузер самостоятельно.

Браузер Microsoft Internet Explorer: не требуется дополнительных настроек.

- Проверьте корректность установки на [странице проверки плагина](#). Для этого в открывшемся окне подтвердите доступ путем нажатия кнопки «Да».



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



Не нашли что искали?



Задать вопрос в техническую поддержку