

РЕКОМЕНДАЦИИ

**по работе с усиленной квалифицированной электронной подписью
при использовании личного кабинета финансовой организации,
размещенного на официальном сайте финансового уполномоченного в сети
«Интернет»**

Содержание:

1. Общая информация.	3
1.1. Область применения и необходимость использования финансовой организацией электронной подписи.	3
1.2. Требования к программному и информационному обеспечению.	3
1.3. Получение финансовой организацией электронной подписи.	4
2. Подготовка к работе.	5
2.1. Настройка браузера Internet Explorer.	5
2.2. Установка плагина для электронной подписи.	6
2.3. Импорт сертификата удостоверяющего центра.	9
2.4. Установка КриптоПро CSP	12
2.5. Проверка программных средств и решение проблем.	23
3. Создание и подписание исходящего документа в личном кабинете финансовой организации.	23

1. Общая информация

1.1. Область применения и необходимость использования финансовой организацией электронной подписи

Взаимодействие финансового уполномоченного с финансовыми организациями осуществляется посредством использования информационного ресурса, размещённого на официальном сайте финансового уполномоченного в информационно-телекоммуникационной сети Интернет, путем предоставления финансовым организациям доступа к личному кабинету финансовой организации (далее – Личный кабинет).

Ведение личного кабинета осуществляется Автономной некоммерческой организацией «Служба обеспечения деятельности финансового уполномоченного» (далее – АНО «СОДФУ»).

Личный кабинет представляет собой web-приложение, доступ к которому осуществляется с использованием сети «Интернет».

В соответствии с Федеральным законом от 04.06.2018 № 123-ФЗ «Об уполномоченном по правам потребителей финансовых услуг» и Положением¹ о порядке ведения службой обеспечения деятельности финансового уполномоченного личного кабинета финансовой организации и личного кабинета потребителя финансовых услуг (далее – Положение), утвержденным решением Совета Службы финансового уполномоченного от 07.12.2018 (Протокол № 1), при работе с Личным кабинетом финансовой организацией должна использоваться усиленная квалифицированная электронная подпись юридического лица или физического лица (далее – УКЭП) в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – Закон № 63-ФЗ), позволяющая идентифицировать владельца квалифицированного сертификата ключа проверки электронной подписи (далее – квалифицированный сертификат) и обеспечить целостность электронного документа.

Финансовая организация должна использовать квалифицированный сертификат, который выдается удостоверяющим центром, аккредитованным Министерством связи и массовых коммуникаций Российской Федерации (далее – Минкомсвязи России) в соответствии с пунктом 1 части 2 статьи 8 Закона № 63-ФЗ.

1.2. Требования к программному и информационному обеспечению

Документы, предоставляемые финансовой организацией через Личный кабинет, должны быть подписаны УКЭП, созданной с применением криптографических средств, сертифицированных ФСБ России, и сертификата от удостоверяющего центра, аккредитованного Минкомсвязи России.

Электронный документ, подписанный УКЭП, по юридической силе равнозначен документу, изготовленному на бумажном носителе и подписанному собственноручно.

В соответствии с пунктом 3 статьи 14 Закона № 63-ФЗ в случае выдачи сертификата ключа проверки электронной подписи юридическому лицу в качестве владельца сертификата ключа проверки электронной подписи наряду с указанием наименования юридического лица указывается физическое лицо, действующее от имени юридического лица на основании учредительных документов юридического лица или доверенности.

В целях предотвращения отзыва сертификата пользователям Личного кабинета необходимо самостоятельно отслеживать истечение срока действия сертификата.

¹ Размещено на официальном сайте финансового уполномоченного в сети «Интернет» по адресу <https://finombudsman.ru/> в разделе «Регулирование».

При наличии необходимости пользователи Личного кабинета могут выполнить повторную загрузку действующего сертификата. Для выпуска сертификата для нового пользователя в рамках одной финансовой организации необходимо произвести загрузку сертификата.

Для работы в Личном кабинете АНО «СОДФУ» рекомендует использовать квалифицированный сертификат, выданный удостоверяющим центром ООО «КриптоПро», а также следующие программные средства:

1. Криптопровайдер КриптоПро CSP (<https://www.cryptopro.ru/products/csp>);
2. ПАК «КриптоПро TSP» (<https://www.cryptopro.ru/products/pki/tsp>);
3. Плагин к браузеру КриптоПро ЭЦП Browser plug-in (<https://www.cryptopro.ru/products/cades/plugin>).

Внимание: Указанные программные средства являются лицензируемыми на ограниченный срок, за исключением плагина к браузеру. Продление лицензии необходимо осуществлять своевременно. Пакет на приобретение ключа электронной подписи как правило содержит лицензию на криптопровайдер КриптоПро CSP и всегда включает в себя лицензию на службу времени КриптоПро TSP. В подобном случае лицензия на данное программное обеспечение приобретается отдельно.

Для корректной работы программных средств создания УКЭП в случае использования финансовой организацией квалифицированных сертификатов, выданных иными удостоверяющими центрами, необходимо установить в качестве доверенных сертификаты Головного удостоверяющего центра Минкомсвязи России и аккредитованного удостоверяющего центра ООО «КриптоПро» (подробная информация размещена в сети «Интернет» по адресу <http://q.cryptopro.ru>).

Примечание: При использовании в качестве ключевого носителя сертифицированного USB-ключа eToken перед началом работы с Личным кабинетом eToken необходимо подключить к компьютеру.

Важно: С 01.01.2019 применяется стандарт формирования квалифицированной электронной подписи ГОСТ Р 34.10-2012 (в соответствии с выпиской из письма ФСБ России от 31.01.2014 № 149/7/1/3-58 «О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования»), стандарт ГОСТ Р 34.10-2001 утратил силу.

1.3. Получение финансовой организацией электронной подписи

В соответствии с пунктом 1 части 2 статьи 8 Закона № 63-ФЗ получить усиленную квалифицированную электронную подпись можно в одном из удостоверяющих центров, аккредитованных Минкомсвязи России. Перечень аккредитованных Минкомсвязи России удостоверяющих центров размещен на сайте Минкомсвязи России в сети «Интернет» по web-адресу <http://minsvyaz.ru>.

Внимание: ключ электронной подписи имеет ограниченный срок действия (1 год). Необходимо своевременно получать новый ключ электронной цифровой подписи.

2. Подготовка к работе

Обязательно: Для отправки и приема данных из сети «Интернет» должны быть открыты Порты 80, 443. Необходимо убедиться, что сетевые соединения не блокируются сетевыми экранами.

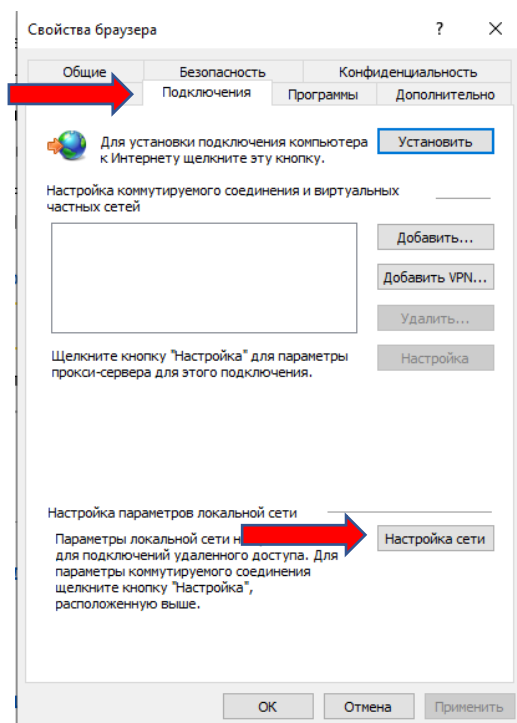
2.1. Настройка браузера Internet Explorer

Рекомендуется использовать актуальную версию браузера Internet Explorer (в зависимости от используемой операционной системы), а также регулярно проводить Windows -обновления и доставлять все необходимые патчи и компоненты безопасности для операционной системы и браузера Internet Explorer. Указанные рекомендации относятся также к иным используемым браузерам.

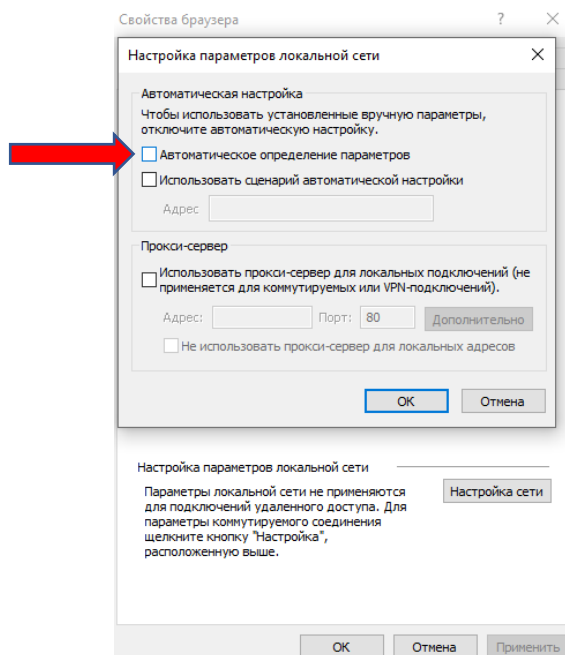
Примечание: В используемом браузере необходимо установить узел <https://finombudsman.ru> в зону надежных узлов.

Перед работой с сайтом финансового уполномоченного (<https://finombudsman.ru>) необходимо осуществить настройку браузера Internet Explorer вне зависимости от того, какая версия браузера используется.

Для настройки необходимо открыть браузер Internet Explorer, в настройках браузера перейти в окно «Свойства браузера (Internet options)», далее во вкладке «Подключения (Connections)» нажать кнопку «Настройка сети (LAN settings)»:



В открывшемся окне необходимо снять галочку напротив «Автоматическое определение параметров (Automatically detect settings)»:



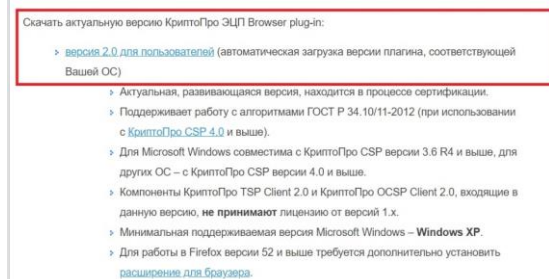
2.2. Установка плагина для электронной подписи

Для установки плагина для электронной подписи необходимо:

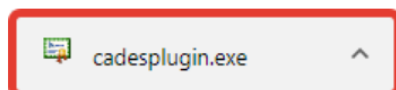
Установить плагин для электронной подписи, перейдя по ссылке:

https://www.cryptopro.ru/products/cades/plugin/get_2_0

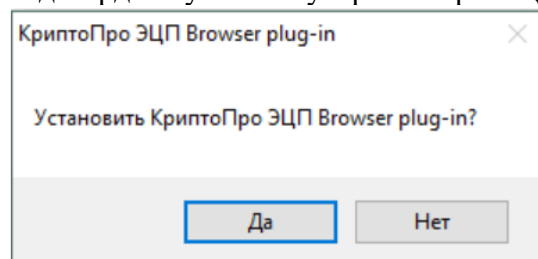
Скачать актуальную версию плагина, ссылка на которую будет отображена в нижней части страницы сайта:



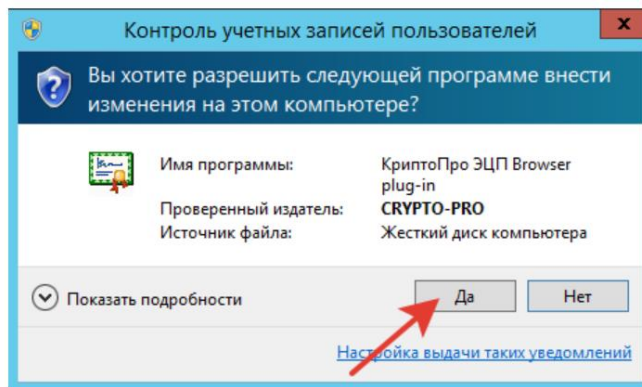
Запустить загруженный файл:



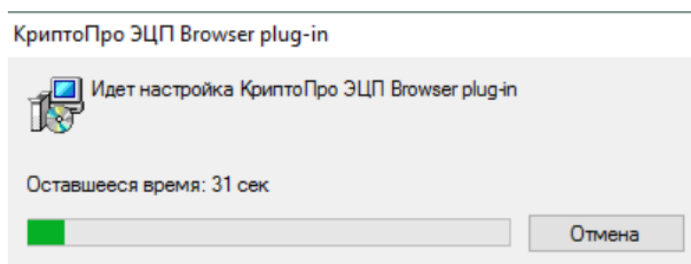
Подтвердить установку КриптоПро ЭЦП Browser plug-in



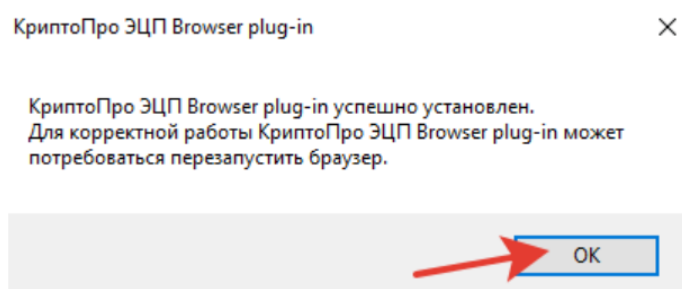
В случае необходимости, разрешить КриптоПро ЭЦП Browser plug-in внести изменения путём нажатия кнопки «Да»:



Дождаться окончания установки КриптоПро ЭЦП Browser plug-in:



После окончания установки КриптоПро ЭЦП Browser plug-in нажать «ОК»:



Дальнейшие настройки различаются в зависимости от используемого браузера.

Для настройки браузера Google Chrome необходимо:

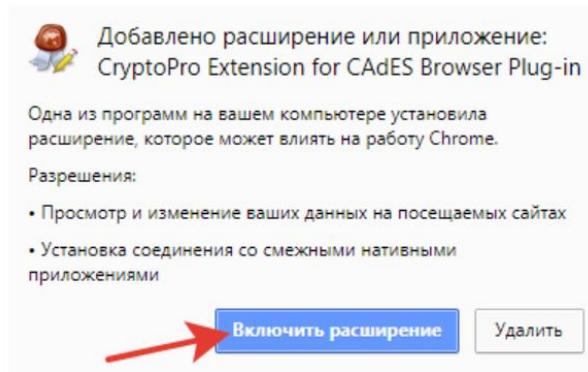
Запустить браузер Chrome и дождаться оповещения об установленном расширении «CryptoPro Extension for CADES Browser Plug-in».

Включить это расширение.

Если на компьютере ранее уже выполнялась установка КриптоПро ЭЦП Browser plug-in, а потом он был удален, требуется отдельно установить расширение. Для этого необходимо скопировать в браузер Chrome следующую ссылку:

<https://chrome.google.com/webstore/detail/cryptopro-extension-for-c/iifchhfnmpdbibifmljnfjhpififfog?hl=ru>

Затем необходимо установить расширение из интернет-магазина Chrome.

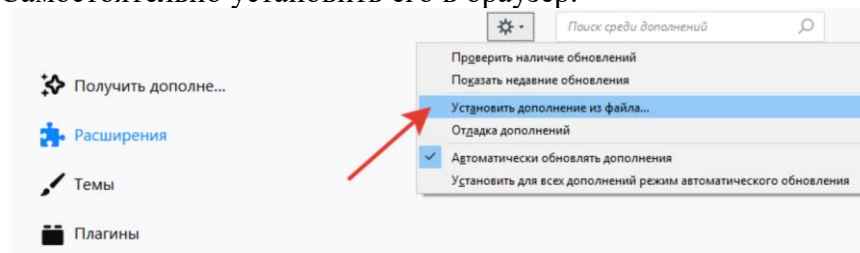


Для настройки Браузера Opera или Яндекс.Браузер необходимо:
Установить расширение, доступное по ссылке:
(<https://addons.opera.com/en/extensions/details/cryptopro-extension-for-ca-des-browser-plug-in>)

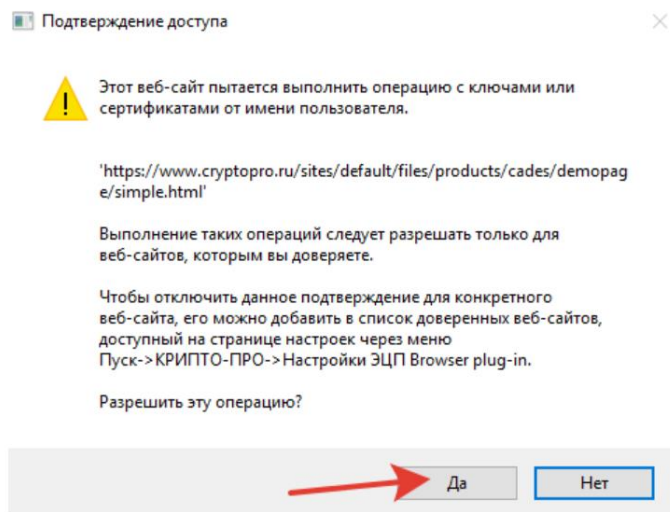


Для настройки браузера Firefox Mozilla необходимо:
Скачать расширение, доступное по ссылке:
(https://www.cryptopro.ru/sites/default/files/products/ca-des/extensions/firefox_cryptopro_extension_latest.xpi)

Самостоятельно установить его в браузер.



Для настройки браузера Microsoft Internet Explorer:
Дополнительная настройка не требуется.
После окончания установки необходимо проверить её корректность на странице проверки плагина по ссылке:
<https://www.cryptopro.ru/sites/default/files/products/ca-des/demopage/simple.html>
В открывшемся окне подтвердить доступ путем нажатия кнопки «Да»:



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

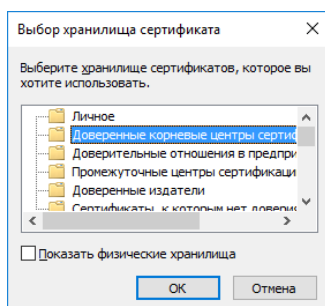
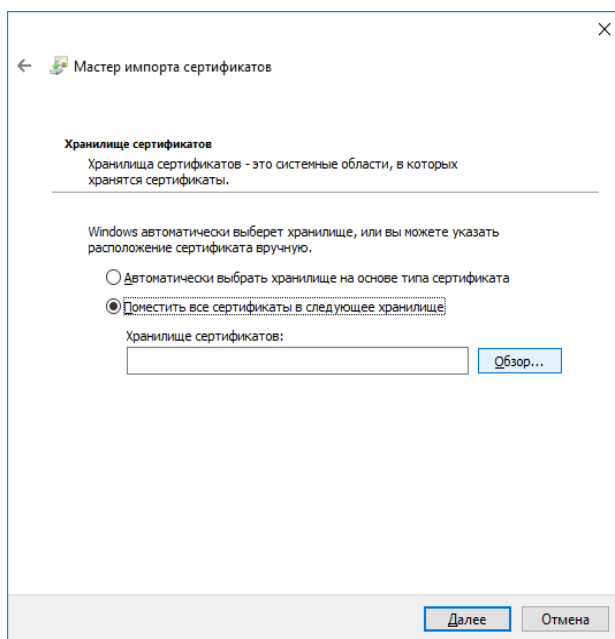
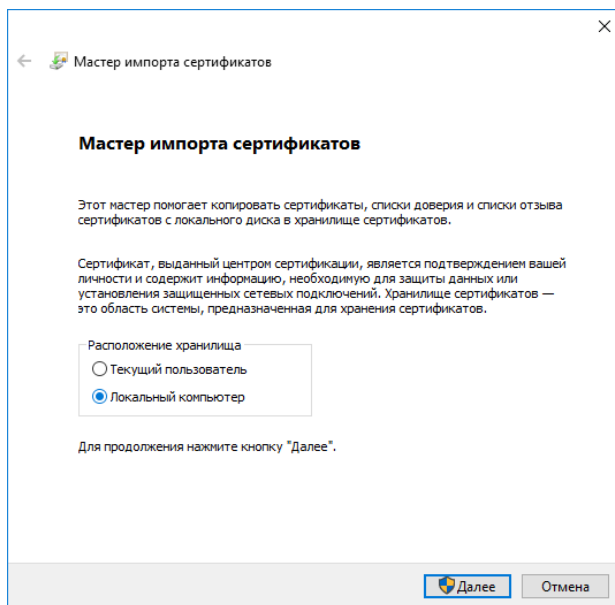


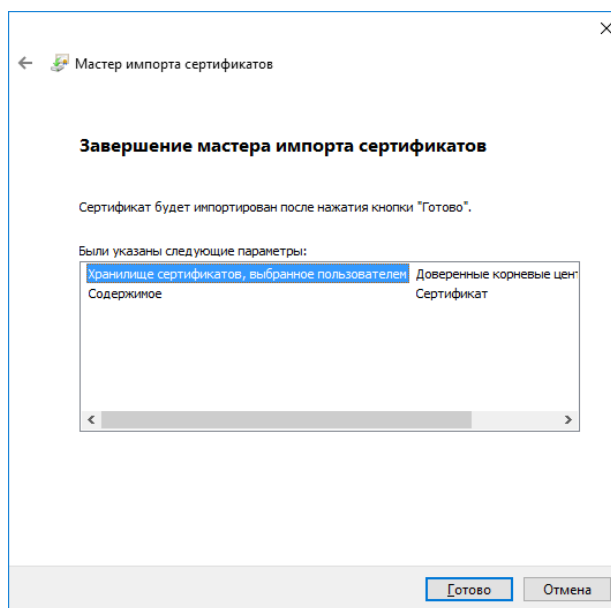
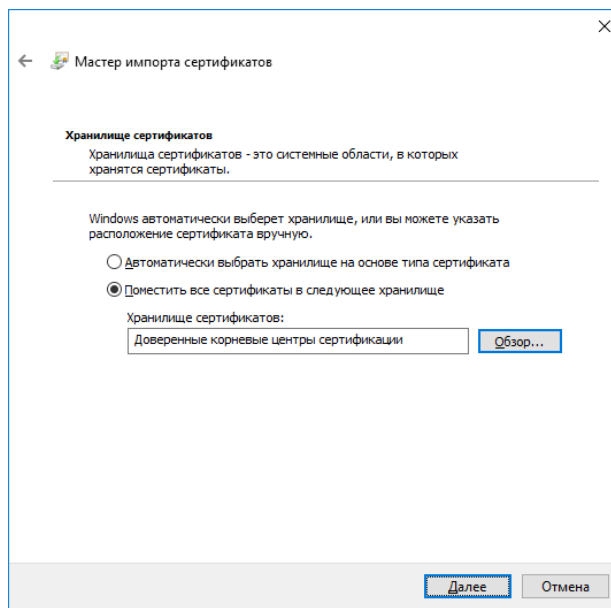
2.3 Импорт сертификата удостоверяющего центра

Для построения цепочки доверия к личному сертификату необходимо выполнить настройку системы и указать, что удостоверяющий центр, выпустивший сертификат, является доверенным. Для этого необходимо получить корневой сертификат или цепочку корневых сертификатов у своего удостоверяющего центра, после чего установить их.

Указанный сертификат или цепочку сертификатов необходимо скачать и установить (через контекстное меню «Установить сертификат»).

В ходе установки необходимо указать место установки сертификата. Рекомендуется устанавливать сертификат в доверенные корневые центры сертификации локального компьютера:

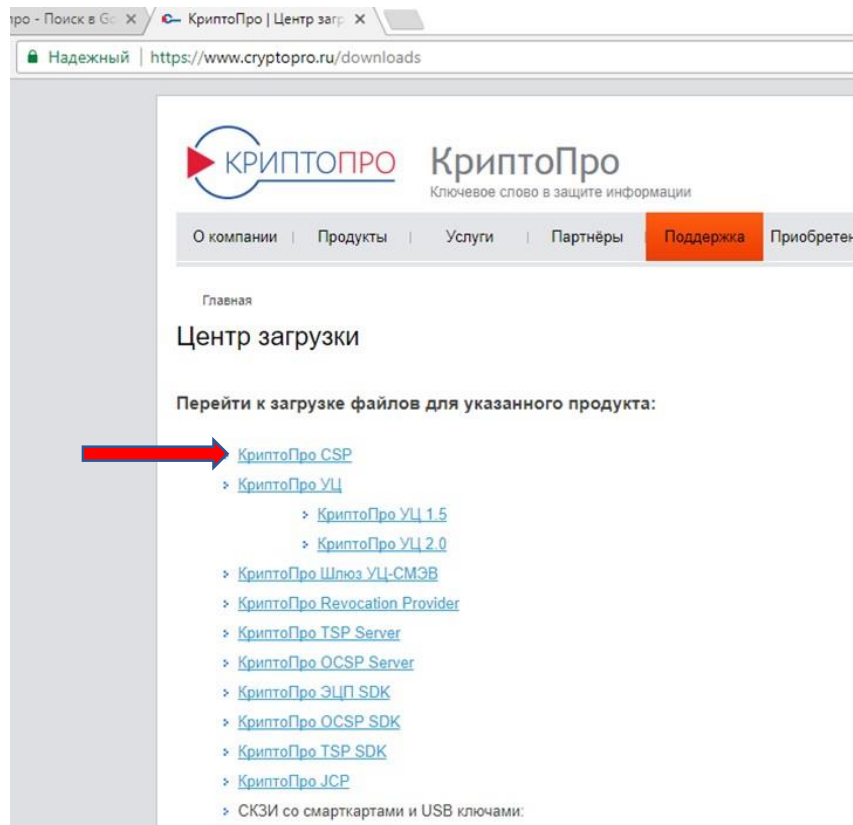




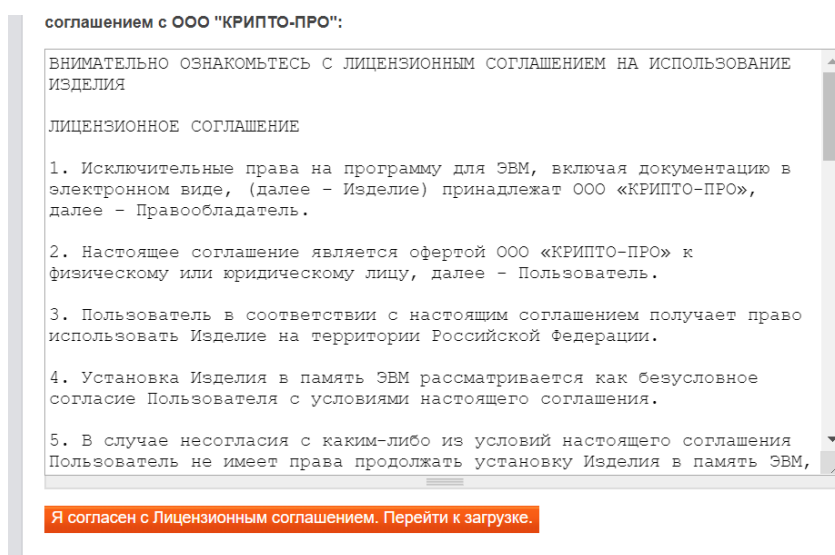
2.4 Установка КриптоПро CSP

Для установки КриптоПро CSP необходимо:

Зайти на сайт [КриптоПро](https://www.cryptopro.ru) и перейти по ссылке «КриптоПро CSP»



После ознакомления с лицензионным соглашением, необходимо нажать кнопку «Я согласен с Лицензионным соглашением. Перейти к загрузке».



Далее необходимо перейти в раздел «КриптоПро CSP 4.0 R2 для Windows, UNIX и macOS» в раздел «Сертифицированные версии»:

Главная > Продукты > СКЗИ КриптоПро CSP

КриптоПро CSP - Загрузка файлов

Предварительные несертифицированные версии

- [КриптоПро CSP 5.0 для Windows, macOS и UNIX](#) (несертифицированный)
- [КриптоПро CSP 4.0 R5 для Windows, macOS и UNIX](#) (несертифицированный)
- [КриптоПро CSP для Google Android](#) (несертифицированный)
- [КриптоПро CSP 3.9 R3 для Windows, UNIX и macOS](#) (несертифицированный)

Сертифицированные версии

- [КриптоПро CSP 4.0 R4 для Windows, macOS и UNIX](#)
- [КриптоПро CSP 4.0 R3 для Windows, macOS и UNIX](#)
- [КриптоПро CSP 3.9 R2 для Windows, UNIX и macOS](#)

иск в G: X КриптоПро | КриптоПро: X

адресный | https://www.cryptopro.ru/products/csp/downloads#latest_csp40r2

Внимание:

- > Все дистрибутивы подписаны цифровой подписью - её можно проверить с помощью обновленной утилиты [cverify](#), [команды для проверки](#)
- > Вопросы можно задать в нашем форуме в ветке [КриптоПро CSP 4.0](#)
- > и на [портале технической поддержки](#).

Документация:

- > [Список изменений \(changelog\)](#)
- > [Документация по установке и использованию КриптоПро CSP 4.0 \(ZIP\)](#)
- > [Документация для разработчиков и примеры \(SDK\)](#)

Для Windows:

- > [КриптоПро CSP 4.0 для Windows](#)

Контрольная сумма

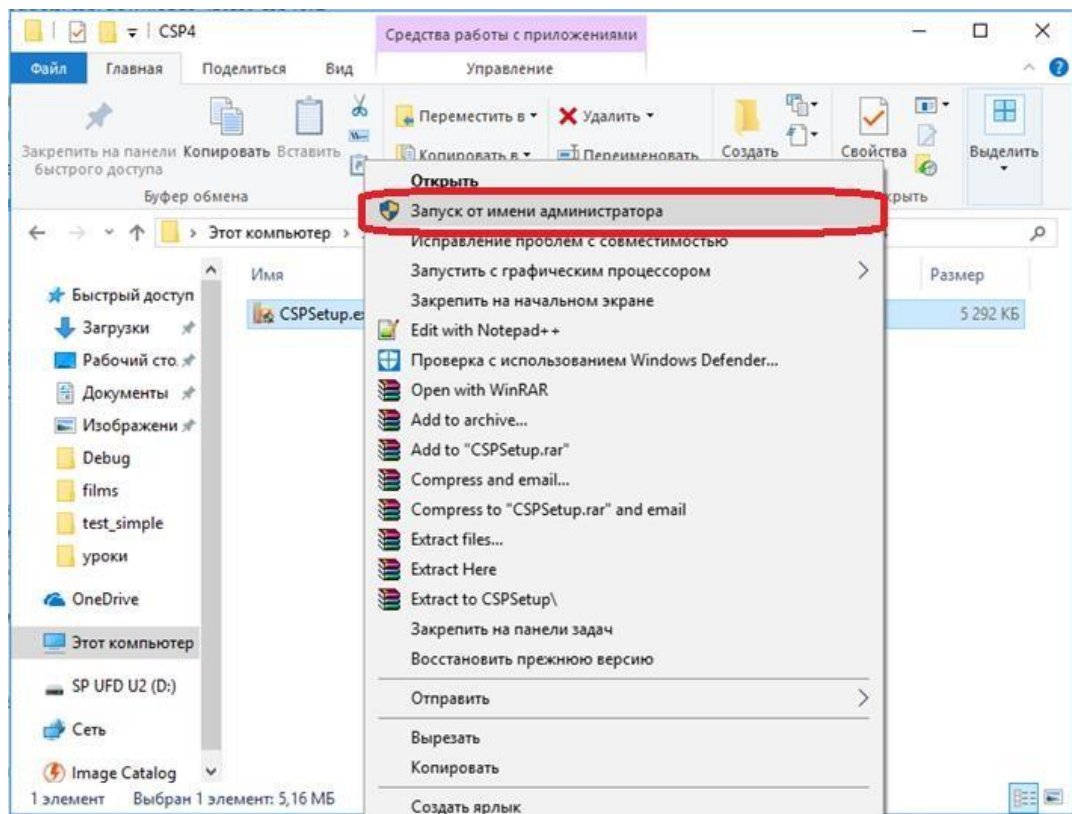
ГОСТ:	86A2828B818135102723A88E97891CF919981CBA8035A12207C98A1E036AD357
ИД5:	0b028b6ef14d0dd5be71068bb6d98b1f

универсальный установщик (настройки, ключи и сертификаты при обновлении сохраняются)

> [Дистрибутивы в формате Windows Installer для автоматизации установки](#)

Скачать по ссылке дистрибутив.

Для установки КryptoПро CSP требуются права администратора компьютера, в связи с этим рекомендуется запускать установщик через контекстное меню и пункт «Запуск от имени администратора»:



Установить программное обеспечение с настройками по умолчанию:



← КристоПро CSP 4.0.9842

Благодарим за выбор КристоПро CSP.

Продолжая установку, Вы принимаете условия Лицензионного соглашения.

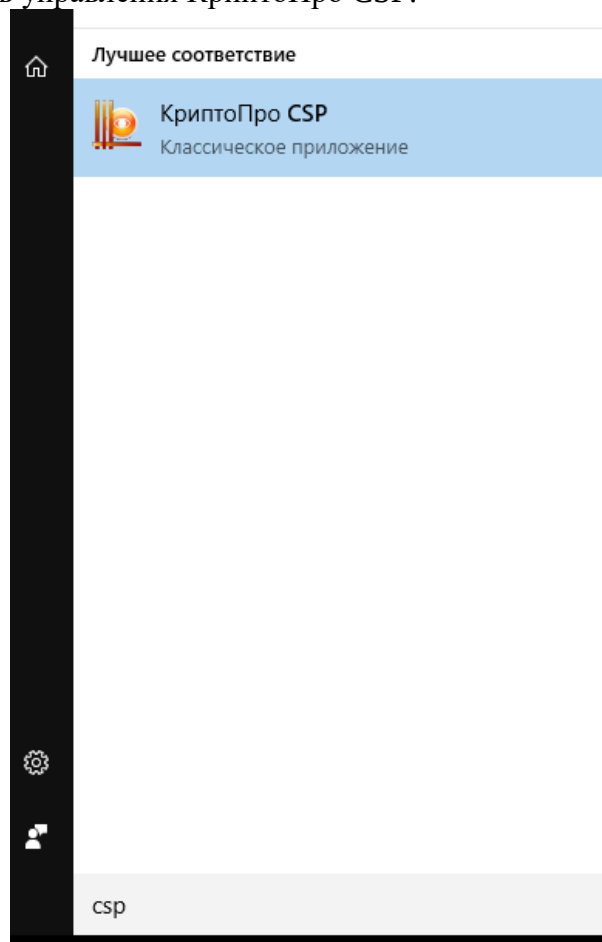
Продукт будет установлен с временной лицензией на 3 месяца.

<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.

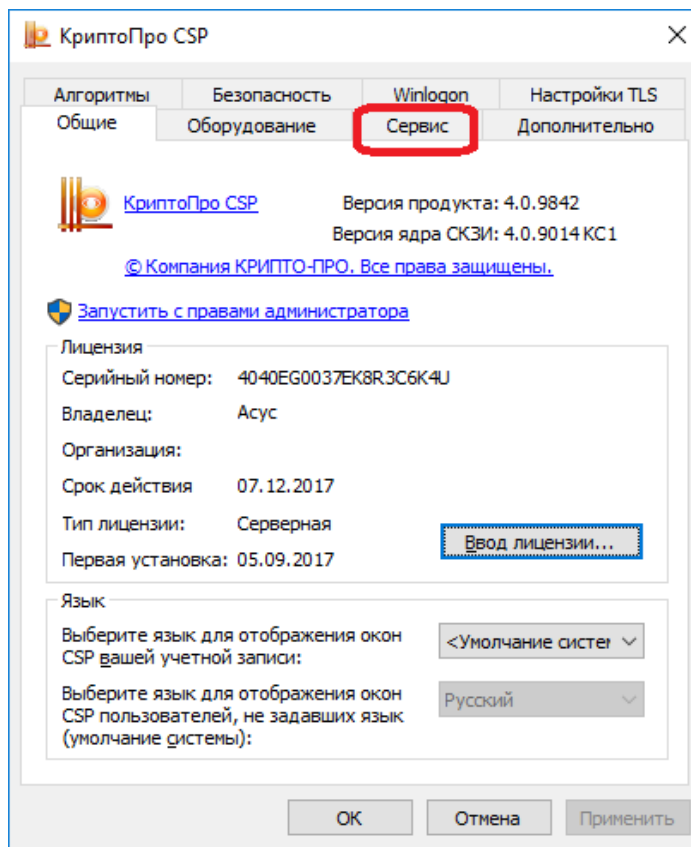
После установки дистрибутива по ключевому слову «CSP» в меню «Пуск» найти панель управления КriptoПро CSP:



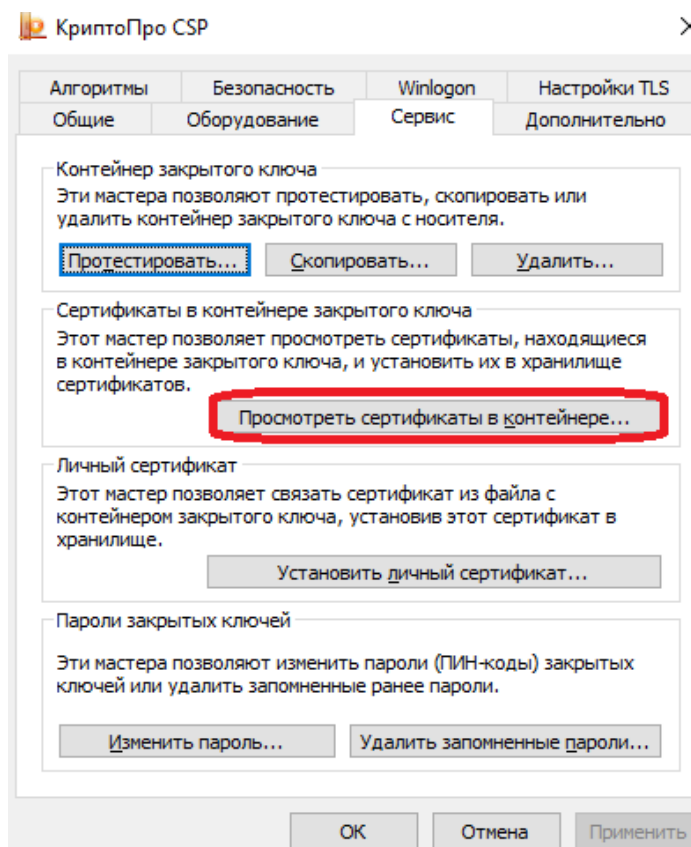
КriptoПро CSP позволяет изменять настройки криптопровайдера и работать с ключевыми носителями – просматривать и устанавливать их сертификаты, копировать ключевые контейнеры, и т.п.

В случае, если ключ сертификата пользователя ранее не был установлен в личное хранилище, то для его установки с помощью КriptoПро CSP необходимо:

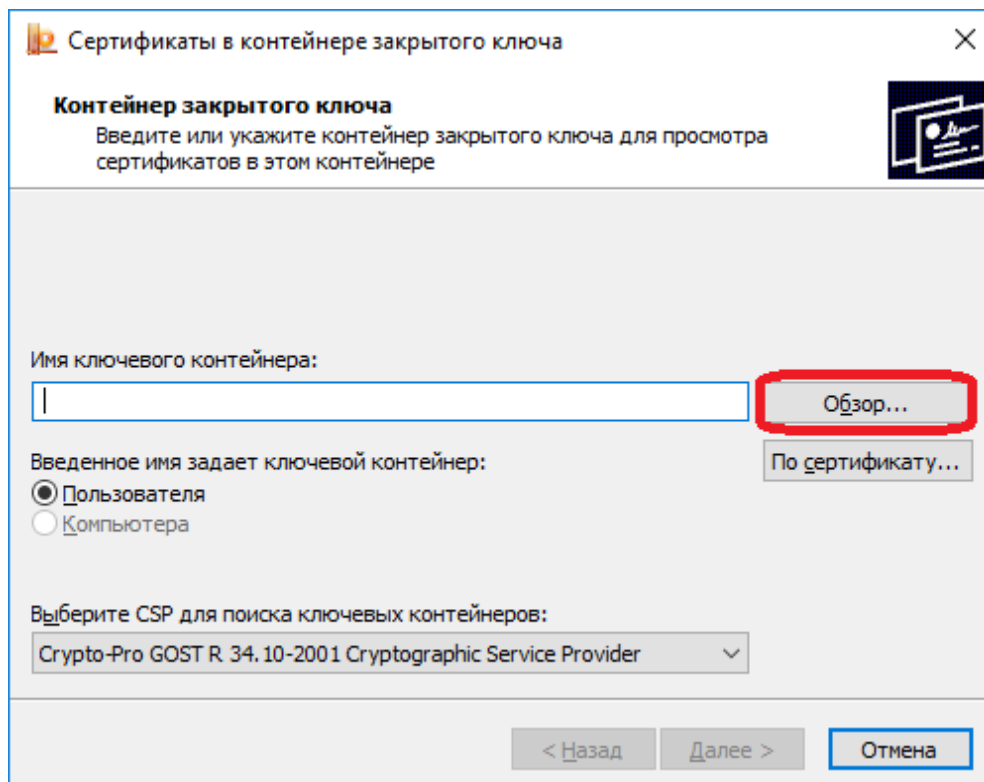
Перейти во вкладку «Сервис»:



Нажать кнопку «Просмотреть сертификаты в контейнере»:

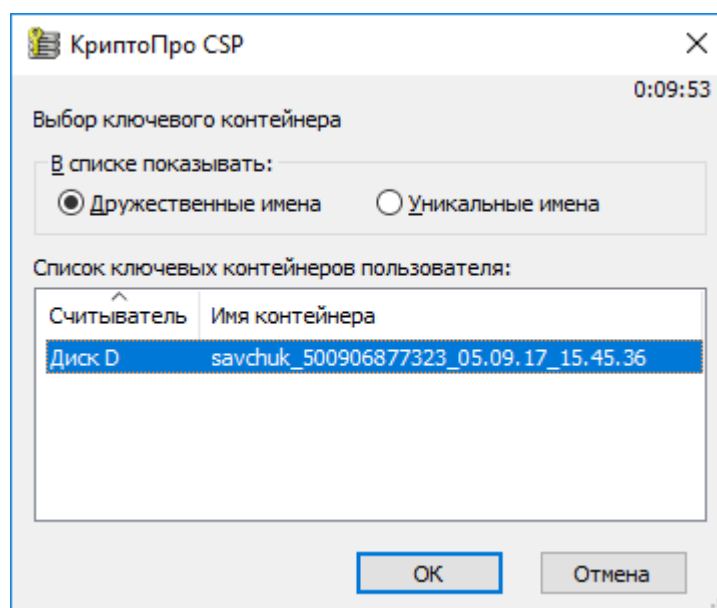


В появившемся окне через кнопку «Обзор» необходимо выбрать контейнер ключа:

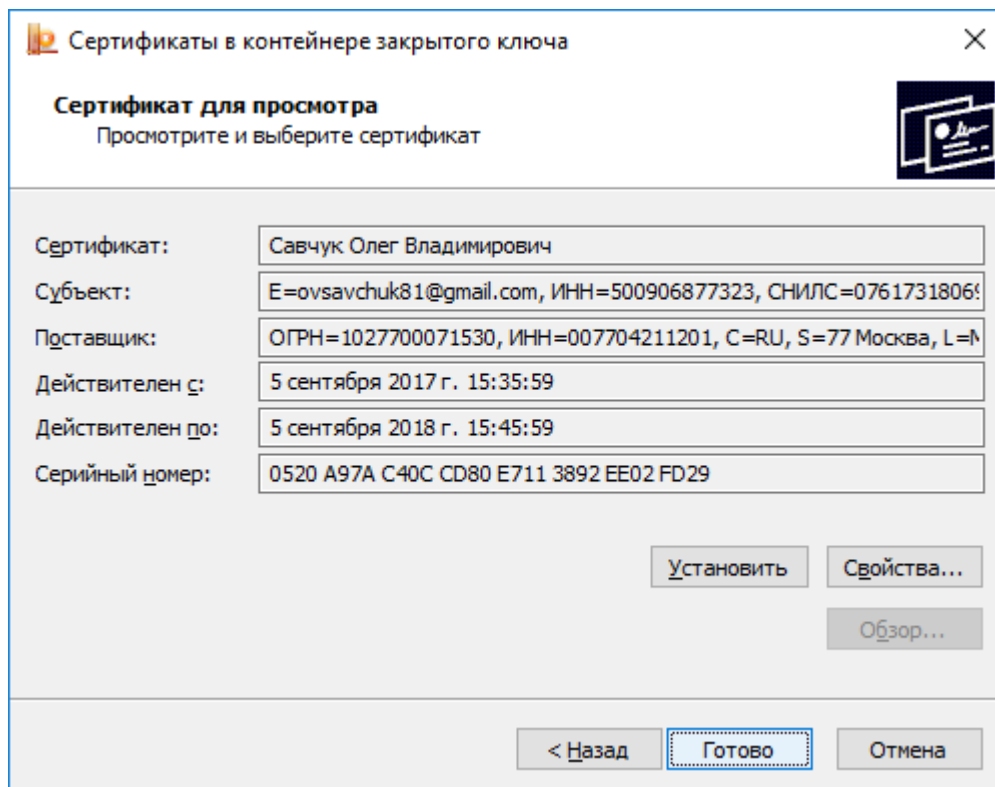


Далее выбрать ключ и нажать кнопку «ОК».

В списке ключевых контейнеров пользователя автоматически отразятся все уже установленные на компьютере сертификаты.



Отобразится информация о сертификате выбранного ключевого носителя:

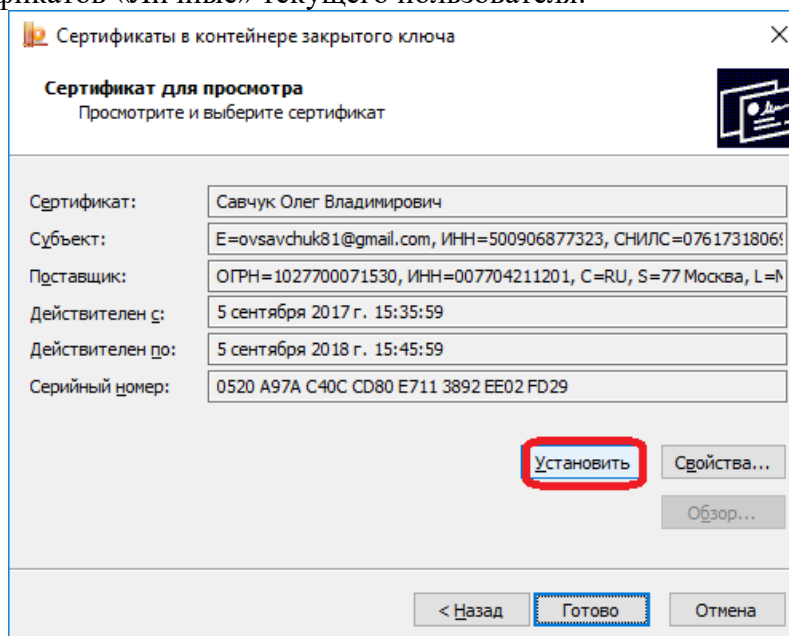


Сертификаты в контейнере закрытого ключа

Сертификат для просмотра
Просмотрите и выберите сертификат

Сертификат:	Савчук Олег Владимирович
Субъект:	E=ovsavchuk81@gmail.com, ИНН=500906877323, СНИЛС=07617318066
Поставщик:	ОГРН=1027700071530, ИНН=007704211201, C=RU, S=77 Москва, L=Moscow
Действителен с:	5 сентября 2017 г. 15:35:59
Действителен по:	5 сентября 2018 г. 15:45:59
Серийный номер:	0520 A97A C40C CD80 E711 3892 EE02 FD29

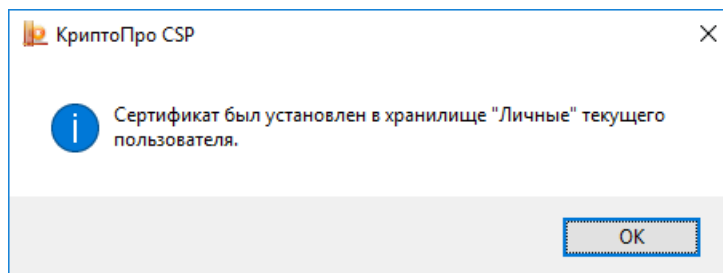
С помощью кнопки «Установить» сертификат может быть перемещён в хранилище сертификатов «Личные» текущего пользователя:



Сертификаты в контейнере закрытого ключа

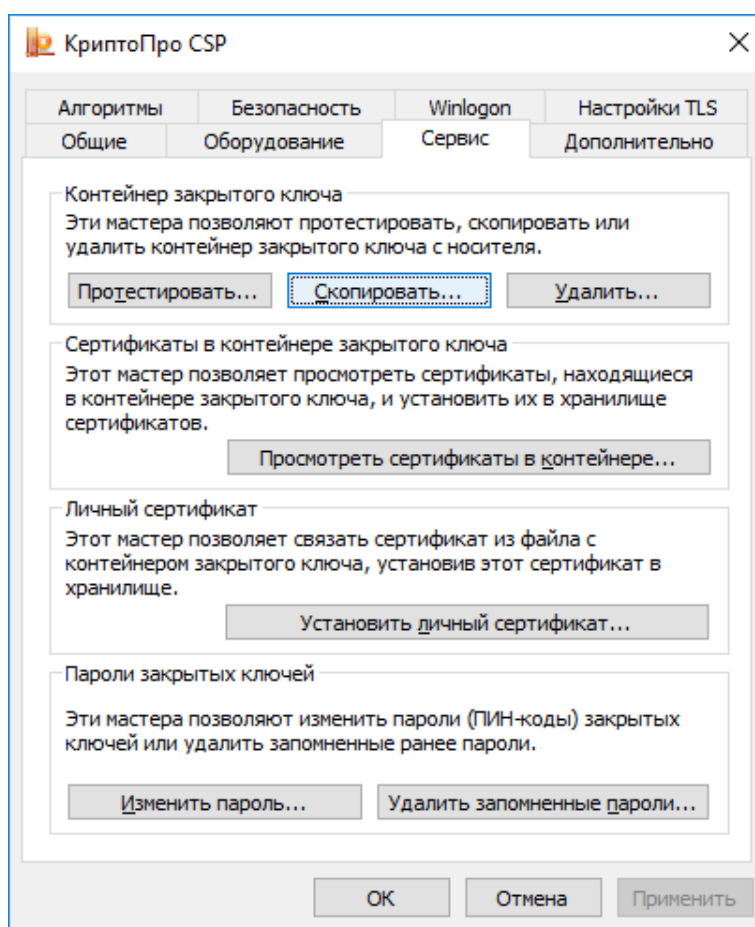
Сертификат для просмотра
Просмотрите и выберите сертификат

Сертификат:	Савчук Олег Владимирович
Субъект:	E=ovsavchuk81@gmail.com, ИНН=500906877323, СНИЛС=07617318066
Поставщик:	ОГРН=1027700071530, ИНН=007704211201, C=RU, S=77 Москва, L=Moscow
Действителен с:	5 сентября 2017 г. 15:35:59
Действителен по:	5 сентября 2018 г. 15:45:59
Серийный номер:	0520 A97A C40C CD80 E711 3892 EE02 FD29

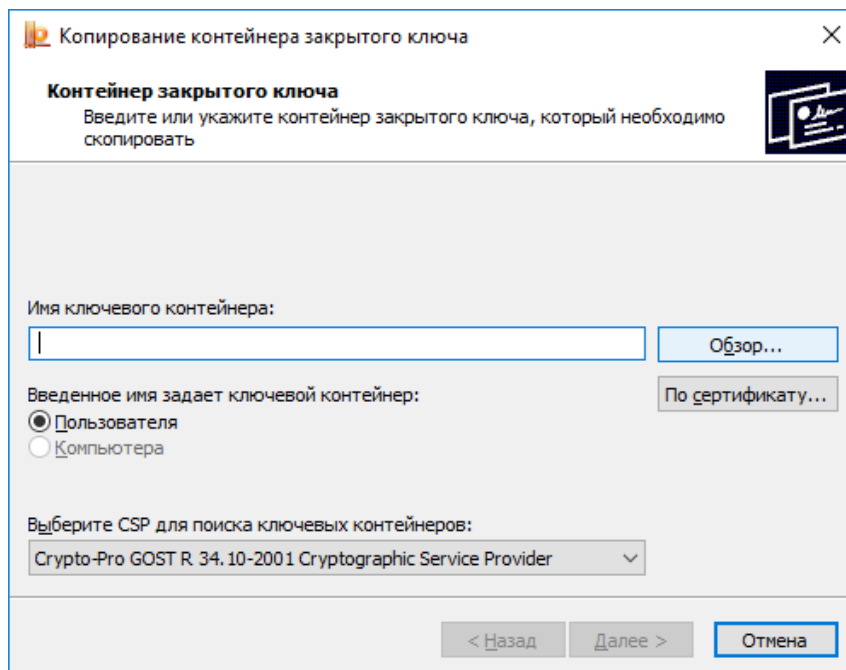


Для копирования закрытого ключа на другой носитель с помощью КриптоПро CSP необходимо:

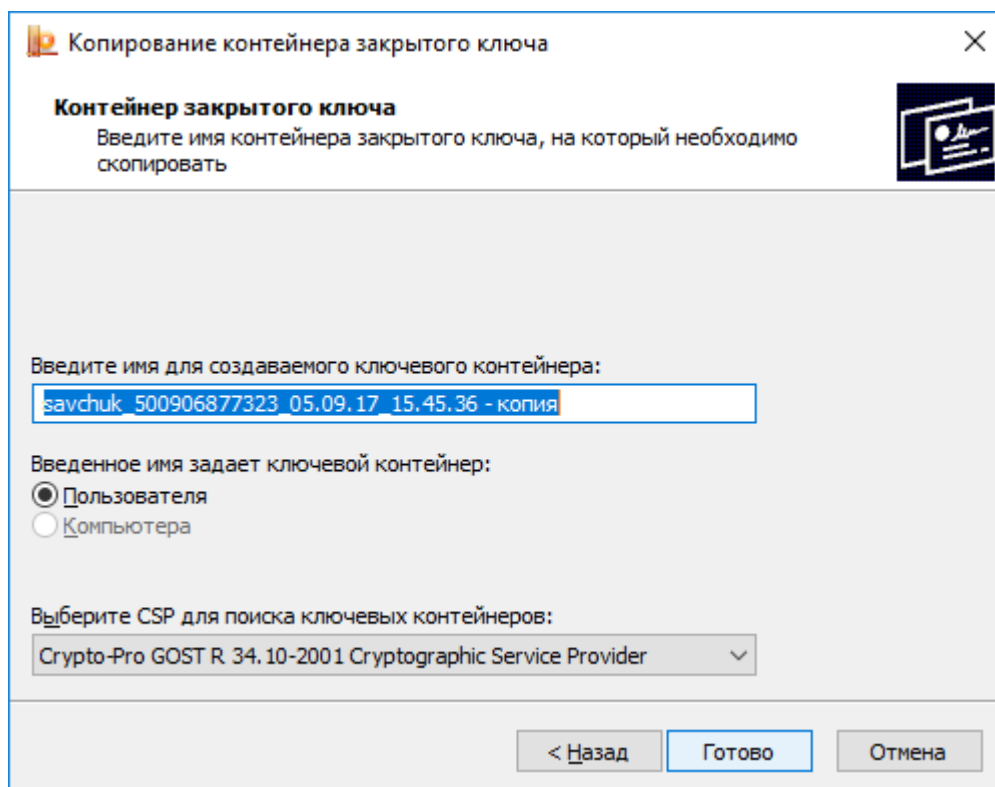
Во вкладке «Сервис» воспользоваться кнопкой «Скопировать»:



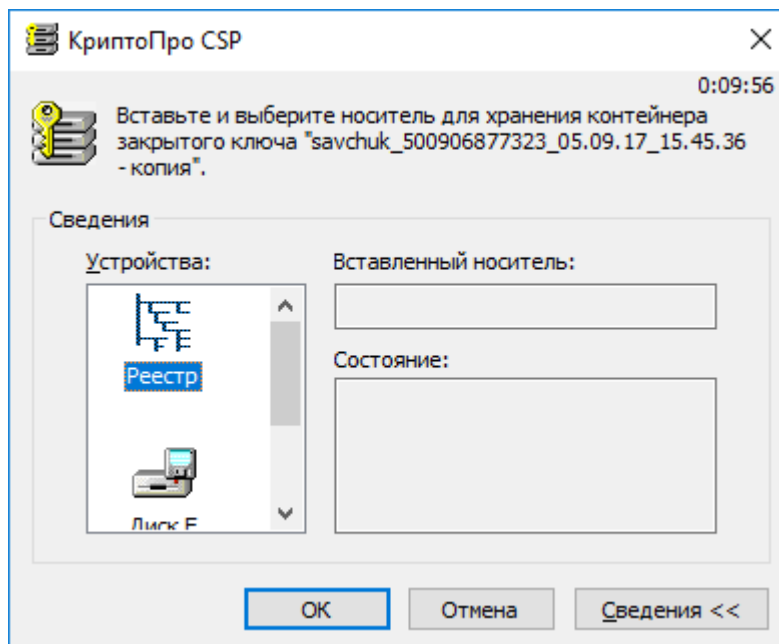
При помощи мастера выбрать ключевой контейнер, который будет скопирован:



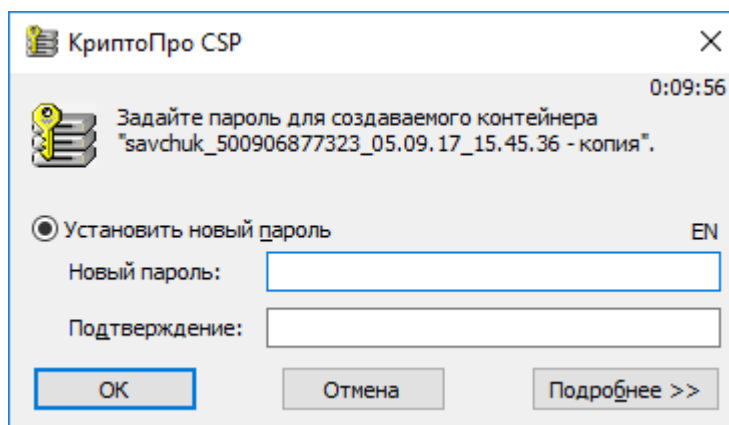
Ввести название для вновь создаваемого ключевого контейнера:



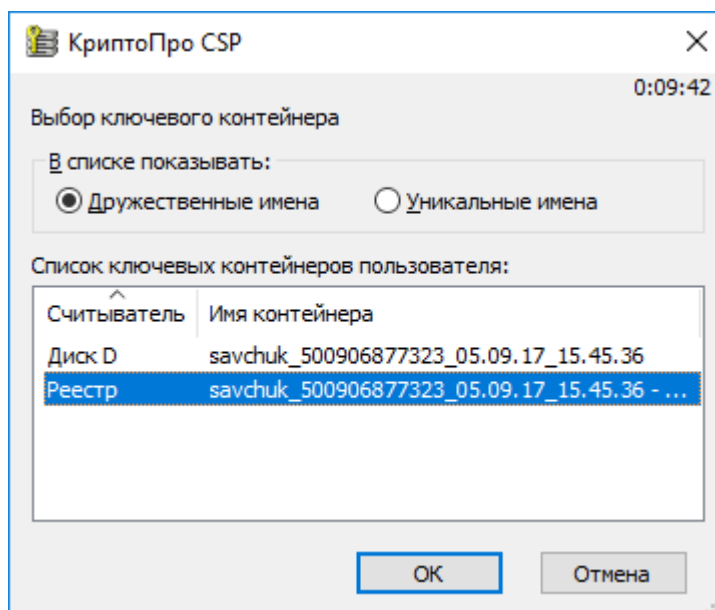
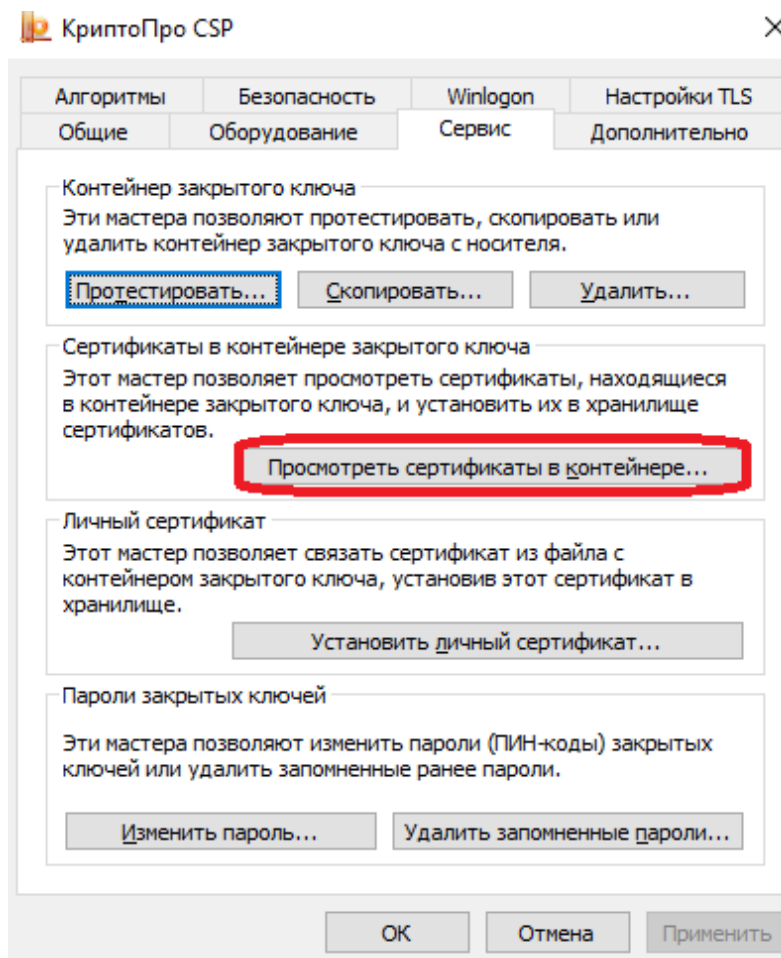
После нажатия кнопки «Готово» выбрать расположение нового ключевого контейнера. Для этого может быть выбран реестр Windows, или какие-либо внешние носители:

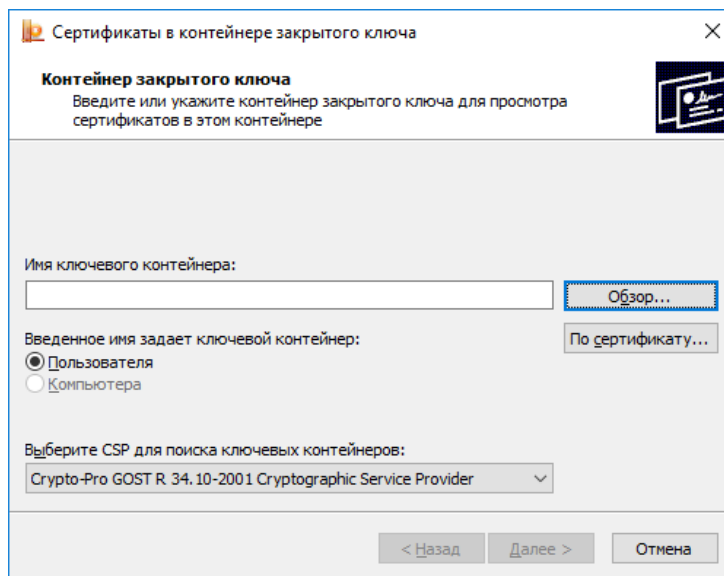


На создаваемый контейнер может быть установлен пароль. Если подпись используется в автоматическом режиме, пароль на контейнер остаётся пустым:



После копирования контейнера через просмотр сертификатов в контейнере необходимо убедиться, что в списке контейнеров ключей появился новый контейнер с ранее указанным при копировании названием:





2.5 Проверка программных средств и решение проблем

Для проверки соответствия ключа электронной подписи требованиям к УКЭП, а также корректной установки и настройки программных средств, необходимо воспользоваться сервисом онлайн-проверки ключа компании КриптоПро по ссылке:

https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_t_sample.html

Перечень основных связанных с использованием электронной подписи в браузере проблем и возможных путей их устранения приведен на странице Базы знаний КриптоПро ЭЦП Browser plug-in по ссылке:

<https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/257/12/chts-delt-esli-voznikli-problemy-s-kriptopro-ehcp-browser-plug-in-os-windows>

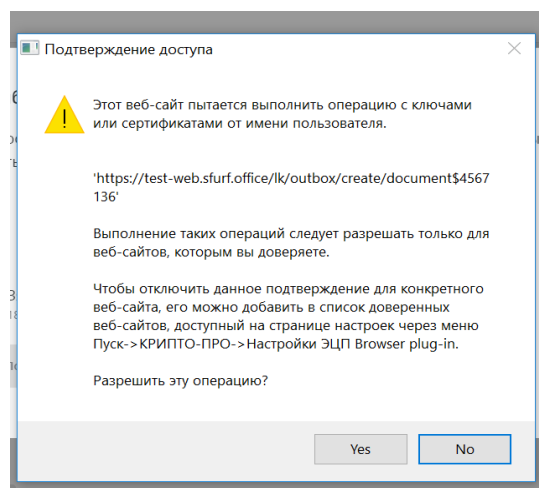
3. Создание и подписание исходящего документа в личном кабинете финансовой организации

При отправке документа в Службу финансового уполномоченного посредством Личного кабинета появляется окно:

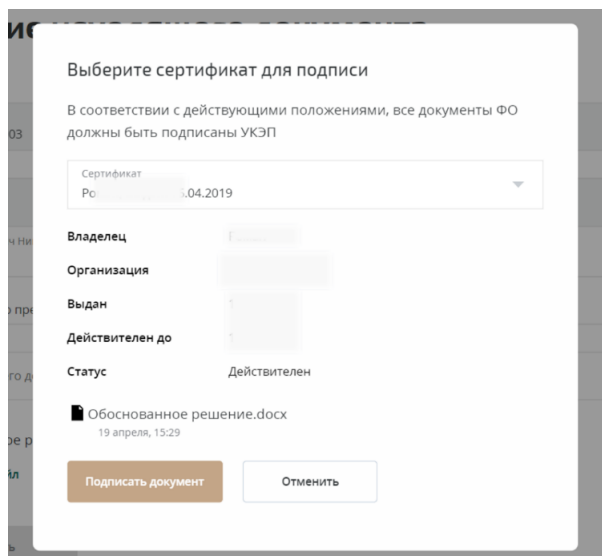
(Поля: Номер документа, Номер обращения, Тип документа, Номер исходящего документа заполняются в соответствии с ситуацией)

The screenshot shows a web form titled "Создание исходящего документа" (Creating outgoing document). At the top left is a back arrow and the text "Назад". The form contains several fields: "Номер документа" (Document number) with the value "У-19-3677/0000-003" and a green checkmark; "Номер обращения" (Request number) with the value "У-19-3677" and a green checkmark; "Заявитель: Петрова Светлана Андреевна 08.11.2018 9163510813"; a dropdown menu for "Тип документа" (Document type) with the selected value "Ответ на запрос о предоставлении обоснованного решения"; and an empty field for "Номер исходящего документа" (Outgoing document number). Below these fields is a green link "+ Добавить файл" (+ Add file) and a grey button "Отправить" (Send).

Необходимо добавить отправляемый файл, для этого следует нажать кнопку «+Добавить файл» и выбрать необходимый файл. После добавления файла в появившемся окне нажать кнопку «Да», разрешив веб-сайту обратиться к УКЭП финансовой организации.



После выбора файла и нажатия кнопки «Да» автоматически появится окно с полем «Сертификат». Кнопка «Подписать документ» будет отображаться как неактивная. В поле «Сертификат» будут представлен перечень установленных сертификатов финансовой организации, среди которых необходимо выбрать сертификат относящийся к финансовой организации, от лица которой документ направляется в Службу финансового уполномоченного.



После осуществления вышеуказанных действий кнопка «Подписать документ» станет активной. По нажатии на кнопку «Подписать документ» вновь появится окно «Создание исходящего документа» с активной кнопкой «Отправить».

Создание исходящего документа

Номер документа
У-19-3769/0000-003 ✓

Номер обращения
У-19-3769 ✓
Заявитель: Дабстепович Никита Кучерявый 11.11.1901 9128234898

Тип документа
Ответ на запрос о предоставлении обоснованного решения ▼

Номер исходящего документа

Обоснованное р... x ✓
+ Добавить файл

Отправить

Для отправки выбранного документа в Службу финансового уполномоченного необходимо нажать кнопку «Отправить».