Руководство пользователя по настройке персонального компьютера для работы с ГИИС ДМДК

09.04.2021

Для работы с ГИИС ДМДК необходимо:

1. Получить сертификат усиленной квалифицированной электронной подписи.

Сертификат ключа электронной подписи используется в ГИИС ДМДК для аутентификации пользователя, организации защищённого канала связи и подписи юридически значимых документов в системе.

2. Подготовить рабочее место, установив необходимое для работы ПО.

На рабочем месте должен быть установлен браузер с поддержкой шифрования по ГОСТ: «Спутник» (рекомендуемый вариант браузера, в дальнейшем на его базе планируется предоставление услуги расширенной технической поддержки), «Яндекс.Браузер» или «Chromium GOST». Установить можно только один браузер или все три. Инсталляционный пакет браузера «Спутник» (со встроенным СКЗИ «КриптоПро CSP») содержит в своем составе все необходимые для работы компоненты (СКЗИ КриптоПро CSP, КриптоПро ЭЦП Browser plug-in, корневые сертификаты), то есть при установке браузера «Спутник», загруженного с сайта ООО «Крипто-Про», эти компоненты будут установлены в ОС автоматически. При использовании только браузеров «Яндекс.Браузер» или «Chromium GOST» СКЗИ КриптоПро CSP, КриптоПро ЭЦП Browser plug-in необходимо загрузить и установить вручную.

3. Установить сертификаты.

1. Получение сертификата усиленной квалифицированной электронной подписи

Для работы в ГИИС ДМДК обязательно необходим сертификат ключа электронной подписи руководителя организации (персональные данные владельца сертификата должны соответствовать персональным данным руководителя организации, указанным в ЕГРЮЛ). После регистрации руководителя организации, он может назначать права себе и другим сотрудникам организации. Для того, чтобы назначить права другим сотрудникам организации, им также необходимо получить сертификат ключа электронной подписи в удостоверяющем центре и зарегистрироваться в ГИИС ДМДК, после чего руководитель организации сможет назначить сотруднику необходимые права.

В ГИИС ДМДК допускается использование только усиленной квалифицированной электронной подписи.

Для получения сертификата усиленной квалифицированной электронной подписи необходимо обратиться в удостоверяющий центр, аккредитованный Министерством цифрового развития, связи и массовых коммуникаций в соответствии с требованиями Федерального закона от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Со списком аккредитованных удостоверяющих центров можно ознакомиться по ссылке. Обращаем внимание, что некоторые удостоверяющие центры являются ведомственными и не выпускают сертификаты электронной подписи сторонним организациям.

Порядок получения сертификата электронной подписи и перечень необходимых для этого документов размещаются на сайте удостоверяющего центра.

Таким образом, необходимо выбрать из списка аккредитованных удостоверяющих центров наиболее удобный и ознакомиться с информацией, представленной на сайте выбранного удостоверяющего центра.

Лицензию на использование СКЗИ КриптоПро CSP также можно приобрести в удостоверяющем центре.

Существуют следующие варианты лицензий на использование СКЗИ КриптоПро CSP:

- лицензия на один год, записанная в сертификат ключа электронной подписи, которая может быть использована только с данным сертификатом (приобретается в удостоверяющем центре);
- лицензия на один год на использование на одном рабочем месте с любыми сертификатами (приобретается в удостоверяющем центре, в ООО «КРИПТО-ПРО» или у поставщиков программного обеспечения);
- бессрочная лицензия на использование на одном рабочем месте (приобретается в удостоверяющем центре, в ООО «КРИПТО-ПРО» или у поставщиков программного обеспечения).

Требования к сертификату ключа проверки электронной подписи для работы в ГИИС ДМДК:

1. Форма сертификатов ключей проверки электронной подписи, владельцами которых являются российские юридические лица и индивидуальные предприниматели, и используемых в ГИИС ДМДК, должна удовлетворять требованиям Приказа ФСБ РФ от 27 декабря 2011 года № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи», а также дополнительным требованиям.

Сертификат ключа проверки электронной подписи должен содержать следующие **стандартные атрибуты**:

- уникальный номер квалифицированного сертификата;
- даты начала и окончания действия квалифицированного сертификата;
- ключ проверки электронной подписи;
- наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствует ключ электронной подписи и ключ проверки электронной подписи;
- наименования средств электронной подписи и средств аккредитованного удостоверяющего центра, которые использованы для создания ключа электронной подписи, ключа проверки электронной подписи, квалифицированного сертификата, а также реквизиты документа, подтверждающего соответствие указанных средств требованиям, установленным в соответствии с Федеральным законом;
- наименование и место нахождения аккредитованного удостоверяющего центра, который выдал квалифицированный сертификат;
- номер квалифицированного сертификата аккредитованного удостоверяющего центра;
- ограничения использования квалифицированного сертификата (если такие ограничения установлены).

Сертификат ключа проверки электронной подписи должен содержать следующие **дополнительные атрибуты**:

- «Улучшенный ключ» (OID 2.5.29.37) – в данном дополнении должны быть указаны OID 1.3.6.1.5.5.7.3.2 («Проверка подлинности клиента») и OID 1.3.6.1.5.5.7.3.4 («Защищенная электронная почта»);
- «Точка распространения списка отозванных сертификатов» (OID 2.5.29.31) – данное дополнение должно содержать протоколы доступа и адреса публикации списка отозванных сертификатов, на основании которого может быть установлен статус сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи должен содержать следующие **атрибуты имени**:

Атрибут	**Значение для юридического лица**	**Значение для индивидуального предпринимателя**
Стандартные атрибуты имени		
Общее имя (CN, OID 2.5.4.3)	Наименование юридического лица	Фамилия, имя, отчество (если имеется) индивидуального предпринимателя
Организация (O, OID.2.5.4.10)	Наименование юридического лица	*Не применимо*
Подразделение юридического лица (OU, OID 2.5.4.11)	Наименование подразделения юридического лица (необязательный атрибут)	*Не применимо*
Страна (C, OID 2.5.4.6)	Код страны в соответствии с ISO 3166 = «RU»	
Субъект РФ (S, OID 2.5.4.8)	Наименование субъекта РФ, где зарегистрирована организация или индивидуальный предприниматель	
Населённый пункт (L, OID 2.5.4.7)	Наименование населённого пункта, где зарегистрирована организация или индивидуальный предприниматель	
Адрес (STREET, OID 2.5.4.9)	Часть адреса места нахождения организации или индивидуального предпринимателя, включающая наименование улицы, номер дома, а также корпуса, строения, квартиры, помещения (если имеется)	
Фамилия (SN, OID 2.5.4.4)	Фамилия владельца сертификата ключа проверки электронной подписи	
Приобретённое имя (G, OID 2.5.4.42)	Имя и отчество (если имеется) владельца сертификата ключа проверки электронной подписи	
Должность (T, OID 2.5.4.12)	Должность владельца сертификата ключа проверки электронной подписи	Текстовое значение «Индивидуальный предприниматель»
Дополнительные атрибуты имени		
ИНН (OID 1.2.643.3.131.1.1)	ИНН юридического лица (12 цифр = «00» + ИНН)	ИНН индивидуального предпринимателя (12 цифр)
ОГРН (OID 1.2.643.100.1)	ОГРН организации (13 цифр)	*Не применимо*
ОГРНИП (OID 1.2.643.100.5)	*Не применимо*	ОГРН индивидуального предпринимателя (15 цифр)

Атрибут	Значение для юридического лица	Значение для индивидуального предпринимателя
СНИЛС (OID 1.2.643.100.3)	СНИЛС владельца сертификата ключа проверки электронной подписи (11 цифр)	
Электронная почта (E, OID 1.2.840.113549.1.9.1)	Адрес электронной почты владельца сертификата ключа проверки электронной подписи	

Стандартные и дополнительные атрибуты имени сертификата ключа проверки электронной подписи должны заполняться на русском языке с использованием символов кириллического алфавита, кроме адреса электронной почты.

2. Сертификаты ключей проверки электронной подписи и ключи электронной подписи должны использоваться совместно со средством электронной подписи КриптоПро CSP (версии 4.x или 5.x), сертифицированным ФСБ России.

3. Ключи электронной подписи должны создаваться на ключевых носителях, предназначенных для хранения ключевой информации (смарт-карты, USB-«токены»). Данные ключевые носители должны поддерживаться применяемым средством электронной подписи КриптоПро CSP.

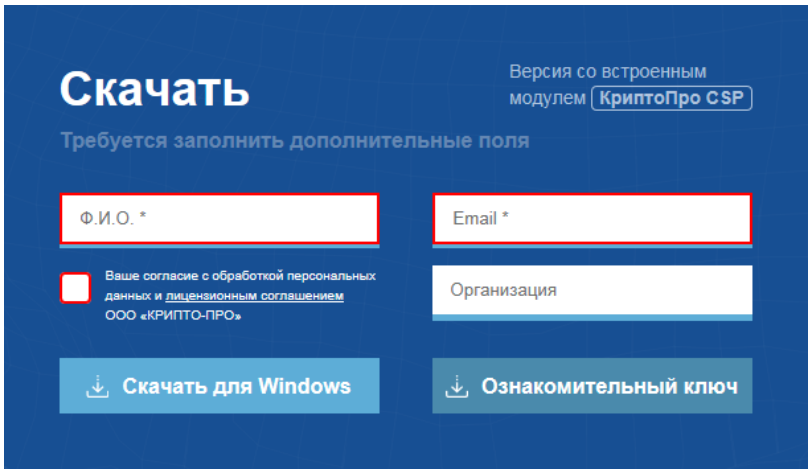
4. Срок действия сертификата ключа проверки электронной подписи **должен быть не менее 10 лет** после окончания срока действия закрытого ключа электронной подписи. Данное требование связано с необходимостью обеспечения возможности проверки цепочки сертификатов в течение срока хранения электронных документов, составляющего 10 лет.

2. Подготовка рабочего места

В качестве рабочего места используется персональный компьютер с операционной системой Microsoft Windows 7/8/10 или Astra Linux CE/SE. Далее описывается подготовка рабочего места на ПК с ОС Windows, для ПК с ОС Astra Linux см. инструкцию «ГИИС ДМДК Настройка окружения в ОС Astra Linux».

2.1. Установка браузера «Спутник» со встроенным СКЗИ «КриптоПро CSP»

Загрузите установочный файл браузера «Спутник» с сайта ООО «Крипто-Про» по ссылке. При загрузке требуется указать ФИО, адрес электронной почты и дать согласие на обработку персональных данных:



Запустите установочный файл браузера «Спутник» и подтвердите установку, отвечая «Да» на запросы программы установки. Установка всех компонентов будет выполнена в тихом режиме и завершится появлением ярлыка браузера на рабочем столе:

Для активации лицензии браузера «Спутник» запустите браузер, найдите в настройках раздел «О Спутнике». На странице «О Спутнике» нажмите «Загрузить ключ лицензии из файла», в открывшемся окне выберите файл ключа лицензии license.lic и перезапустите браузер.

2.2. Установка браузеров «Яндекс.Браузер» и «Chromium GOST»

Если вы уже установили браузер «Спутник», то следующие 2 пункта (установка СКЗИ КриптоПро CSP и установка КриптоПро ЭЦП Browser plug-in) пропустите.

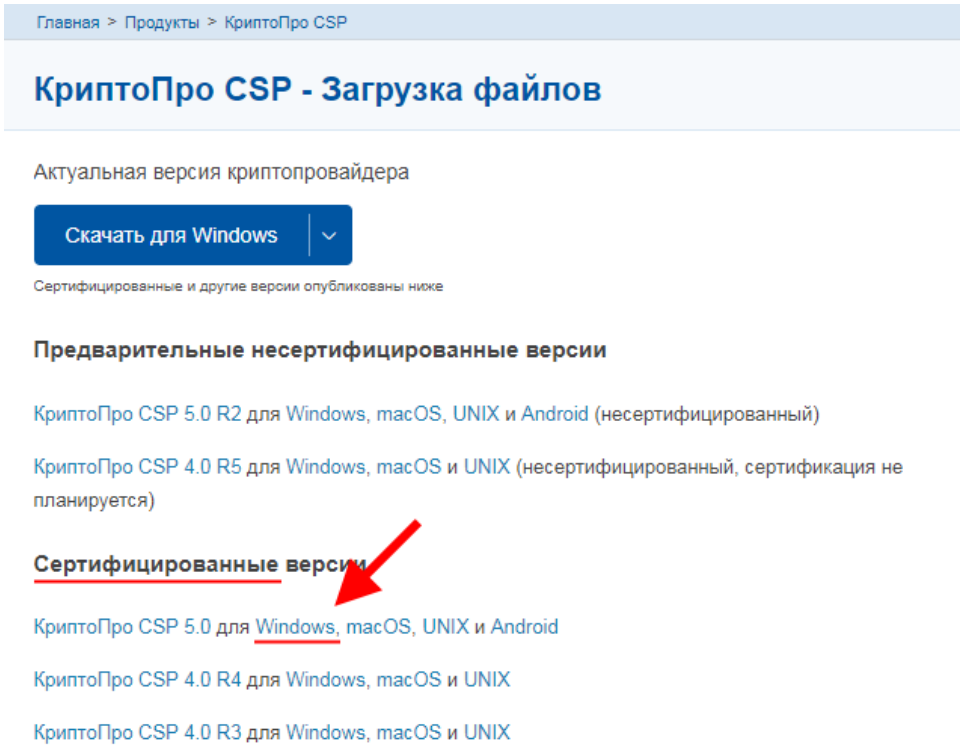
Установка СКЗИ КриптоПро CSP

Для получения дистрибутива СКЗИ КриптоПро CSP необходимо зарегистрироваться на сайте КриптоПро по ссылке.

После регистрация становится доступным раздел «КриптоПро CSP - Загрузка файлов» по ссылке. В данном разделе необходимо скачать подходящую версию КриптоПро CSP.

Если уже имеется действующая лицензия на СКЗИ КриптоПро, то скачайте последнюю сертифицированную версию, соответствующую имеющейся лицензии.

Если лицензия отсутствует, то рекомендуется скачать последнюю сертифицированную версию СКЗИ КриптоПро CSP 5.0:



Выполните установку СКЗИ КритоПро CSP, следуя инструкциям установщика. Какие-либо специальные настройки при установке не требуются. После установки СКЗИ КриптоПро CSP необходимо перезагрузить компьютер.

Если лицензия отсутствует, то СКЗИ КриптоПро CSP будет автоматически активировано временной лицензией сроком на 3 месяца, в течение этого времени необходимо приобрести лицензию.

Установка КриптоПро ЭЦП Browser plug-in

Дистрибутив **КриптоПро ЭЦП Browser plug-in** необходимо загрузить с сайта КриптоПро по ссылке.

На той же странице размещена ссылка на инструкцию по установке плагина и ссылка на сервис проверки работы плагина (проверка работы плагина выполняется после установки интернет-браузера с поддержкой шифрования по ГОСТ).

Установка Яндекс.Браузер

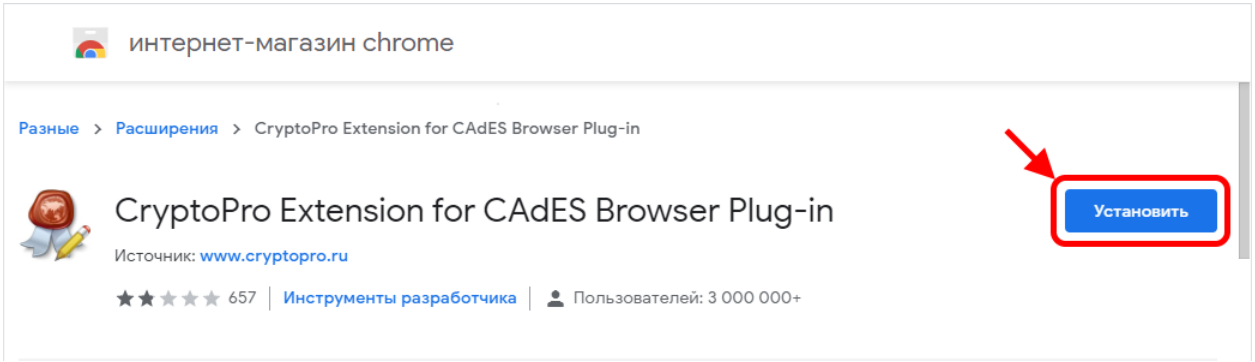
Интернет-браузер «Яндекс.Браузер» можно загрузить по ссылке.

После установки интернет-браузера «Яндекс.Браузер» необходимо установить и включить дополнение «КриптоПро ЭЦП»:

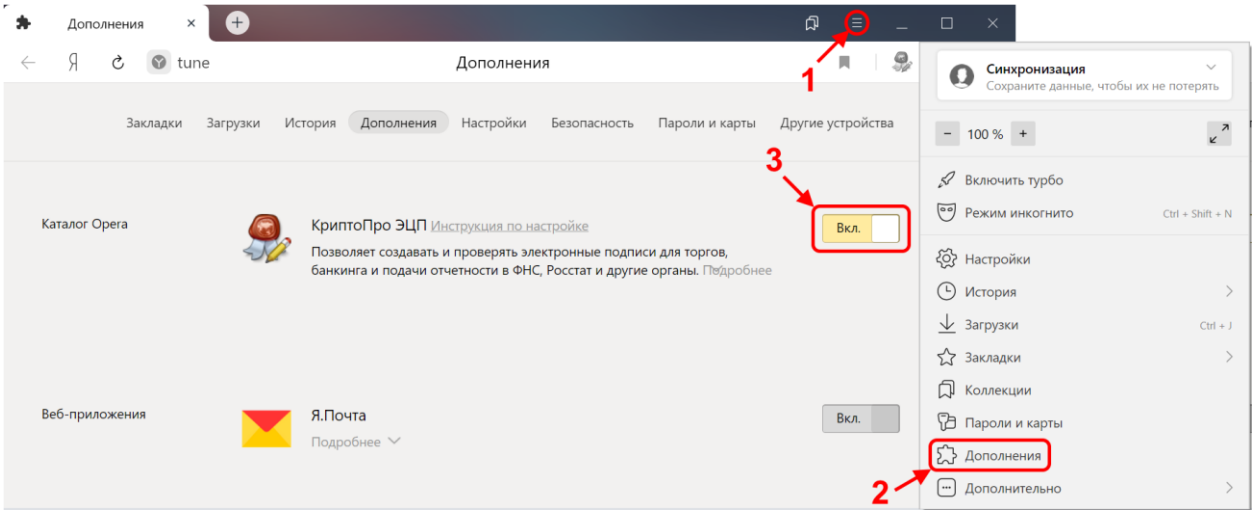
1. Открыть в интернет-браузере «Яндекс.Браузер» ссылку (скопировать и вставить):

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

2. Нажать кнопку «Установить». Если на месте кнопки «Установить» располагается кнопка «Удалить из Chrome», то это значит, что дополнение было установлено ранее и установка не требуется, перейдите к шагу 3.



3. Включите дополнение.



4. В Яндекс.Браузер также необходимо включить опцию «Подключаться к сайтам, использующим шифрование по ГОСТ. Требуется Крипто.Про CSP.». Без включения этой опции при попытке входа в ГИИС ДМДК будет выдаваться ошибка «ERR_SSL_VERSION_OR_CIPHER_MISMATCH», так как по умолчанию браузер не работает с сертификатами, использующими шифрование по ГОСТ.

Установка Chromium GOST

Интернет-браузер «Chromium GOST» можно загрузить по ссылке. Если не знаете, какую версию выбрать, то выбирайте «chromium-gost-***-windows-386-installer.exe».

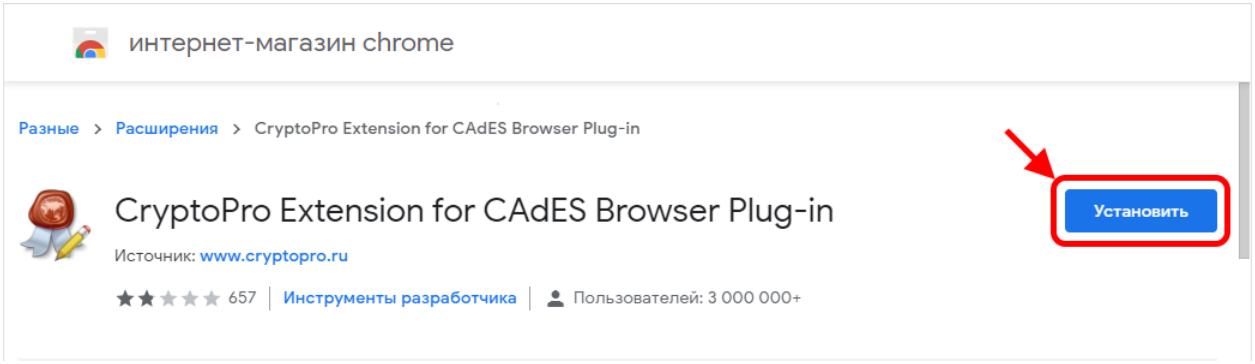
С дополнительной информацией по установке, настройке и работе с интернет-браузером «Chromium GOST» можно ознакомиться на сайте КриптоПро по ссылке.

После установки интернет-браузера «Chromium GOST» необходимо установить и включить дополнение «КриптоПро ЭЦП»:

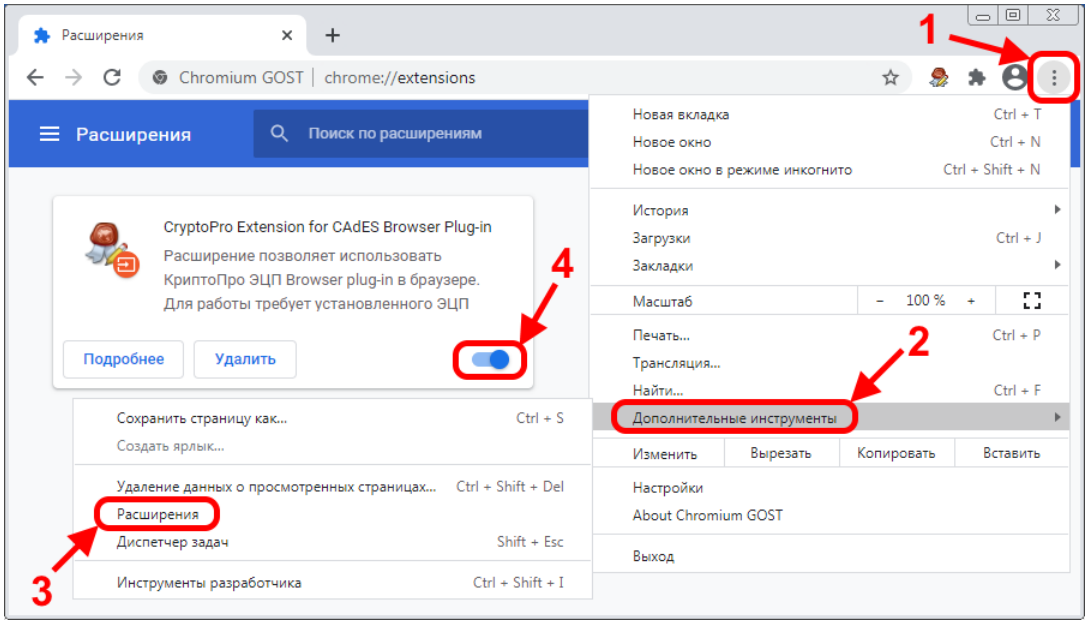
1. Открыть в интернет-браузере «Chromium GOST» ссылку (скопировать и вставить):

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

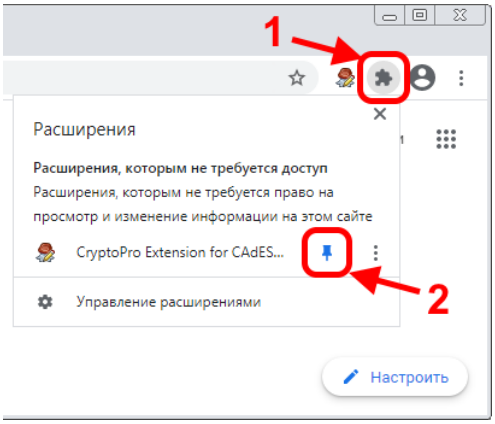
2. Нажать кнопку «Установить». Если на месте кнопки «Установить» располагается кнопка «Удалить из Chrome», то это значит, что дополнение было установлено ранее и его установка не требуется, перейдите к шагу 3.



3. Включите дополнение.



4. Закрепите значок дополнения.



В случае, если защищённое соединение с порталом ГИИС ДМДК не устанавливается, необходимо включить протоколы TLS 1.1 и TLS 1.2 в Windows. Статья о включении указанных протоколов размещена на сайте Microsoft по ссылке (перевод на русский язык).

Также для включения протоколов TLS 1.1 и TLS 1.2 в Windows можно воспользоваться файлом реестра (.reg) следующего содержания:

```
Windows Registry Editor Version 5.00


[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000
```

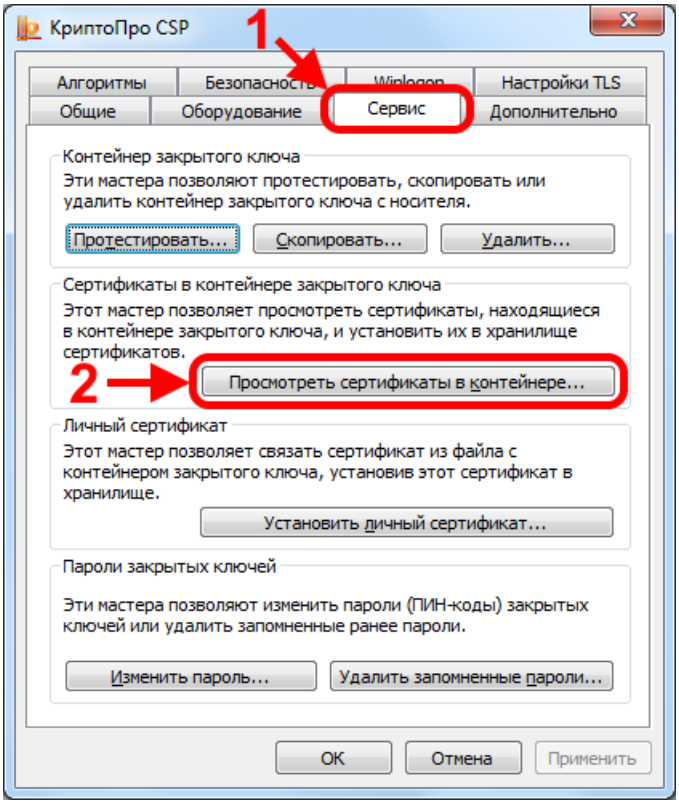
3. Установка сертификатов

Скачайте корневой сертификат Минкомсвязи России по ссылке и установите в хранилище «Доверенные корневые центры сертификации».

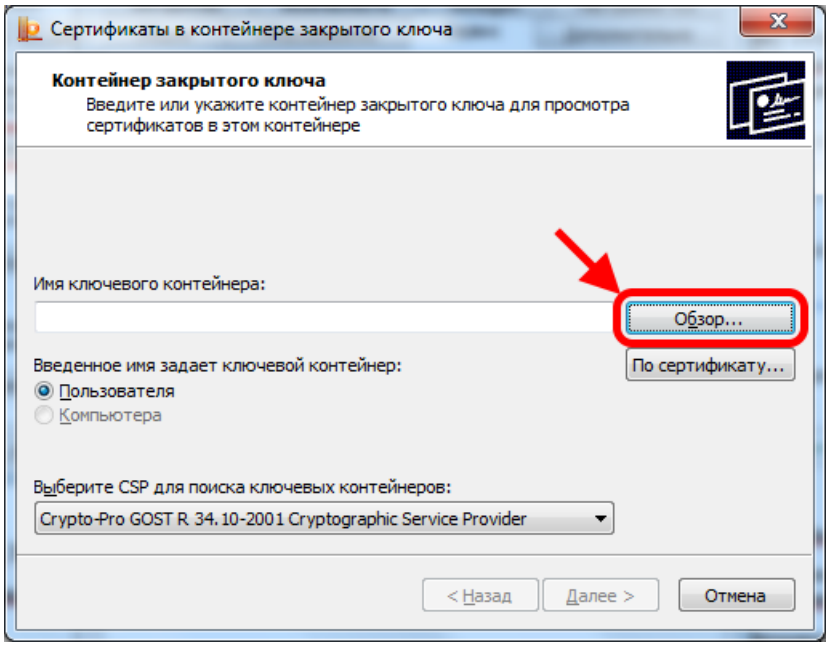
Скачайте промежуточный сертификат ЗАО «Национальный удостоверяющий центр» по ссылке и установите в хранилище «Промежуточные центры сертификации».

Для установки сертификата пользователя подключите к компьютеру «токен», который был получен в удостоверяющем центре, найдите в меню «Пуск» каталог «КРИПТО-ПРО» и запустите «КриптоПро CSP».

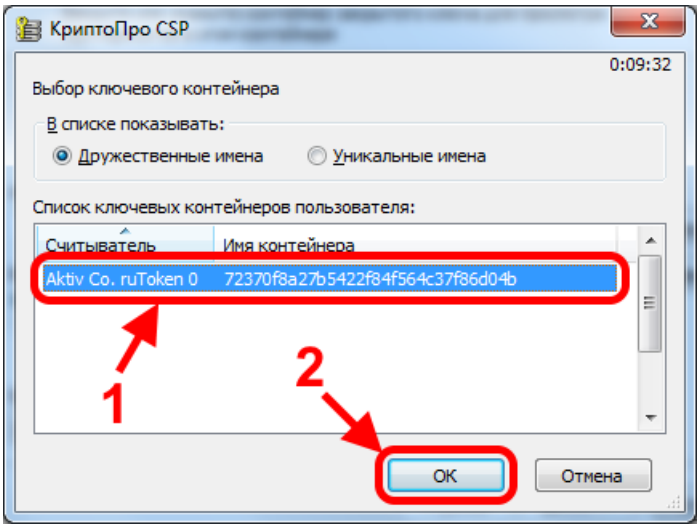
В открывшемся окне перейдите на вкладку «Сервис» и нажмите кнопку «Просмотреть сертификаты в контейнере…».



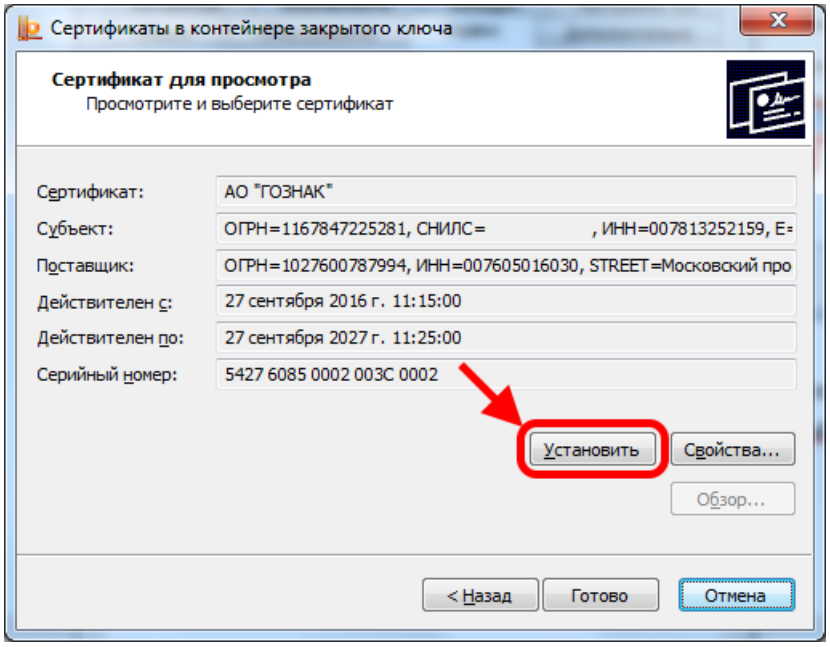
В открывшемся окне нажать кнопку «Обзор».



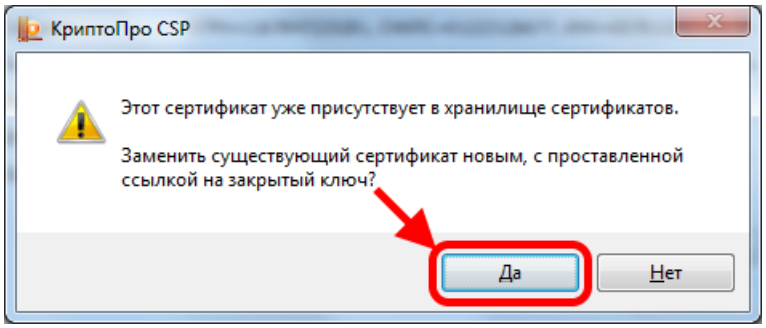
В открывшемся окне выбрать контейнер закрытого ключа (в примере – «Activ Co. ruToken») и нажать кнопку «OK».



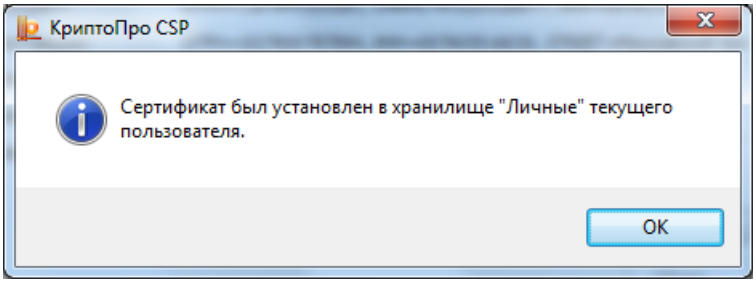
В открывшемся окне нажмите кнопку «Установить».



Если появится вопрос о замене существующего сертификата новым, нажмите «Да».

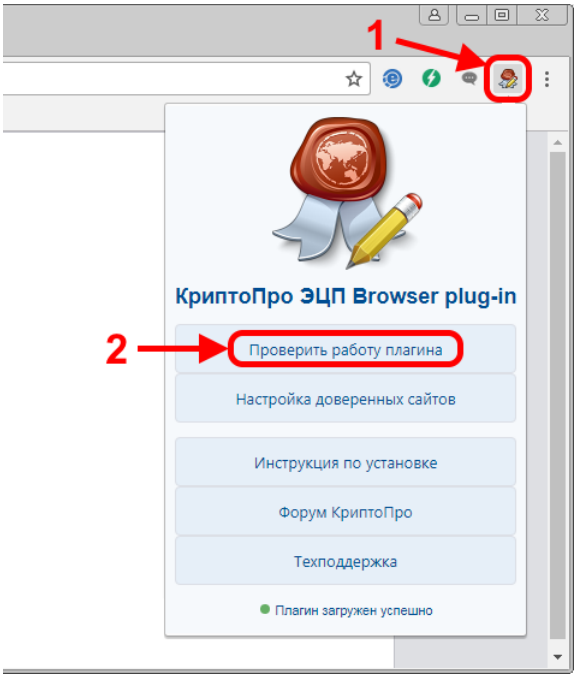


В результате должно появиться сообщение об успешной установке сертификата.



Проверка работы плагина «КриптоПро ЭЦП Browser plug-in»

После установки и настройки интернет-браузеров проверьте работу плагина «КриптоПро ЭЦП Browser plug-in» по ссылке или нажав на значок плагина, расположенный справа от адресной строки, и выбрав пункт «Проверить работу плагина».



В результате должна открыться страница, на которой будет указан результат загрузки плагина, а также будут отображены версия плагина и версия криптопровайдера.