

# Инструкция по работе с плагином CryptoPro и УКЭП

Содержание:

1. [Установка ПО для работы с УКЭП](#)
2. [Установка программы КриптоПро](#)
3. [Загрузка и установка КриптоПро ЭЦП Browser plug-in:](#)
4. [Активация использования «КриптоПро ЭЦП Browser plug-in»](#)
5. [Проверка работы плагина «КриптоПро ЭЦП Browser plug-in»](#)
6. [Добавление корневых сертификатов в список доверенных](#)
7. [Требования к составу и содержанию обязательных параметров сертификата УКЭП](#)
8. [Часто задаваемые вопросы](#)

## 1. Установка ПО для работы с УКЭП

Для работы с УКЭП необходимо загрузить и установить **драйвер Рутокен**, для этого:

- 1.1. Необходимо перейти по прямой [ссылке](https://www.rutoken.ru/) или перейти в раздел «[Центр загрузки](#)» сайта Рутокен (<https://www.rutoken.ru/> – Поддержка – Центр загрузки) (Рис.1.1)

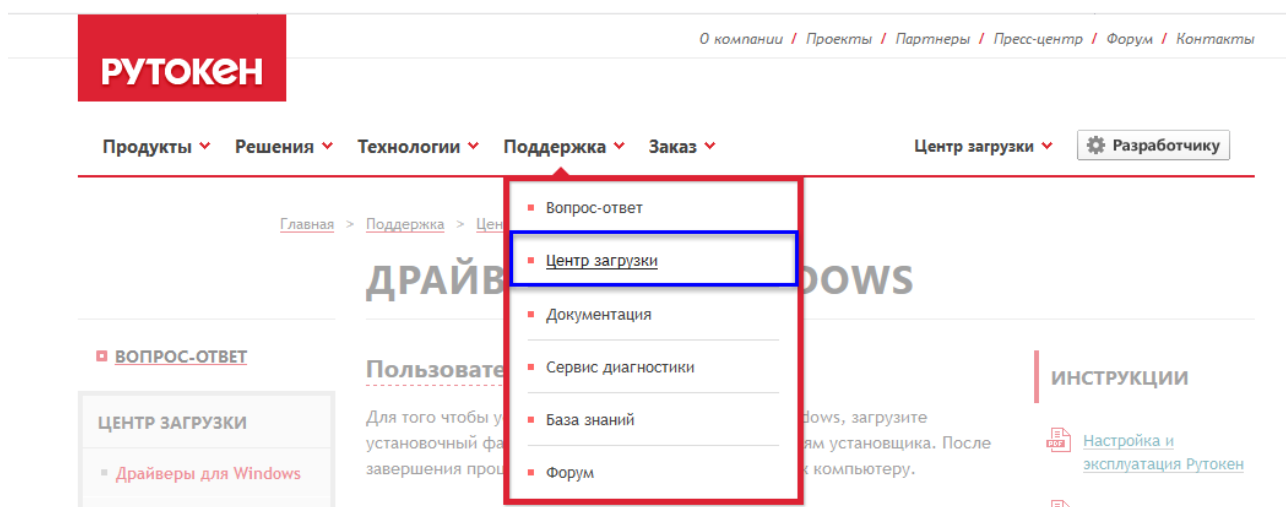


Рис. 1.1 — Рутокен – Поддержка – Центр загрузки

- 1.2. Выбрать версию драйвера Рутокен, соответствующую установленной ОС. Ниже в примере рассмотрим загрузку драйвера для ОС Windows:

- 1.2.1 Для загрузки Драйвера Рутокен для Windows необходимо кликнуть по ссылке «Драйверы Рутокен для Windows, EXE» (Рис. 1.2):

## ДРАЙВЕРЫ ДЛЯ WINDOWS

■ ВОПРОС-ОТВЕТ

ЦЕНТР ЗАГРУЗКИ

- Драйверы для Windows
- Драйверы для macOS
- Рутокен для КриптоПро

### Пользователям Рутокен ^

Для того чтобы установить драйверы Рутокен для Windows, загрузите установочный файл, запустите его и следуйте указаниям установщика. После завершения процесса установки подключите Рутокен к компьютеру.

↓ Драйверы Рутокен для Windows, EXE

Рис. 1.2 — Загрузка драйвера Рутокен для ОС Windows

1.3. Откроется новая страница «Лицензионное соглашение» (Рис.1.3):

## ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

Перед использованием программных продуктов и/или онлайн-сервисов Рутокен (Rutoken), ознакомьтесь с условиями Лицензионного соглашения. Любое использование программных продуктов и/или онлайн-сервисов Рутокен (Rutoken) означает полное и безоговорочное принятие его условий.

[Загрузить Лицензионное соглашение в виде отдельного PDF-документа](#)

Утверждено  
Приказом генерального директора  
ЗАО «Актив-софт»  
№ 01-ЛС от 31.08.2012 г.

**Лицензионное соглашение  
на использование программных продуктов  
и/или онлайн-сервисов Рутокен (Rutoken)**  
Редакция №1 от 31.08.2012 г.

Настоящий документ представляет собой предложение Закрытого акционерного общества «Актив-софт» (далее – «Правообладатель») заключить соглашение на изложенных ниже условиях.

Условия Лицензионного соглашения прочитаны и приняты в полном объеме.

УСЛОВИЯ ПРИНЯТЫ

Рис. 1.3 — Страница «Лицензионное соглашение»

1.3.1 Необходимо принять условия Лицензионного соглашения (поставить галку и кликнуть по кнопке «условия приняты») (Рис. 1.4):

**Лицензионное соглашение  
на использование программных продуктов  
и/или онлайн-сервисов Рутокен (Rutoken)**  
Редакция №1 от 31.08.2012 г.

Настоящий документ представляет собой предложение Закрытого акционерного общества «Актив-софт» (далее – «Правообладатель») заключить соглашение на изложенных ниже условиях.

Условия Лицензионного соглашения прочитаны и приняты в полном объеме.

**УСЛОВИЯ ПРИНЯТЫ**

Рис. 1.4 — Согласие с условиями Лицензионного соглашения

1.4. Перейти к загрузке драйвера Рутокен (Рис. 1.5):

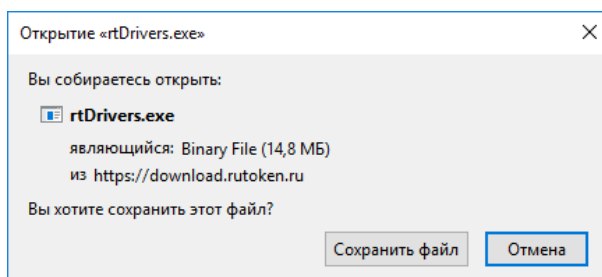


Рис. 1.5 — Перейти в загрузки и сохранить установочный файл драйвера Рутокен

1.4.1 Открыть сохраненный файл и установить драйвер Рутокен, выполнив загруженный установщик (Рис. 1.6).

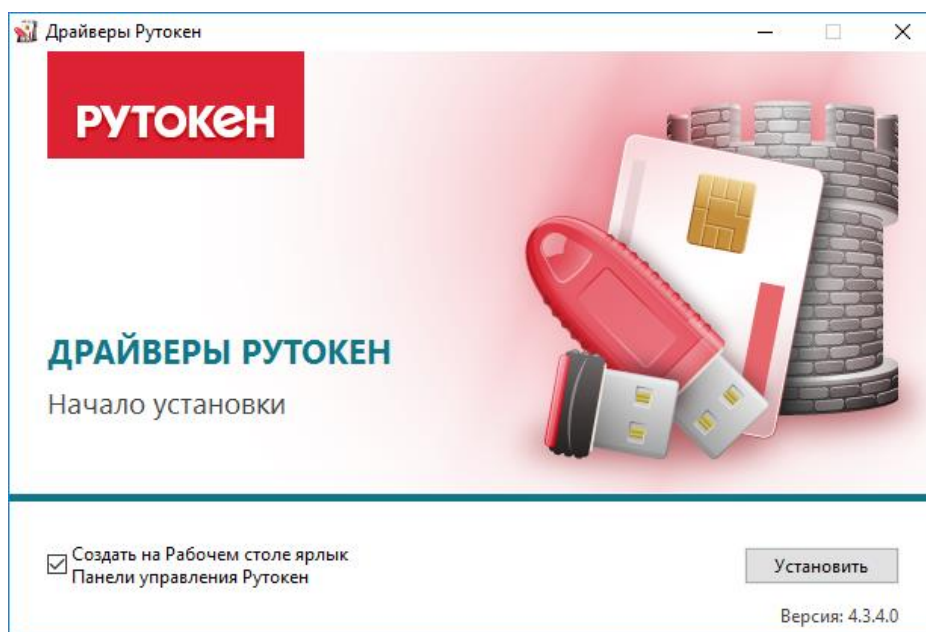


Рис. 1.6 — Установить Драйвер Рутокен

1.4.2 Дождаться завершения установки и «закрыть» (Рис.1.7)

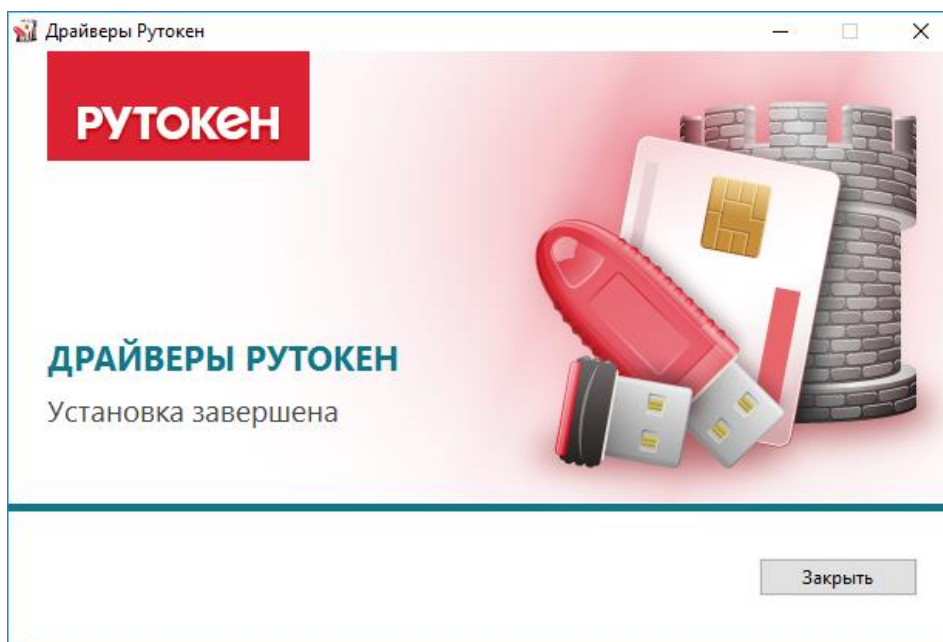


Рис. 1.7 — Драйвер Рутокен установлен

## 2. Установка программы КристоПро

Для установки программы [КристоПро](#) необходимо:

### 2.1 [Зарегистрироваться на сайте CryptoPro](#):

#### 2.1.1 Открыть форму регистрации, заполнив обязательные поля (Рис. 2.1)

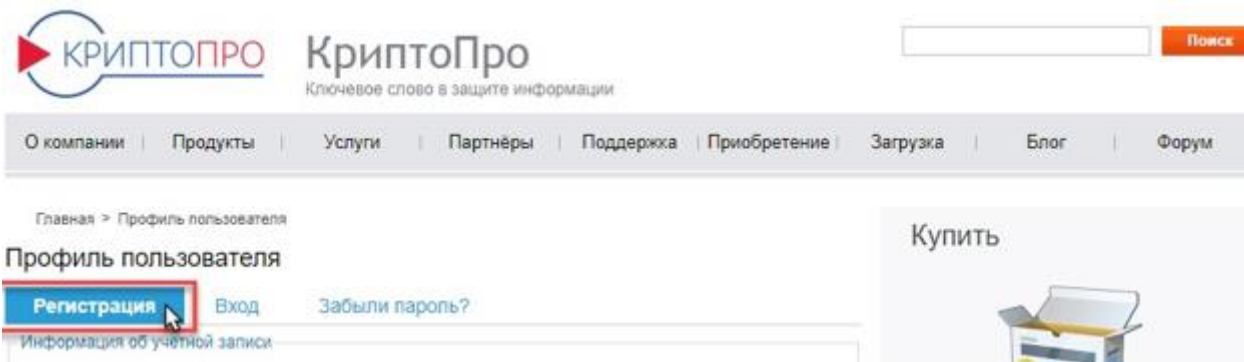


Рис. 2.1 — Открытие формы регистрации на сайте [CryptoPro](#)

#### 2.1.2 После заполнения формы регистрации принять «Согласие на обработку персональных данных», ввести проверочный код из предложенной картинке, нажать кнопку «Регистрация» (Рис. 2.2)

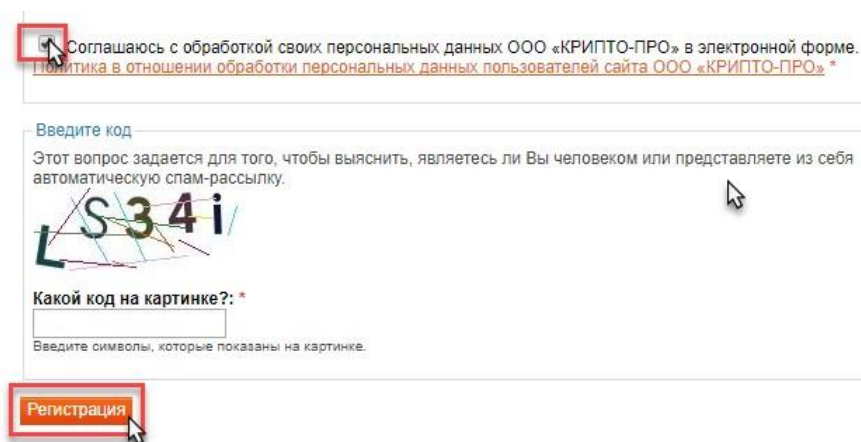


Рис. 2.2 — Подтверждение регистрации на сайте [CryptoPro](#)

### 2.2 Перейти в раздел «Центр загрузки» сайта [КристоПро](#) (Загрузка – КристоПро CSP) или по [ссылке](#) (Рис. 2.3):

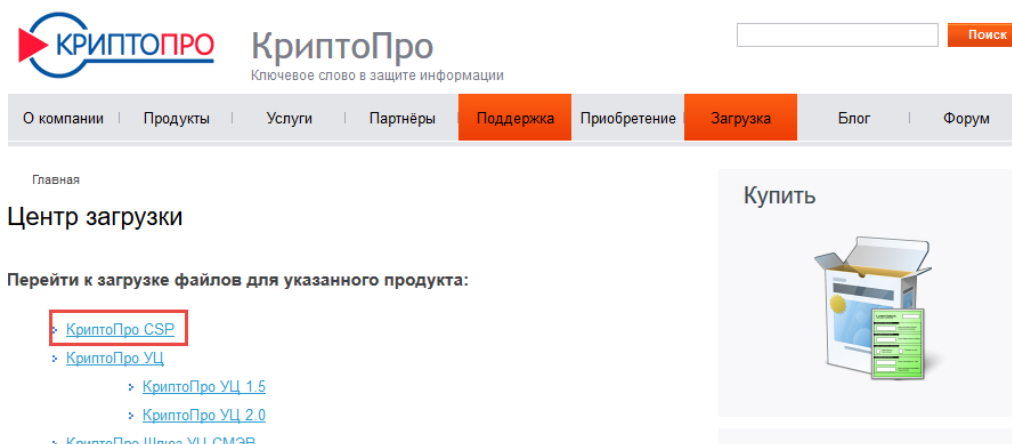


Рис. 2.3 — Раздел «Центр загрузки» сайта КристоПро

## 2.3 Принять условия Лицензионного соглашения и перейти к загрузке (Рис. 2.4):

Использование программного обеспечения регламентируется приведенным ниже Лицензионным соглашением с ООО "КРИПТО-ПРО":

ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

1. Исключительные права на программу для ЭВМ, включая документацию в электронном виде, (далее – Изделие) принадлежат ООО «КРИПТО-ПРО», далее – Правообладатель.
2. Настоящее соглашение является офертой ООО «КРИПТО-ПРО» к физическому или юридическому лицу, далее – Пользователь.
3. Пользователь в соответствии с настоящим соглашением получает право использовать Изделие на территории Российской Федерации.
4. Установка Изделия в память ЭВМ рассматривается как безусловное согласие Пользователя с условиями настоящего соглашения.
5. В случае несогласия с каким-либо из условий настоящего соглашения Пользователь не имеет права продолжать установку Изделия в память ЭВМ, а в случае установки Изделия в память ЭВМ обязан удалить Изделие из

Я согласен с Лицензионным соглашением. Перейти к загрузке.

### Услуги СЭП

- СЭП Аккредитованного УЦ 63-ФЗ
- СЭП Неаккредитованного УЦ
- СЭП со сторонним УЦ

### Подписка на обновления

- Новости
- Блог

Читать

Рис. 2.4 — Согласие с условиями Лицензионного соглашения

## 2.4 Выбрать последнюю сертифицированную версию КриптоПро CSP (Рис. 2.5)

КРИПТОПРО КриптоПро  
Ключевое слово в защите информации

О компании | **Продукты** | Услуги | Партнёры | Поддержка | Приобретение | Загрузка | Блог | Форум

Главная > Продукты > СКЗИ КриптоПро CSP

## КриптоПро CSP - Загрузка файлов

**Предварительные несертифицированные версии**

- [КриптоПро CSP 4.0 R4 для Windows, macOS и UNIX](#) (несертифицированный)
- [КриптоПро CSP 3.9 R3 для Windows, UNIX и macOS](#) (несертифицированный)
- [КриптоПро CSP 5.0 для Windows, macOS и UNIX](#) (несертифицированный)
- [КриптоПро CSP для Google Android](#) (несертифицированный)

**Сертифицированные версии**

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

СКЗИ КриптоПро CSP

- Использование
- КриптоПро TLS
  - Совместимость реализаций TLS
- КриптоПро EAP-TLS
- Настройка КриптоПро CSP для nginx и Apache
- КриптоПро Java CSP
- КриптоПро Winlogon
- Считыватели
- Библиотека считывателей
- Загрузка файлов**
- История версий
- Сравнение версий
- Совместимость реализаций X.509 и

Рис. 2.5 — Выбор последней сертифицированной версии КриптоПро CSP

## 2.5 Загрузить программу КриптоПро CSP, соответствующую ОС (Рис. 2.6).

Для Windows:

> **КриптоПро CSP 4.0 для Windows**

Контрольная сумма  
ГОСТ: 86A28288818135182723A88E97891CF919981CBA8035A12207C98A1ED36AD357  
MD5: ebc28b6ef14d8dd5be71868bb6d98b1f

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

CSPSetup.exe

## Сертифицированные версии

[КриптоПро CSP 4.0 R3](#) для [Windows](#), [macOS](#) и [UNIX](#)

[КриптоПро CSP 3.9 R3](#)

Сертифицирован

[КриптоПро CSP 3.6 R3](#)

[КриптоПро CSP 3.6 R2](#)

СКЗИ с долговре

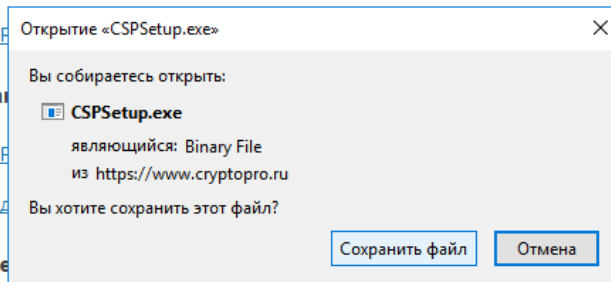


Рис. 2.6 — Загрузка программы КриптоПро CSP

2.6 Установить программу КриптоПро, для этого нужно выполнить ранее загруженный установщик (Рис. 2.7).

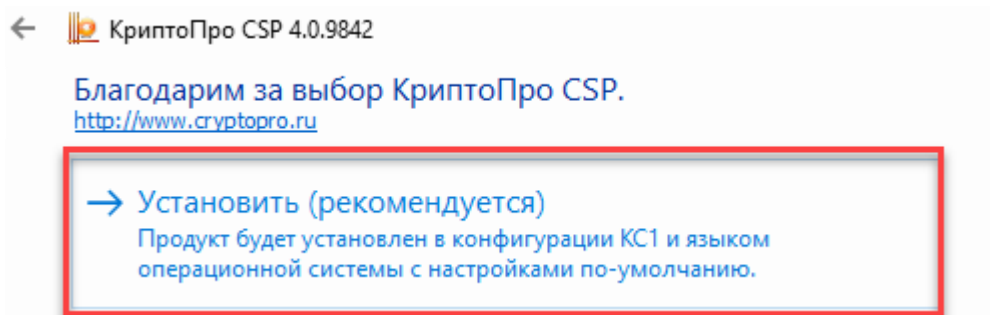


Рис. 2.7 — Установка программы КриптоПро CSP

## 3. Загрузка и установка КриптоПро ЭЦП Browser plug-in:

3.1 Перейти по прямой [ссылке](#) или выбрать продукт «КриптоПро ЭЦП Browser plug-in» в разделе «Продукты» сайта [КриптоПро](https://www.cryptopro.ru/) (<https://www.cryptopro.ru/> – Продукты – КриптоПро ЭЦП Browser plug-in) (Рис. 3.1):

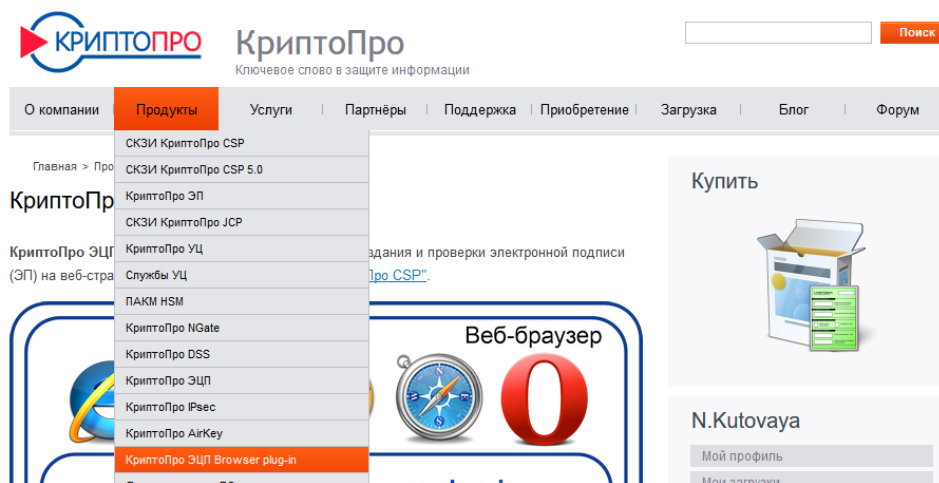
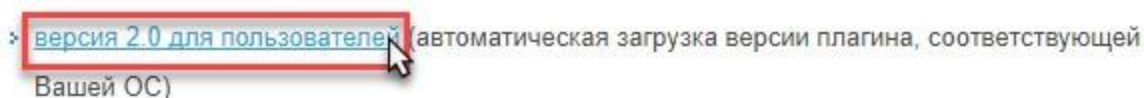


Рис. 3.1 — Выбор продукта «КриптоПро ЭЦП Browser plug-in»

3.2 Загрузить актуальную версию КриптоПро ЭЦП Browser plug-in (для пользователей) (Рис. 3.2):

Скачать актуальную версию КриптоПро ЭЦП Browser plug-in:



- › [версия 2.0 для пользователей](#) (автоматическая загрузка версии плагина, соответствующей Вашей ОС)

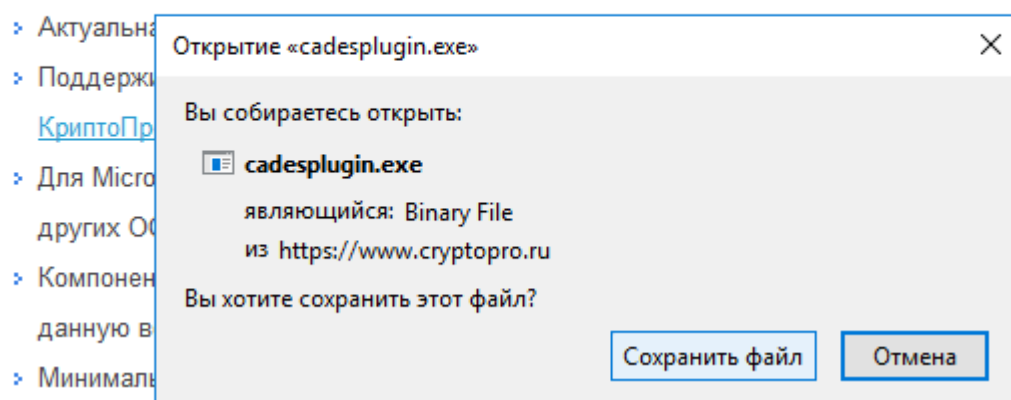


Рис. 3.2 — Загрузка КриптоПро ЭЦП Browser plug-in

3.3 Установить «КриптоПро ЭЦП Browser plug-in», для этого нужно выполнить ранее загруженный установщик (Рис. 3.3):

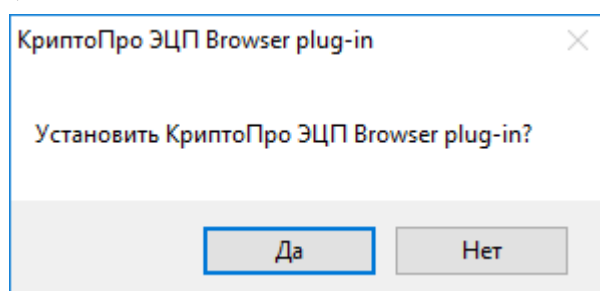


Рис. 3.3 — Установка КриптоПро ЭЦП Browser plug-in

3.4 Перезагрузить браузер

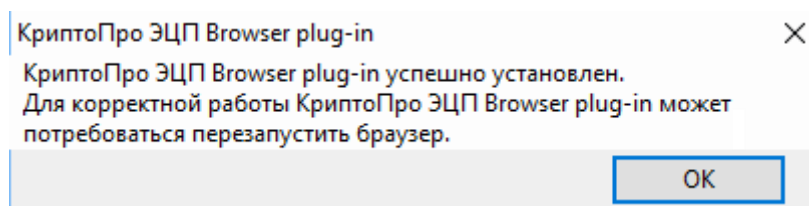


Рис. 3.4 — Завершение установки КриптоПро ЭЦП Browser plug-in

## 4. Активация плагина «КриптоПро ЭЦП Browser plug-in»:

Чтобы активировать плагин «КриптоПро ЭЦП» в Вашем браузере, кликните по одной из ссылок ниже, в зависимости от используемого Вами браузера.

[Google Chrome](#)

[Yandex Browser](#)

[Opera](#)

### 4.1 Google Chrome

Необходимо перейти по ссылке для установки расширения в интернет-магазине Chrome:

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

И нажать “Установить” (Рис.4.1)

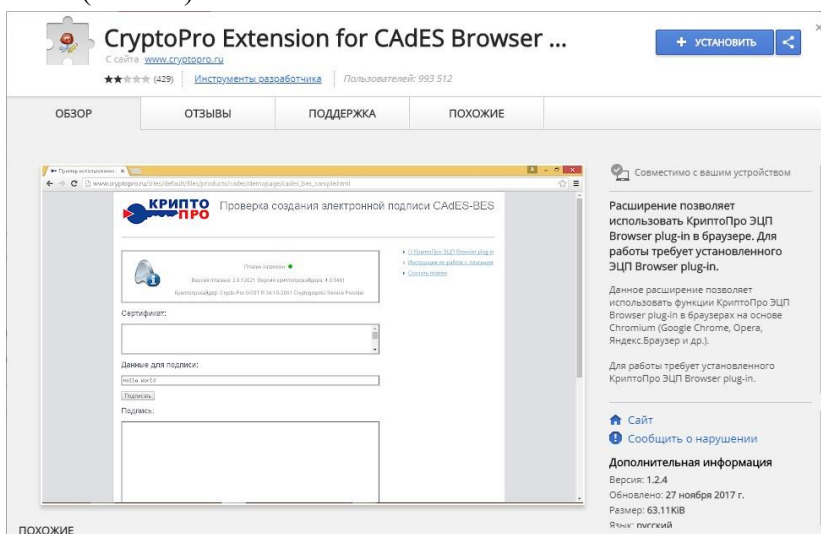
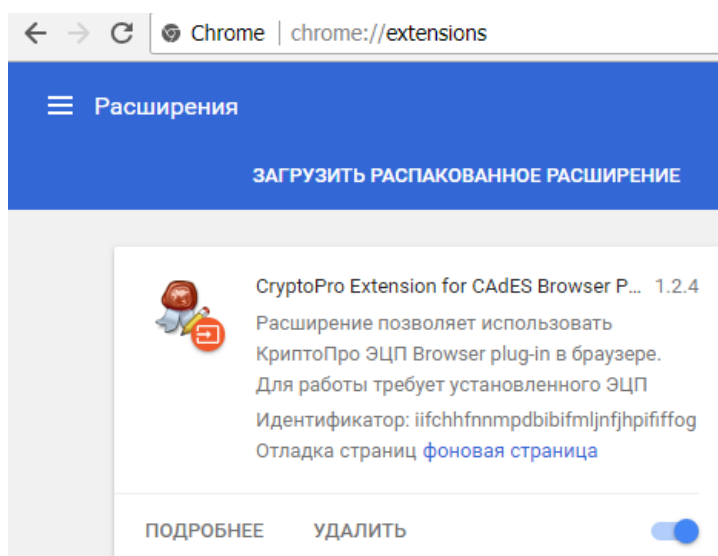
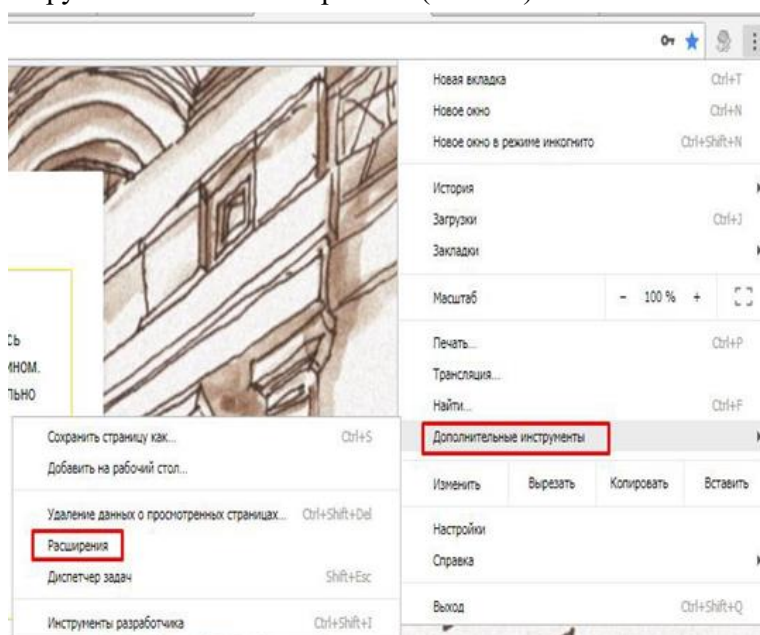


Рис. 4.1 — Установка CryptoPro Extension

В дальнейшем включить или отключить плагин вы можете в настройках браузера «Дополнительные инструменты» — «Расширения» (Рис.4.2)





**Примечание:** Если расширения «CryptoPro Extension for CAAdES Browser Plug-in» нет в списке доступных, нужно перезапустить браузер.

## 4.2 Yandex Browser

Скачайте расширение по [ссылке](#) и нажмите установить (Рис.4.3)

The screenshot shows the Yandex Browser extension marketplace page for the 'CryptoPro Extension for CAAdES Browser Plug-in'. At the top, there is a search bar and a compatibility indicator for Yandex Browser. The extension card features a red seal icon, the title 'Расширение CryptoPro для плагина браузера CAAdES по КриптоПро', a 4-star rating from 7 reviews, and a green 'Добавить в Яндекс.Браузер' button. Below the card, there is a description: 'Расширение CryptoPro для CAAdES Browser Plug-in позволяет использовать CryptoPro CSP из JavaScript в браузерах. Требуется модуль браузера CryptoPro для работы.' There are links for 'Разрешения' and 'Скриншот'. The 'Скриншот' section shows a screenshot of the 'КРИПО ПРО' interface for checking the creation of an electronic signature (CAAdES-BES). To the right, there is a section 'О расширении' with statistics: 870,083 downloads, category 'Средства разработки', version 1.2.7, size 60.4 KB, last update July 30, 2018, and support links. Below this is a 'Похожие' section with two other extensions: 'Расширение Codecov' and 'редактировать страницу'. At the bottom, there is a second extension card for the same extension, but with a yellow 'Установка' button. A dialog box is overlaid on the bottom card, asking 'Установить "CryptoPro Extension for CAAdES Browser Plug-in"?' and listing permissions: 'Просматривать и изменять ваши данные на посещаемых сайтах' and 'Работать с приложениями, разработанными специально для ОС этого устройства'. The 'Установить расширение' button in the dialog is highlighted with a red box.

Рис. 4.3 — Установка CryptoPro Extension Yandex Browser

Возможно потребуется дополнительно включить расширение, для этого необходимо зайти в раздел «Дополнения» и включить КриптоПро ЭЦП, затем перезапустить браузер (Рис.4.4)

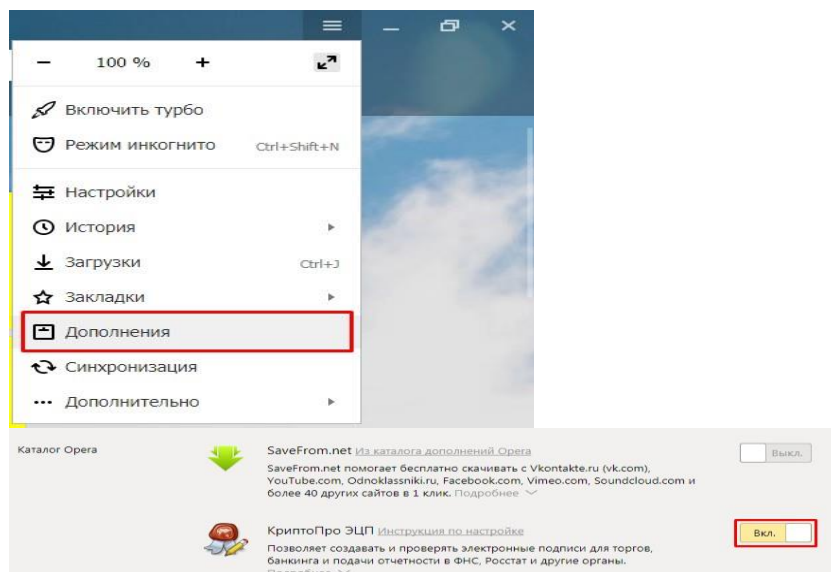


Рис. 4.4 — Активация CryptoPro Extension Yandex Browser

### 4.3 Opera

Для корректной работы плагина необходимо добавить расширение КриптоПро: Opera – расширение доступно по [ссылке](#). (Рис.4.5)



Рис. 4.5 — Установка CryptoPro Extension Opera

Нажать «Добавить в Опера»

Зайти в меню в Опера – расширения и отметить все чекбоксы на вкладке Extensions: (Рис.4.6)

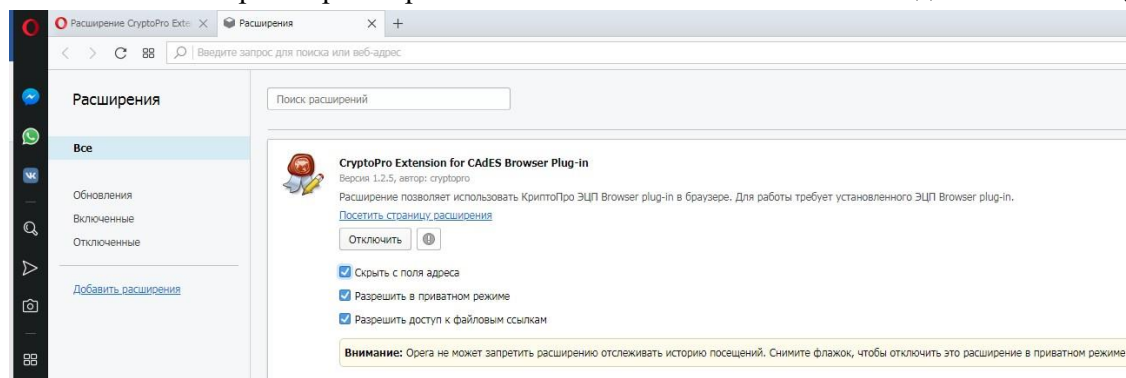


Рис. 4.6 — Активация CryptoPro Extension Opera

## 5. Проверка работы плагина

Перейдите на [специальную страницу](#)

Если отображается «плагин недоступен» (Рис.5.1):

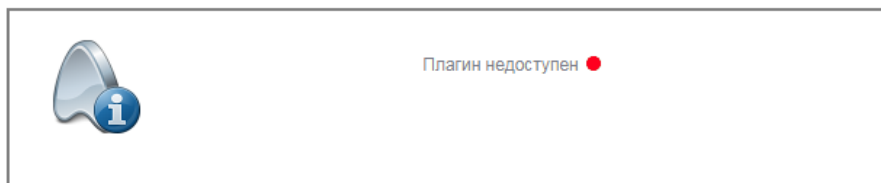


Рис. 5.1 — Плагин CryptoPro недоступен

Необходимо выполнить действия указанные в п.4

Если приложения установлены, при входе на страницу появится предупреждение о том, что плагин запрашивает доступ к ключам и сертификатам (Рис.5.2).



### Проверка работы КриптоПро ЭЦП Browser plug-in

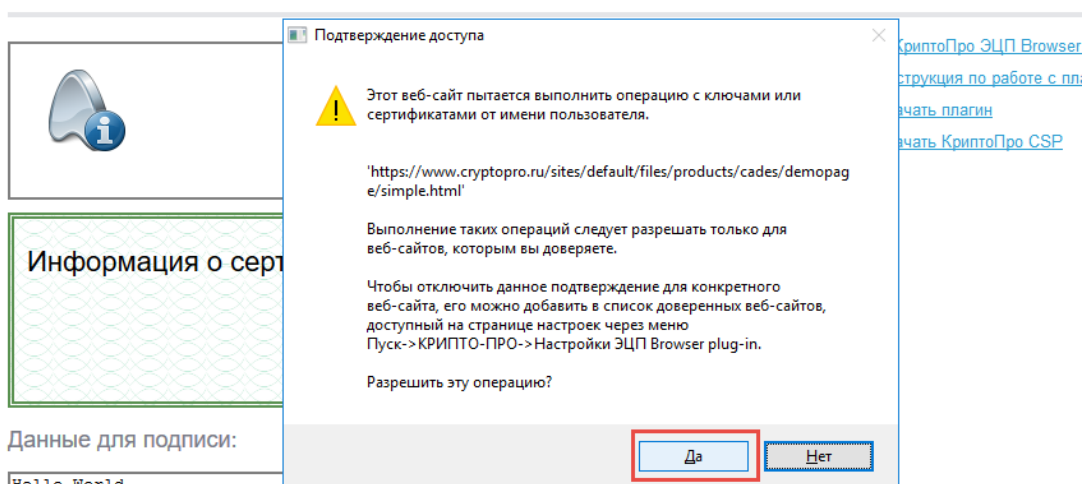


Рис. 5.2 — Подтвердить доступ

Необходимо согласиться.

Если у вас появляется сообщения, то Плагин успешно установлен на компьютер:

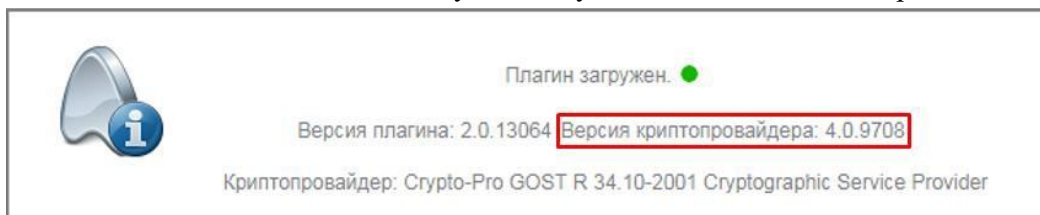


Рис. 5.3 — Плагин CryptoPro доступен

## 6. Добавление корневых сертификатов в список доверенных

Для выполнения добавления сертификатов предварительно необходимо:

- 6.1 Скачать файл открытого ключа УКЭП или иметь на руках носитель с установленным сертификатом, например, [USB ключ "Рутокен КП"](#).
- 6.2 Открыть свойства персонального сертификата (Рис. 6.1) (пример [USB ключ "Рутокен КП"](#))  
Открыть Панель управления Рутокен – Сертификаты – Выбрать сертификат – Свойства

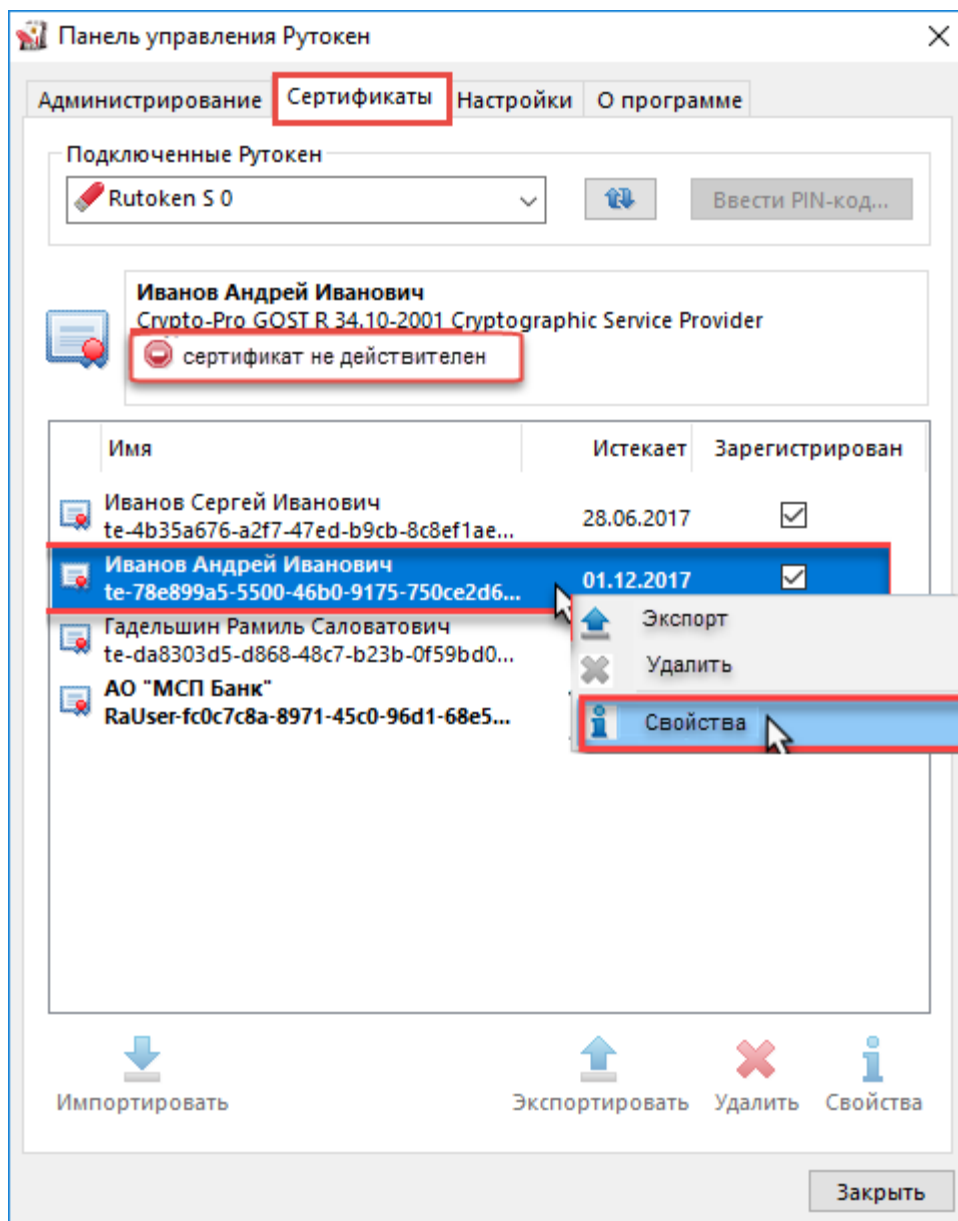


Рис. 6.1 — Открытие свойств персонального сертификата в программе Рутокен

- 6.3 Открыть корневой сертификат (Рис. 6.2) (верхний в цепочке сертификатов)  
**Путь сертификации** – Корневой сертификат – Просмотр сертификата

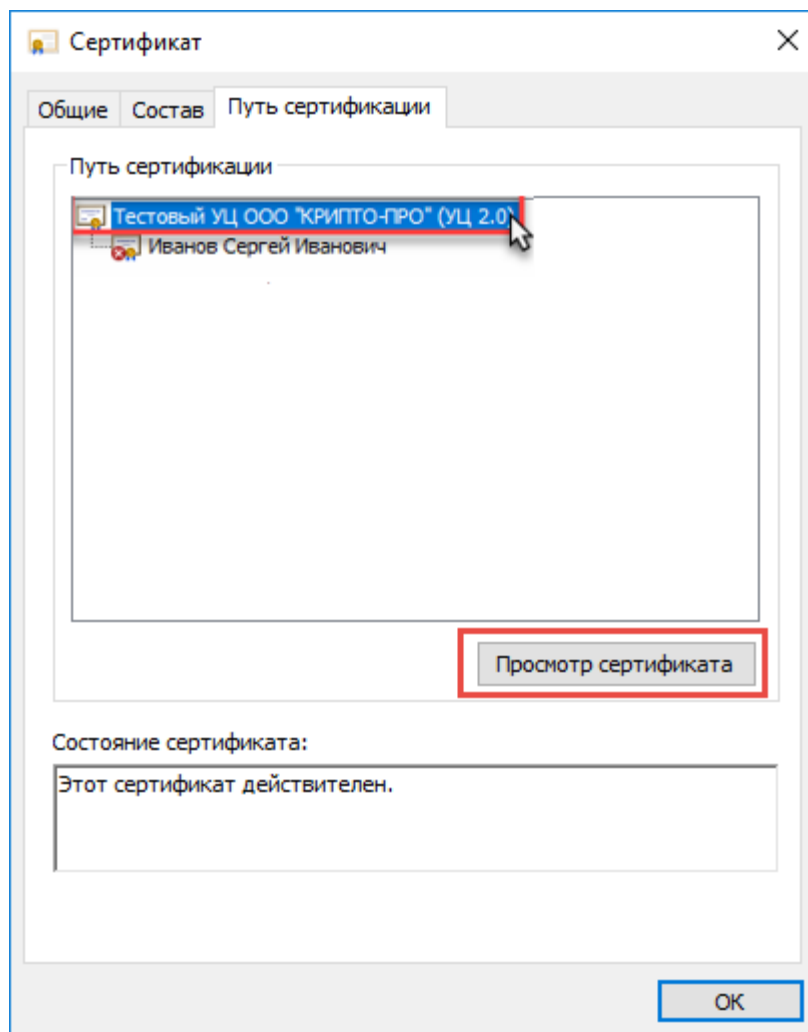


Рис. 6.2 — Открытие корневого сертификата в программе Рутокен

6.4 Экспорт корневого сертификата (Рис. 6.3)  
Состав–Копировать в файл - Далее-далее..

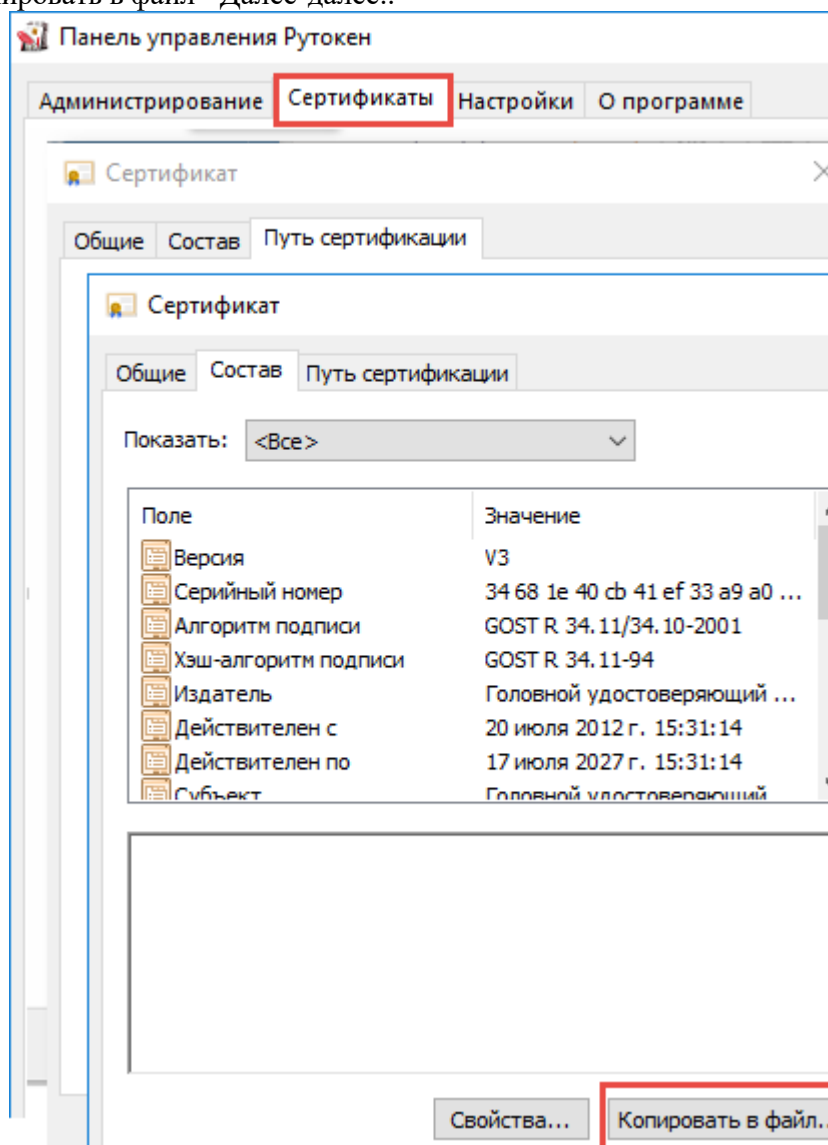


Рис. 6.3 — Экспорт корневого сертификата в программе Рутокен

- 6.5 Выбрать директорию и имя экспортированного сертификата Выбрать директорию и имя файла – Далее – Готово (Рис. 6.4)

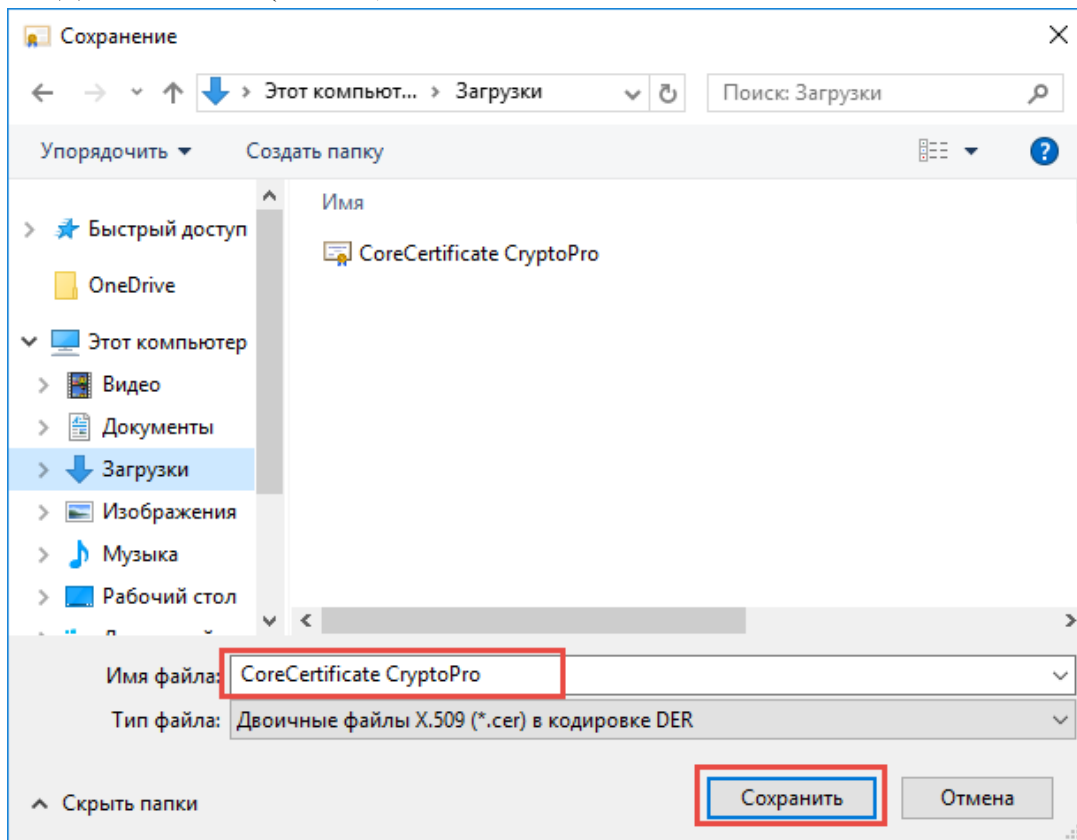


Рис. 6.4 — Сохранение корневого сертификата в программе Рутокен

- 6.6 Добавление корневого сертификата в список доверенных (Рис. 6.5)  
Выбрать файл сертификата – Установить сертификат - Локальный компьютер – Автоматически выбрать хранилище на основе типа сертификата – Далее

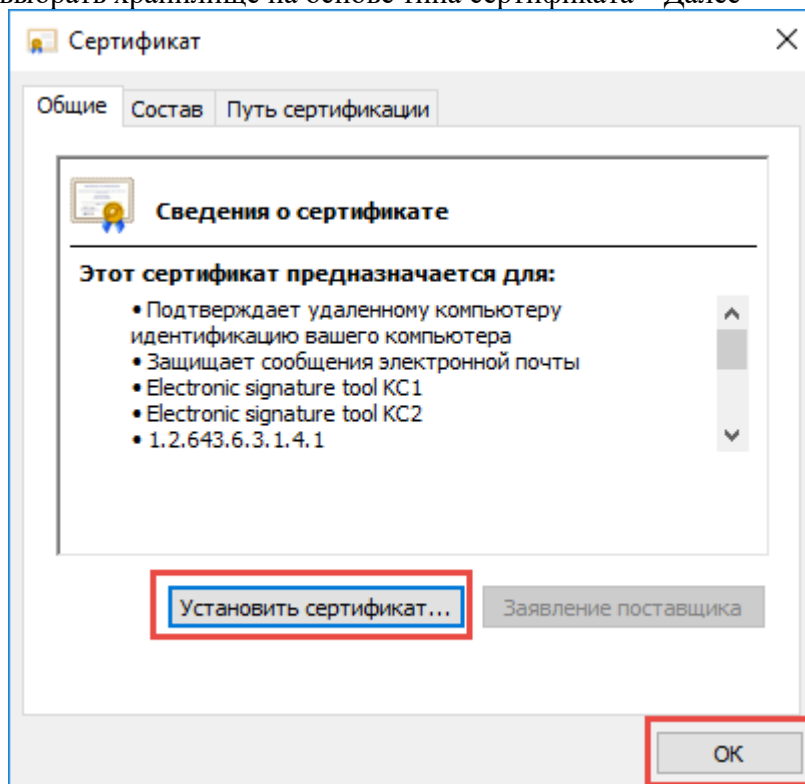


Рис. 6.5 — Добавление корневого сертификата в список доверенных

- 6.7 Выбор хранилища для установки корневого сертификата необходимо установить в Доверенные корневые центры сертификации и Доверенные издатели (Рис. 6.6) Поместить все сертификаты в следующее хранилище – Обзор... – Доверенные корневые центры сертификации + Доверенные издатели – ОК – Далее – Готово

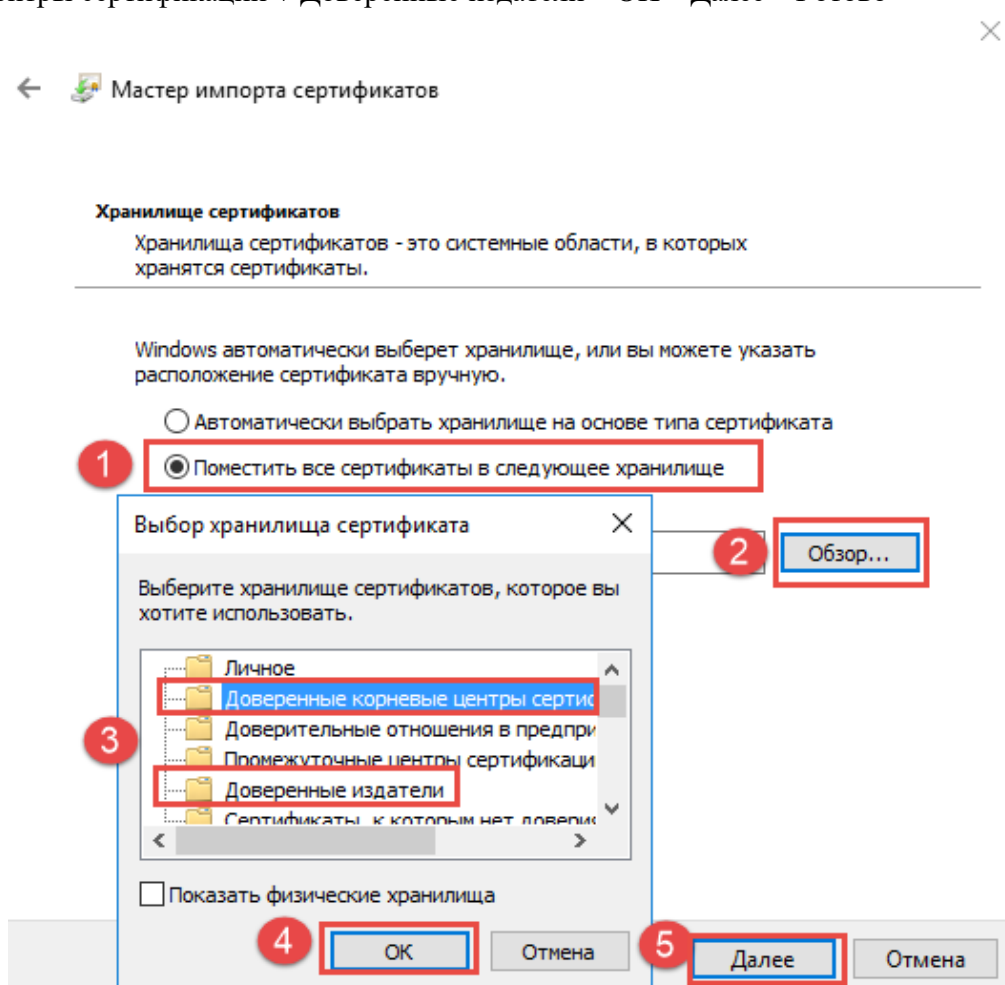


Рис. 6.6 — Выбор хранилища для установки корневого сертификата

После выполнения завершения установки всех программ, плагинов и сертификатов нужно перезагрузить ПК.





## 7.2 Свойства параметра «Владелец сертификата» / «Субъект», см. Рис.7.2:

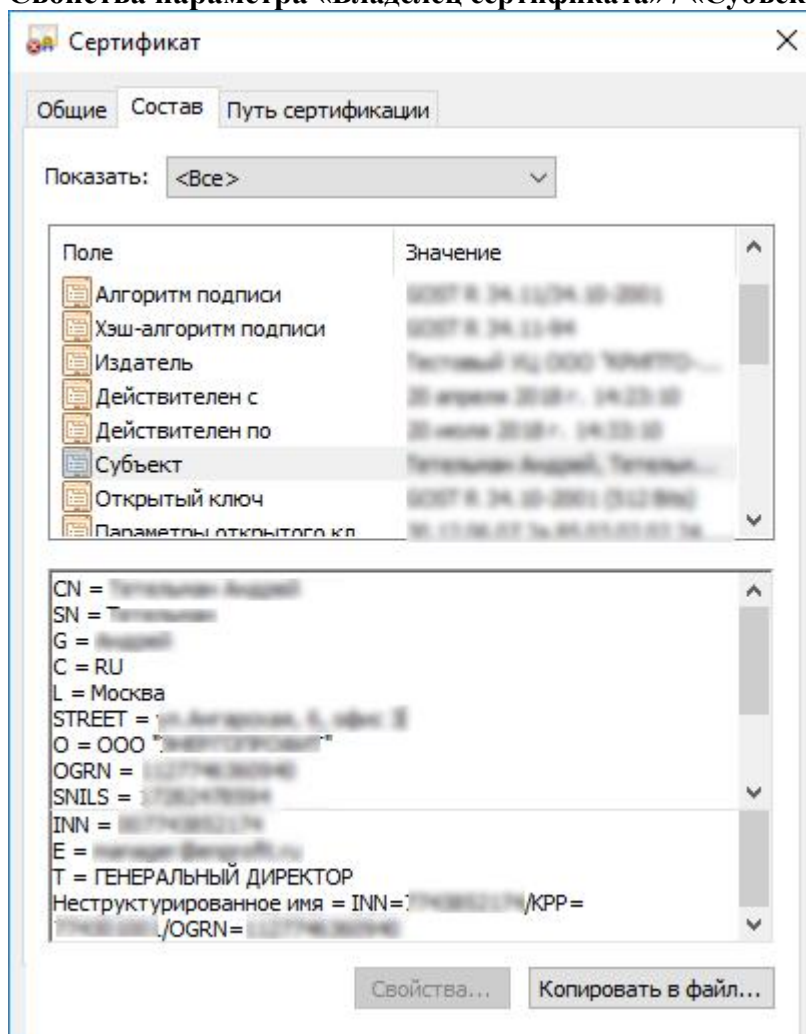


Рис.7.2 Свойства поля «Владелец сертификата» / «Субъект» сертификата УКЭП

7.2.1 Поле «Владелец сертификата» / «Субъект» содержит следующие компоненты имени и формируется следующим образом:

- Параметр «Общее имя» (**CN**, Common Name), содержащий фамилию, имя, отчество (при наличии) владельца сертификата УКЭП – физического лица;
- параметр «Идентификационный номер налогоплательщика владельца сертификата УКЭП – юридического лица, **INN**» (для владельца УКЭП юридического лица);
- параметр «Основной государственный регистрационный номер владельца УКЭП – юридического лица, **OGRN**» (для владельца УКЭП юридического лица);
- параметр «Страховой номер индивидуального лицевого счета владельца УКЭП сертификата физического лица, **SNILS**» (для физического лица);
- параметр «Должность (**T**, Title)», содержащий должность владельца сертификата УКЭП для юридических лиц;
- параметр «Организация (**O**, Organization)», содержащий название юридического лица;
- параметр «Город (**L**, Locality)», содержащий название населенного пункта, в котором расположена организация владельца сертификата;
- параметр «Страна (**C**)», содержащая название страны, в которой расположена организация владельца сертификата;
- параметр «Адрес, **STREET**»;
- параметр «Адрес электронный почты (**E**, EMail)», содержащий адрес электронной почты владельца сертификата ключа подписи.

## 8. Часто задаваемые вопросы

### 8.1 Можно ли подписать документ без наличия ключевого носителя (USB ключа Рутокен)?

Обеспечение аппаратной генерации ключей и формирования ЭП происходит в микропроцессоре ключевого носителя (например, [USB кл юч "РуТ окон К П"](#)), поэтому наличие ключевого носителя является обязательным условием для подписания.

### 8.2 Как посмотреть список сертификатов, доступных для выбора в браузере?

Для просмотра списка установленных сертификатов нужно открыть список персональных сертификатов, выполнить следующие действия (Рис. 8.1):

Панель управления – Сеть и интернет – Свойства браузера – Содержание – Сертификаты – Личные

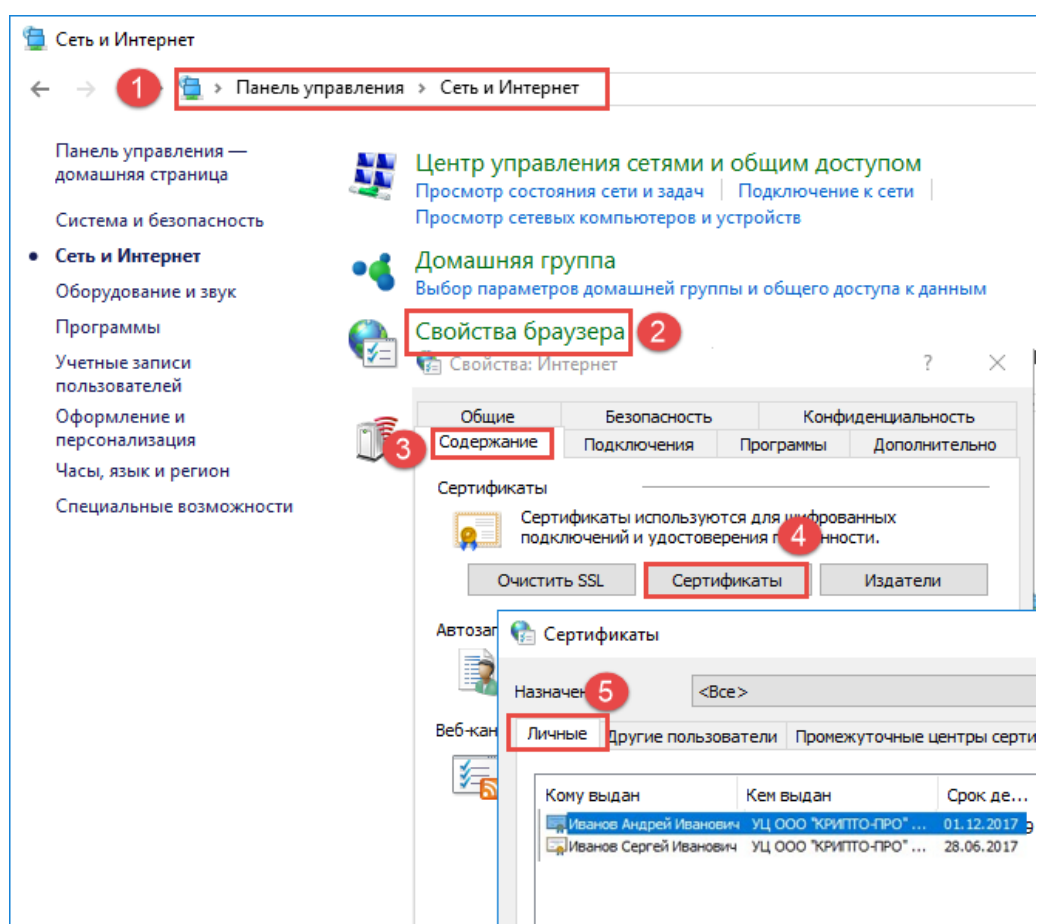


Рис. 8.1 — Просмотр списка установленных персональных сертификатов

Для просмотра списка сертификатов в программе Рутокен необходимо выполнить действия (Рис. 8.2):

Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты

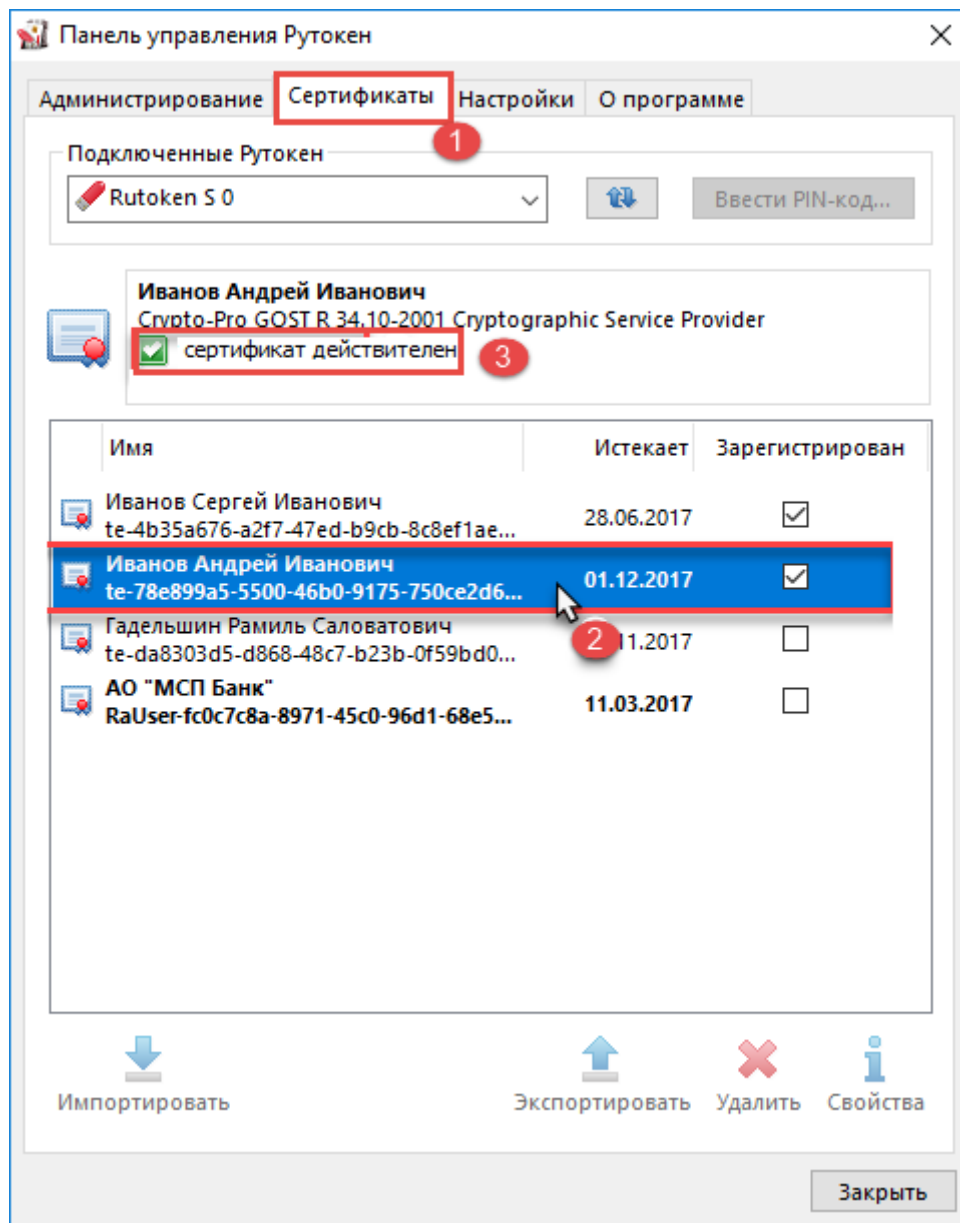


Рис. 8.2 — Просмотр списка сертификатов ключевого носителя, проверить валидность сертификата

Для просмотра статуса сертификата, необходимо открыть список сертификатов ключевого носителя (Рис. 8.2) и выбрать необходимый сертификат. Статус сертификата отобразится в области основной информации.

Также можно посмотреть валидность всей цепочки для выбранного сертификата. Для этого нужно открыть свойства сертификата и посмотреть цепочку сертификатов (перейти на вкладку Путь сертификата) (Рис. 8.3)

Статус сертификата, выбранного из цепочки, отобразится в области Состояние сертификата. Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты – Свойства – Путь сертификации – Выбрать сертификат из цепочки

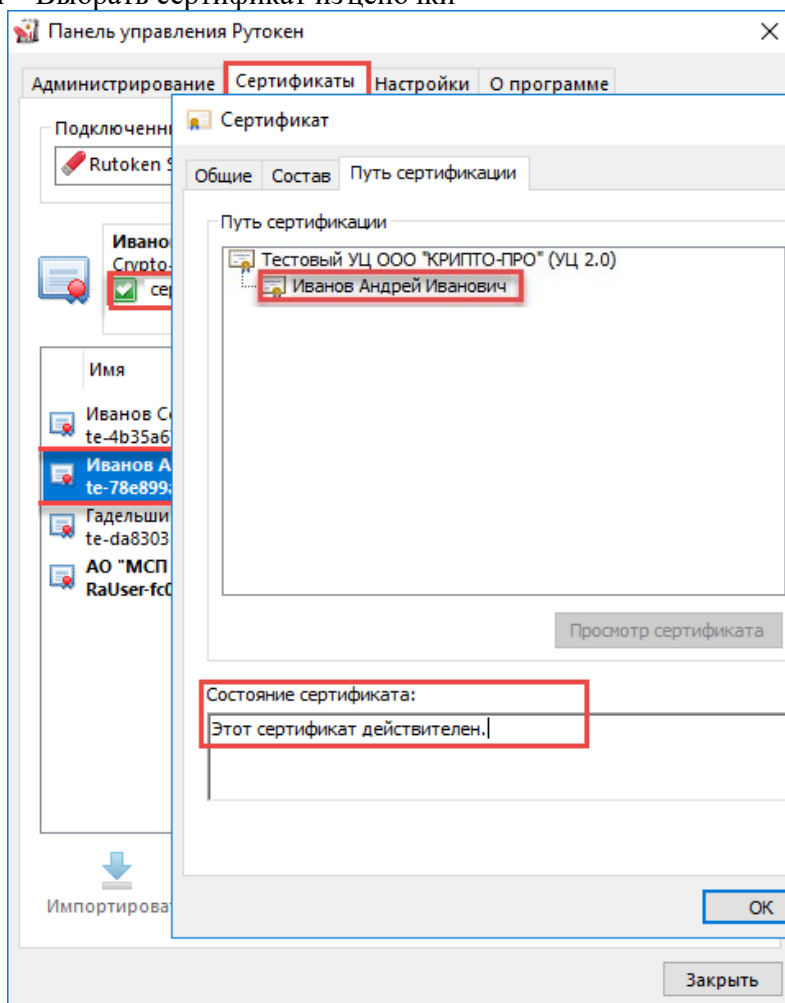


Рис. 8.3 — Просмотр статуса сертификата из цепочки сертификатов

### 8.3 Как добавить новый сертификат, в список доступных для выбора вбраузере?

Доступные для выбора сертификаты можно посмотреть в хранилище персональных сертификатов (пример ОС Windows) (Рис. 8.1).

При использовании программы Рутокен, добавление персональных сертификатов происходит автоматически, для этого должен быть проставлен признак «Зарегистрирован» для соответствующего (поставлен по умолчанию) сертификата в Рутокен (Рис. 8.4).

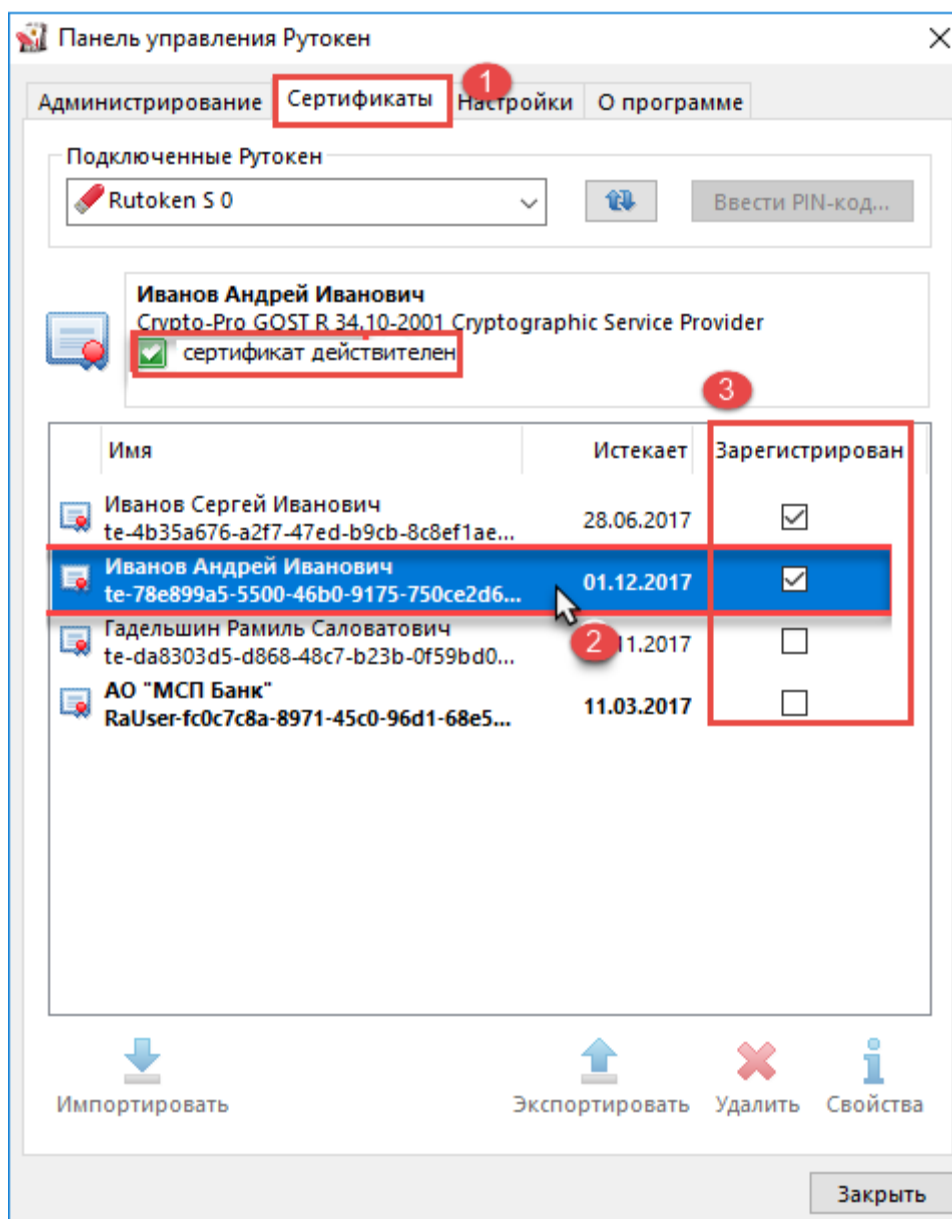


Рис. 8.4 — Просмотр признака Registered сертификатов ключевого носителя

Ручное добавления персонального сертификата аналогично добавлению корневых сертификатов, при этом на этапе выбора хранилища нужно установить значение «Личное» (Рис. 8.1):

Поместить все сертификаты в следующее хранилище – Обзор... – Личное – ОК – Далее – Готово

#### 8.4 Как экспортировать файл сертификата из хранилища ПК, ключевого носителя

Для экспорта файла сертификата из хранилища ПК нужно выполнить действия (Рис. 8.5):

Панель управления – Сеть и интернет – Свойства браузера – Содержание – Сертификаты – Личные (Открыть соответствующее хранилище сертификатов) – Выбрать сертификат – Экспорт... – Далее – Нет, не экспортировать закрытый ключ – Далее – Далее – Обзор.. – заполнить имя и путь файла – Далее – Готово

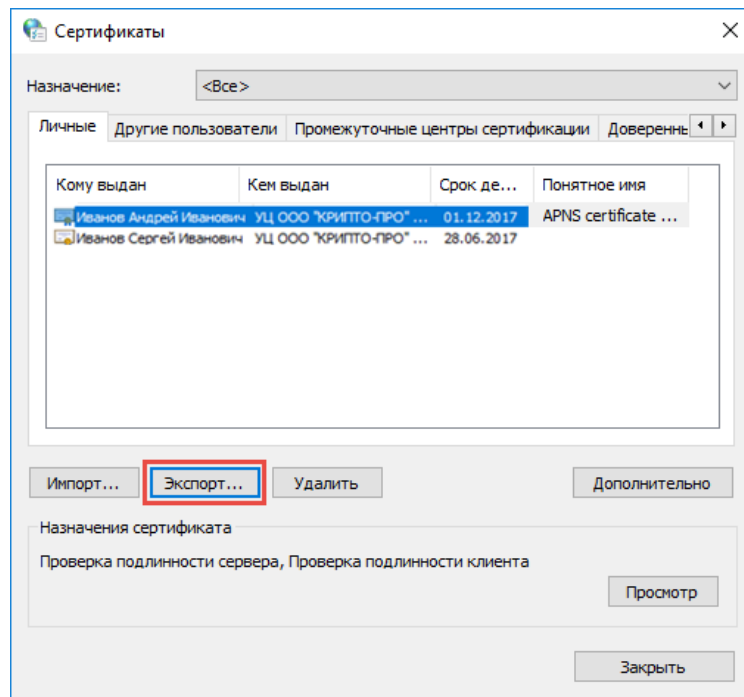


Рис. 8.5 — Экспорт файла сертификата из хранилища ПК

Для экспорта файла сертификата из ключевого носителя нужно выполнить действия (Рис. 8.6): Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты – Свойства – Выбрать сертификат – Экспорт — Обзор – заполнить имя и путь файла – Экспорт

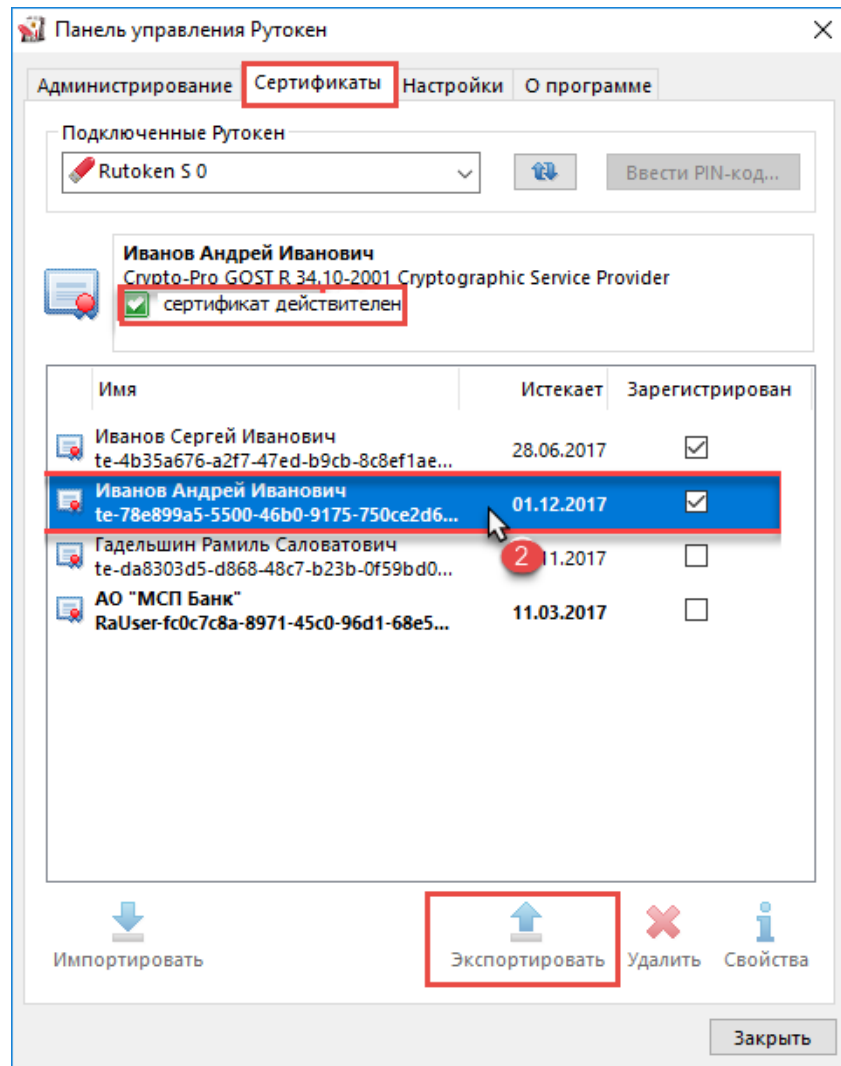


Рис. 8.6 — Экспорт файла сертификата из ключевого носителя средствами программы Рутокен



## 8.5 Как удалить из списка сертификатов, доступных для выбора в браузере, неактуальные записи (отозванные, просроченные...)

Доступные для выбора сертификаты можно посмотреть в хранилище персональных сертификатов (Рис. 8.7). Для удаления персональных сертификатов в ПК, рекомендуется:

Извлечь из ПК [USB ключ](#) (например, "[Рутокен КП](#)") - Открыть хранилище персональных сертификатов – Выбрать неактуальную запись – Remove

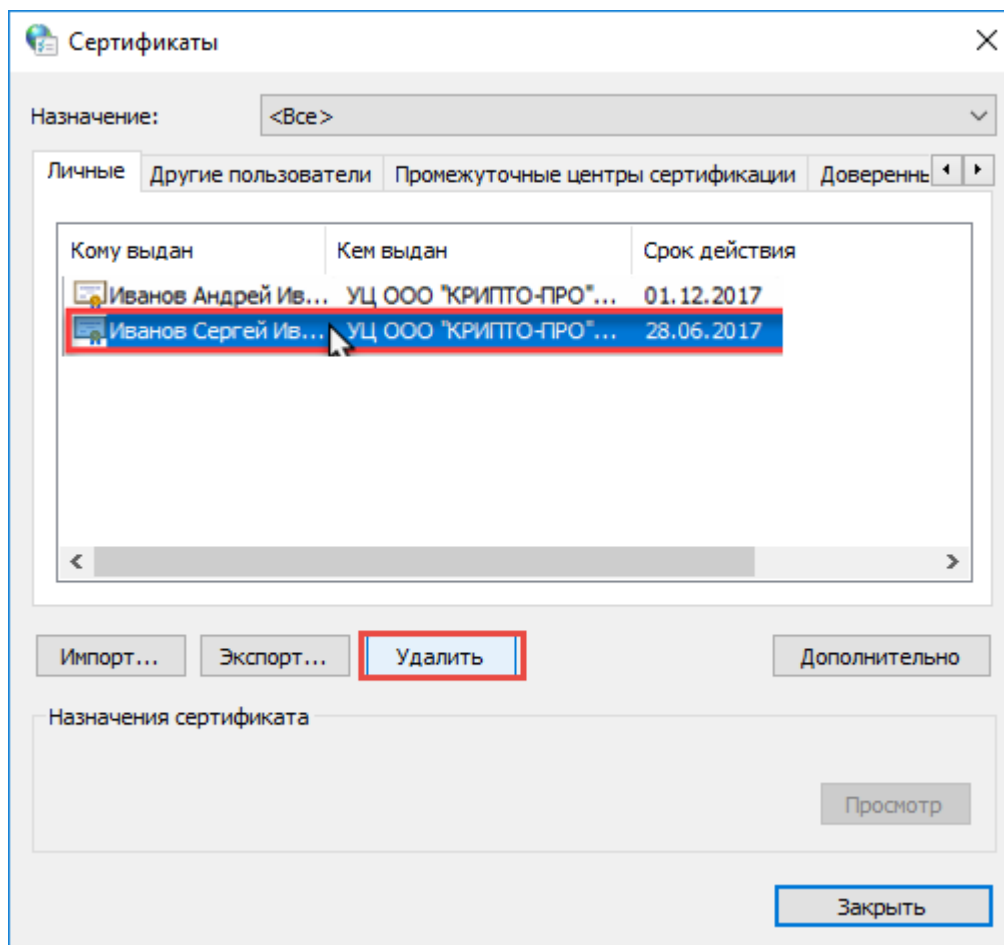


Рис. 8.7 — Удаление сертификата из хранилища ПК

## 8.6 Ошибка при подписании документов на портале [smbfin.ru](#) АИС НГС

Описание ошибки «Ошибка создания подписи A certificate chain could not be built to a trusted root authority» (см.скриншот Рис.8.8):

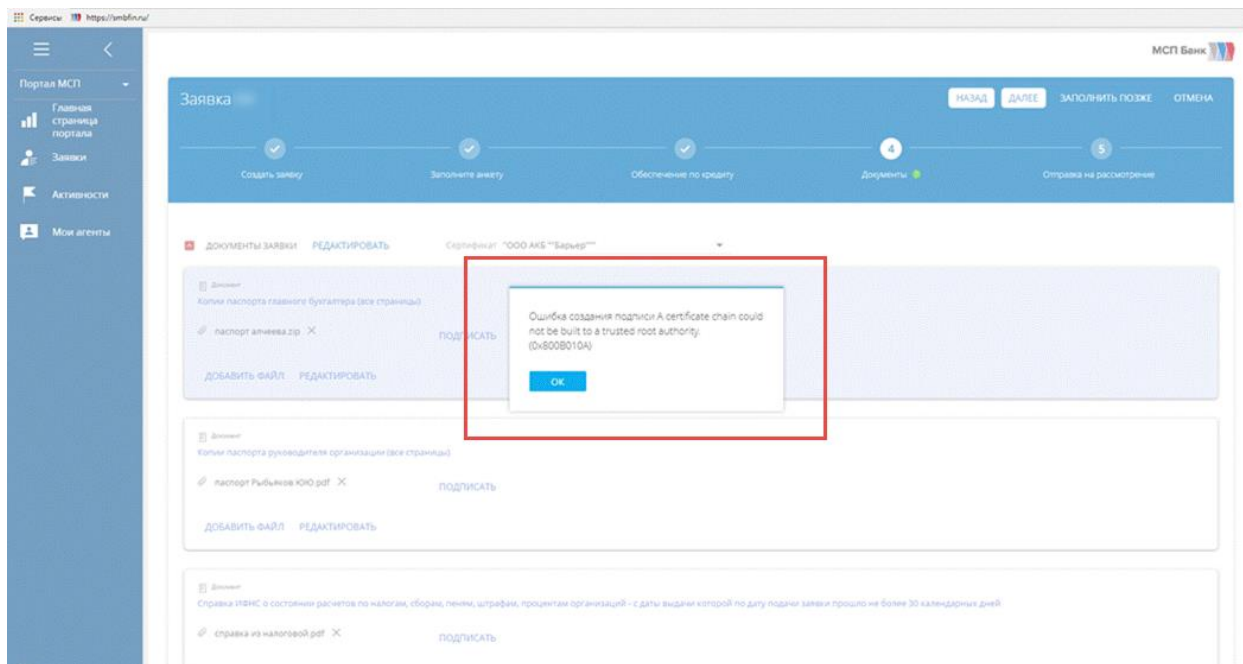


Рис. 8.8 — Ошибка создания подписи

Для решения проблемы нужно:

### 8.6.1. Проверить валидность цепочки сертификатов на ключевом носителе

Для просмотра списка цепочки сертификатов в программе Рутокен необходимо выполнить действия (Рис. 8.9):

Подключить ключевой носитель – Открыть Панель Управления Рутокен – Сертификаты

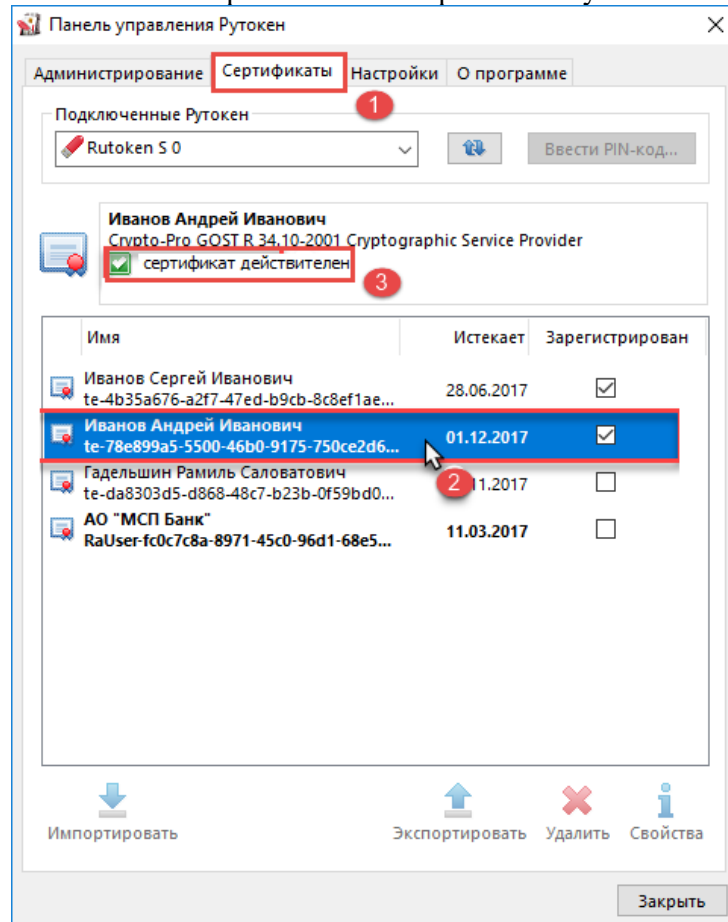


Рис. 8.9 — Просмотр списка сертификатов ключевого носителя, проверка валидности сертификата

Далее нужно просмотреть валидность всей цепочки для выбранного сертификата.

Для этого необходимо открыть свойства сертификата и просмотреть цепочку сертификатов (перейти на вкладку Путь сертификации) (Рис. 8.10)

Статус сертификата, выбранного из цепочки, отобразится в области Статус сертификата. Необходимо просмотреть статусы всех сертификатов цепочки.

Если в цепочке есть невалидные сертификаты – подписание документов невозможно.

Подключить ключевой носитель – Открыть Панель управления Рутокен – Сертификаты – Свойства – Путь сертификации – Выбрать сертификат из цепочки

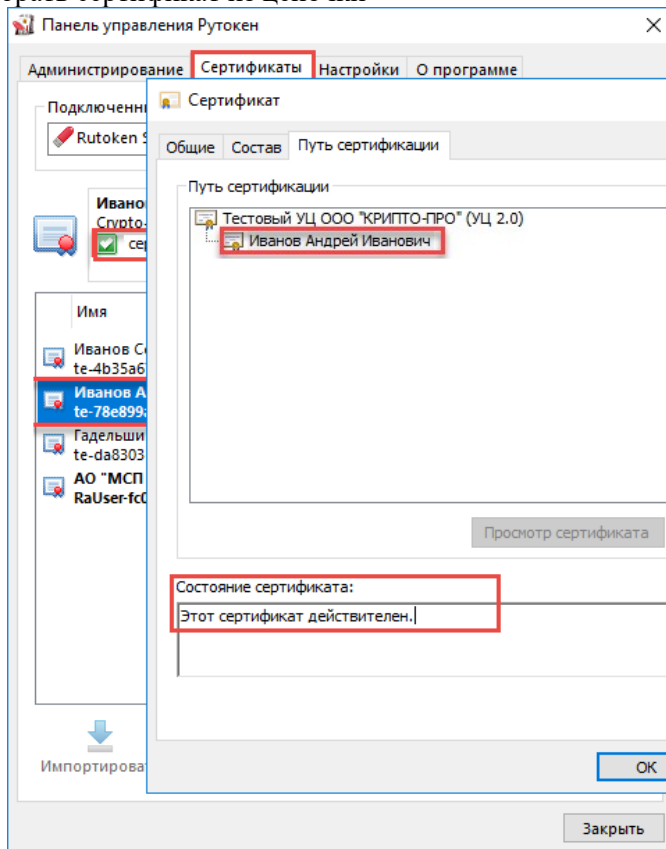


Рис. 8.10 — Просмотр статуса сертификата из цепочки сертификатов

### 8.6.2 Просмотреть список сертификатов ПК

Для просмотра списка установленных сертификатов нужно открыть список персональных сертификатов, выполнить следующие действия (Рис. 8.11):

Панель управления – Сеть и интернет – Свойства браузера – Содержание – Сертификаты – Личные + Доверенные корневые центры сертификации + Доверенные издатели

В хранилище Личные – должен быть только один сертификат пользователя, соответствующий сертификату на ключевом носителе

В хранилищах Доверенные корневые центры сертификации + Доверенные издатели – должны быть корневые сертификаты, соответствующие корневым сертификатам (наивысший в цепочке сертификатов) на ключевом носителе

В хранилище Издатели, не имеющие доверия – не должно быть сертификатов, входящих в состав цепочки ключевого носителя. В случае отсутствия в хранилище корневых сертификатов, их нужно дополнительно установить из ключевого носителя.

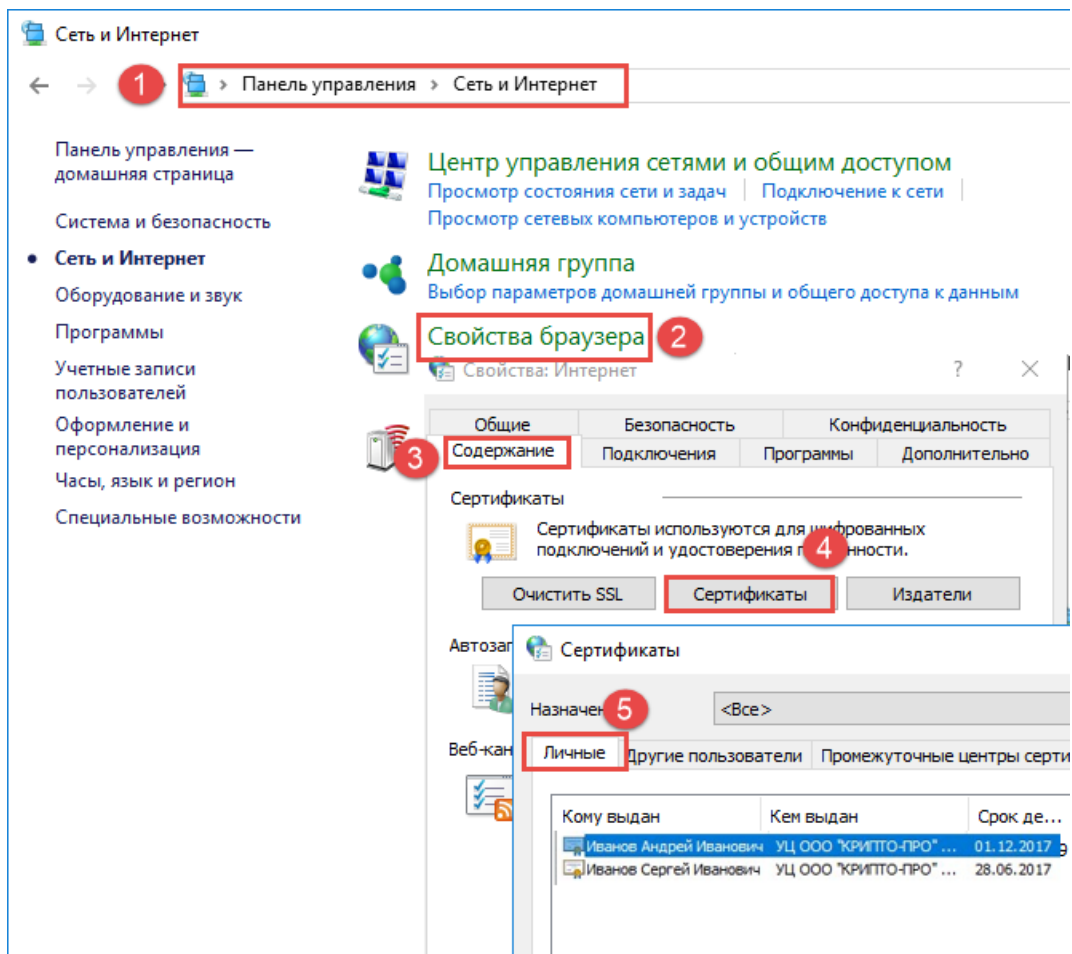


Рис. 8.11 — Просмотр списка установленных персональных сертификатов

### 8.6.3 Проверить подписание документов на сайте CryptoPro по ссылке

#### [Проверка создания электронной подписи CAdES-BES](#)

Для проверки нужно выполнить действия (Рис. 8.12):

- Подключить ключевой носитель [USB ключ](#) – Открыть страницу [Проверка создания электронной подписи CAdES-BES](#) [1] – Выбрать проверяемый сертификат в области «Сертификат» [2] – Загрузить файл [3] (который не удалось подписать в АИС НГС) – Нажать кнопку «Подписать файл» [4] – Проверить результат формирования подписи [4]

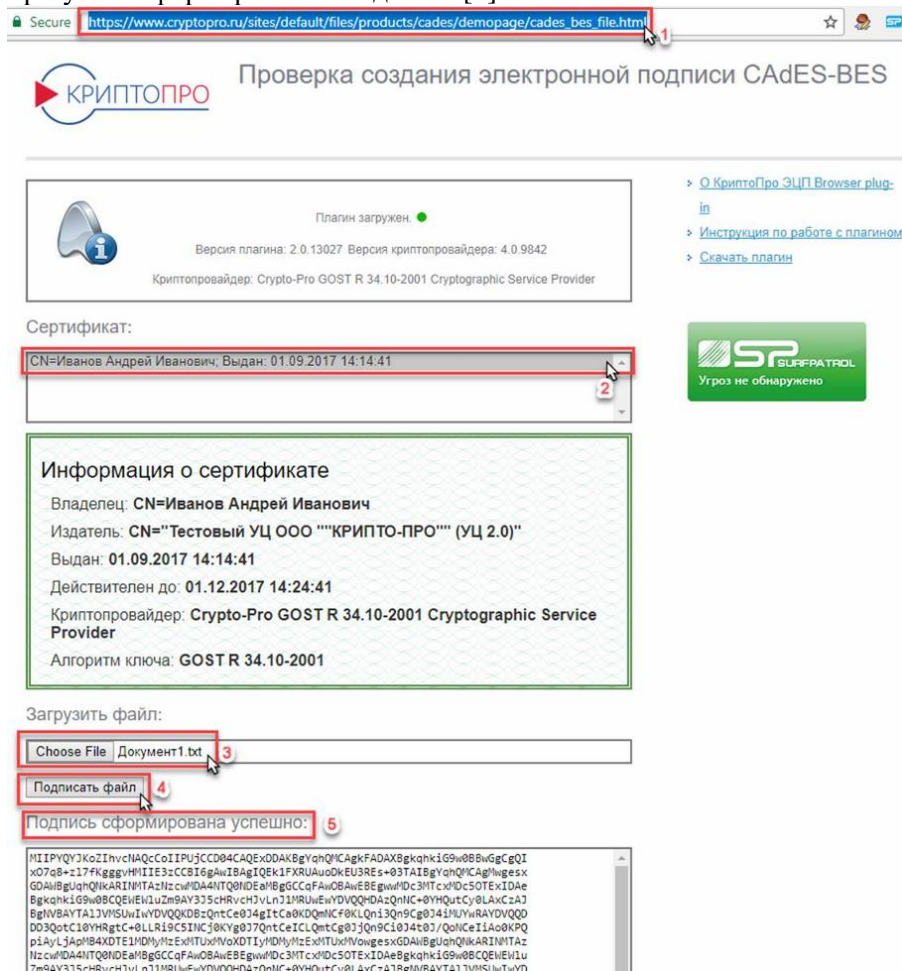


Рис. 8.12 — Проверка подписание документов на сайте CryptoPro

### 8.7 Сообщение: «Сертификат недоступен или не найден закрытый ключ/Ошибка при подписи сертификатов»

- проверить вставлен ли токен;
- [выполнить скрипт](#);
- истекла лицензия:

Для продления лицензии необходимо зайти в Пуск - Крипто-ПРО - КриптоПро CSP (Рис.8.13)

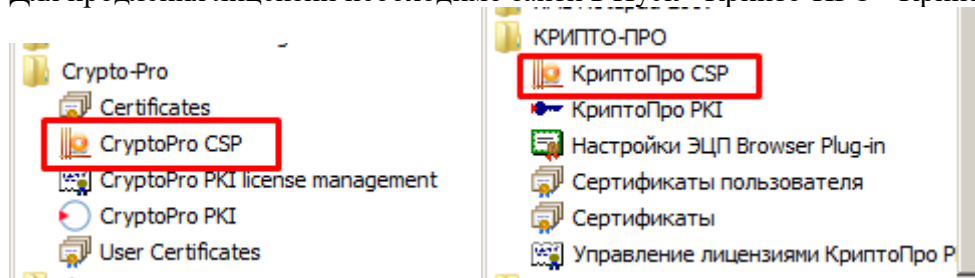


Рис. 8.13 —CryptoPro CSP



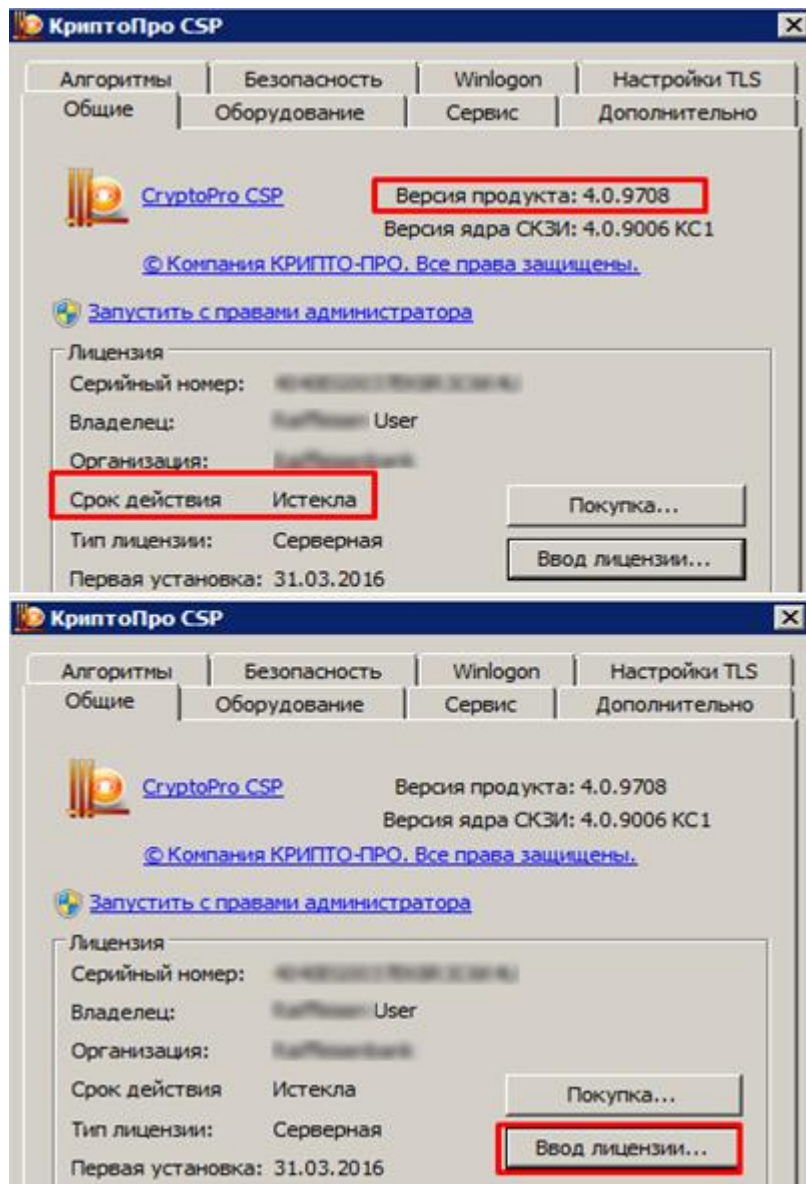


Рис. 8.15 —CryptoPro CSP. Срок действия – Истекла. Ввод лицензии

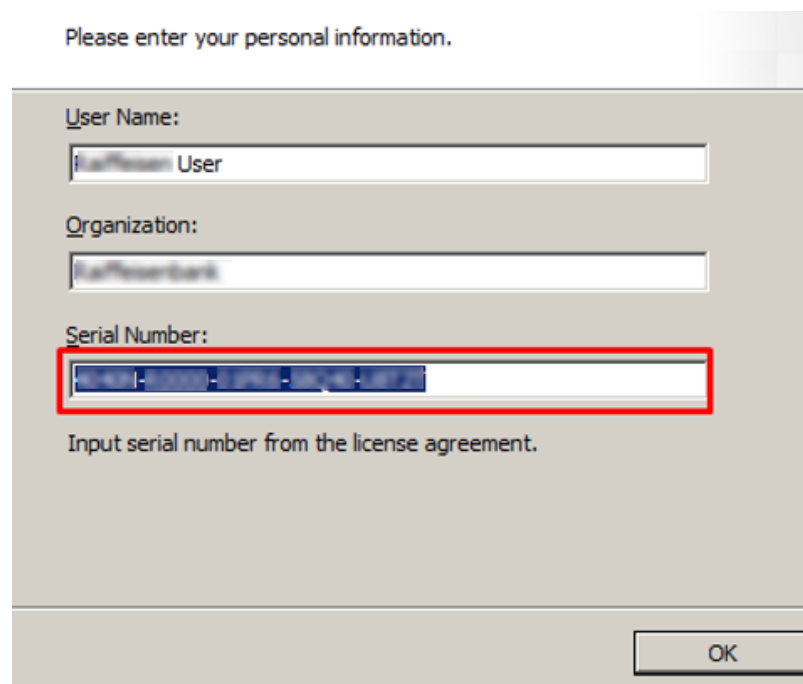


Рис. 8.16 —CryptoPro CSP. Ввод серийного номера

### 8.7 Ошибка «Данный сертификат не содержит все обязательные параметры».

Данная ошибка (Рис.8.17) отображается пользователю при регистрации на портале АИС НГС, если в сертификате не указаны все необходимые параметры.

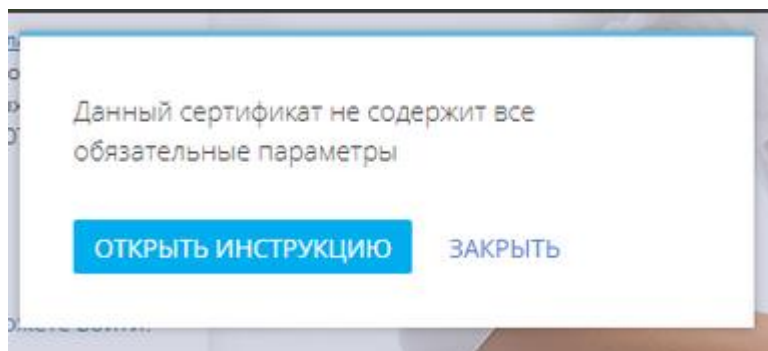


Рис. 8.17 — Ошибка: Данный сертификат не содержит все обязательные параметры

Для устранения ошибки, необходимо проверить наличие обязательных параметров сертификата УКЭП пользователя, которые перечислены в разделе №7 [«Требования к составу и содержанию обязательных параметров сертификата УКЭП»](#) данного документа.

В случае несоответствия требованиям сертификата УКЭП, необходимо обратиться в Удостоверяющий Центр, издавшего сертификат УКЭП и запросить корректные данные.