Инструкция по настройке АРМ пользователя для работы с ППО «СУФД-online»

Краткое описание настройки АРМ пользователя:

1.1. Установить СКЗИ «КриптоПро CSP» версии 4.0 или выше.

1.2. Установить корневые сертификаты и личный сертификат ключа проверки электронной подписи.

1.3. Скачать, установить и настроить браузер Chromium-Gost и «КриптоПро ЭЦП Browser plug-in».

Подробное описание настройки АРМ пользователя:

Все действия должны проводиться под учетной записью Windows с правами администратора.

1.1 Установка СКЗИ «КриптоПро CSP» версии 4.0

Запустите файл с именем «default_ru», записанный на оптический диск с дистрибутивом СКЗИ «КриптоПро» (рис. 1).

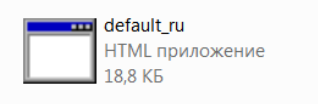


Рисунок 1

На экране появится окно с приглашением. Для установки СКЗИ «КриптоПРО» версии 4.0 выберете пункт меню, указанный на рисунке 2.

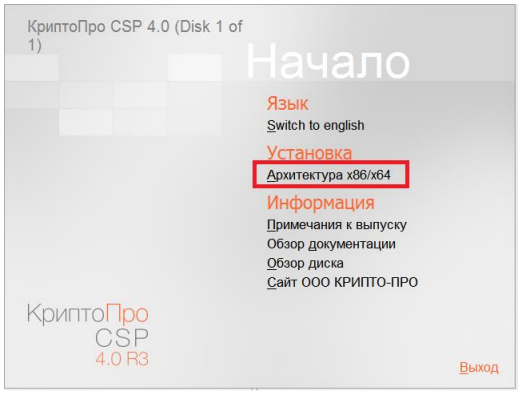


Рисунок 2

В появившемся окне выберете опцию «Установить» (рис. 3).

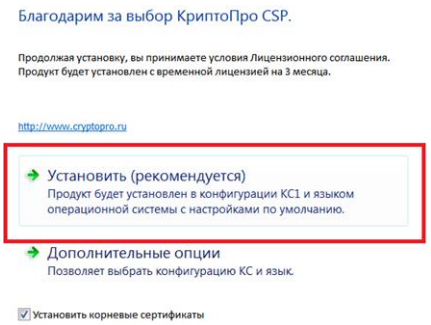


Рисунок 3

Начнется установка СКЗИ «КриптоПро» версии 4.0. По завершении программа установки выведет на экран соответствующее уведомление. После чего необходимо перезагрузить компьютер.

После перезагрузки компьютера необходимо зарегистрировать СКЗИ «КриптоПро». Для регистрации СКЗИ «КриптоПро» версии 4.0 требуется номер лицензии. Номера лицензий организации получают с помощью информационной системы «АОКЗ» (детальная информация размещена на оф. сайте penza.roskazna.ru в разделе ГИС/АОКЗ). Данный номер вводится в программу управления СКЗИ «КриптоПро». Для её запуска воспользуйтесь ярлыком, размещенным в меню «Пуск» Windows: ПУСК – Все программы – КРИПТО-ПРО – КриптоПро CSP. На вкладке «Общие» программы управления размещена кнопка «Ввод лицензии» (рис. 4).

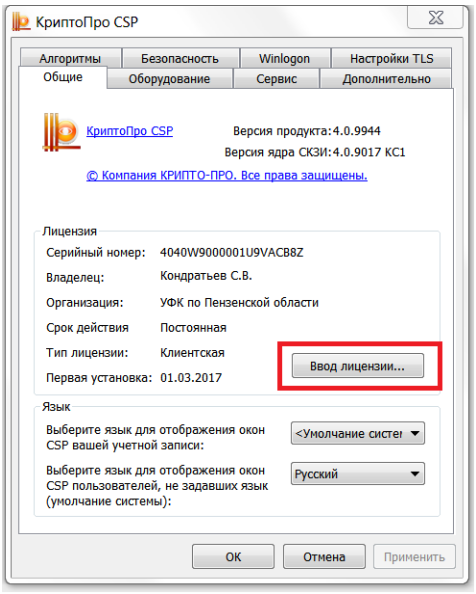


Рисунок 4

По нажатию на данную кнопку выводится окно, изображенное на рисунке 5. Заполните соответствующие поля и нажмите кнопку «ОК».

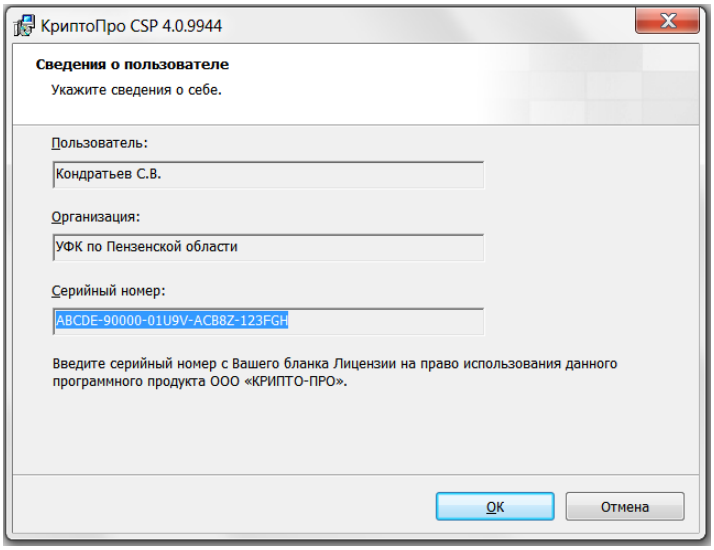


Рисунок 5

Регистрация продукта завершена.

1.2 Установка корневых сертификатов и личного сертификата ключа проверки электронной подписи

1. Необходимо скачать корневые сертификаты по следующим ссылкам:
сертификат Минцифры России (ГУЦ):
https://roskazna.gov.ru/upload/iblock/f5e/Kornevoy-sertifikat-GUTS-2022.CER
сертификаты УЦ ФК:
https://roskazna.gov.ru/upload/iblock/1af/Kaznacheystvo-Rossii.CER
https://www.roskazna.gov.ru/upload/iblock/c8c/UTS-FK_2021.CER
На предложение сохранить файл сертификата выберете локальную директорию АРМ пользователя, в которую необходимо сохранить файл.

2. После скачивания сертификатов их необходимо установить в хранилище сертификатов Windows. Для установки сертификата ГУЦ в хранилище сертификатов компьютера средствами Windows вызовете контекстное меню нажатием правой кнопкой мыши по файлу с сертификатом (рис. 6).

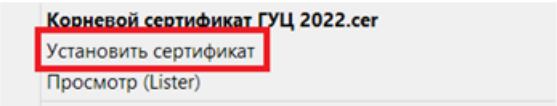


Рисунок 6

Запустится мастер импорта сертификатов (рис. 7).

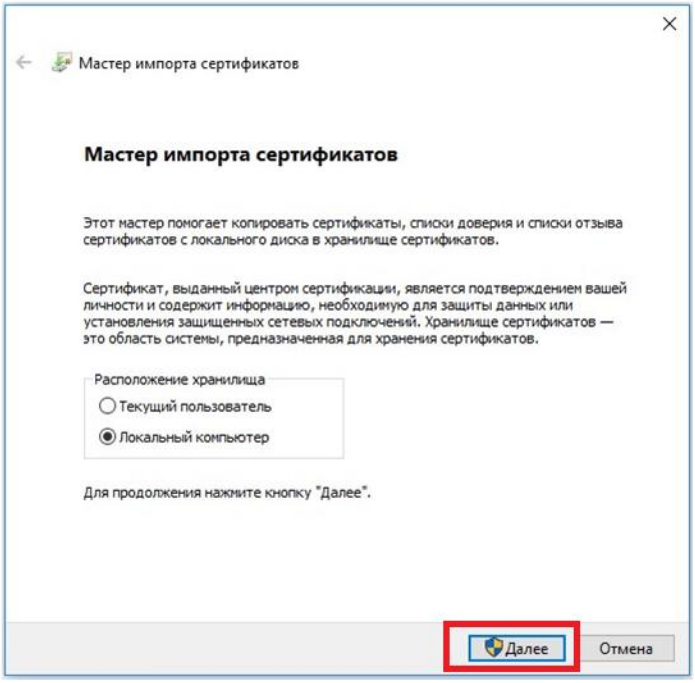


Рисунок 7

3. Выберете хранилище «Локальный компьютер» и нажмите кнопку «Далее». В следующем окне выберете опцию «Поместить сертификаты в следующее хранилище» и нажмите кнопку «Обзор…» (рис. 8).

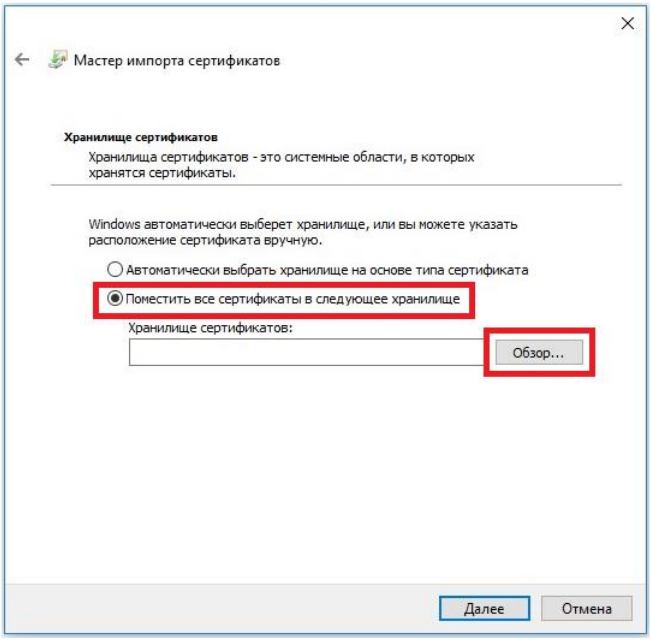


Рисунок 8

4. Выберете хранилище «Доверенные корневые центры сертификации», нажмите кнопку «ОК» (рис. 9).

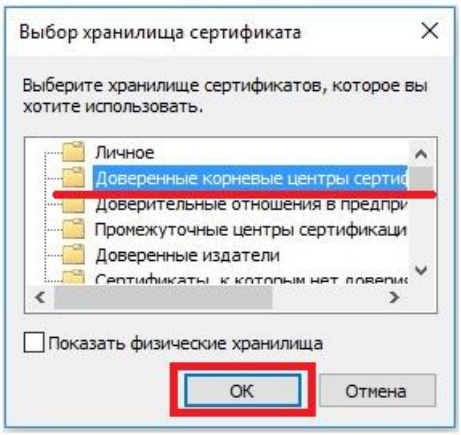


Рисунок 9

5. Откроется окно завершения работы мастера импорта сертификатов (рис. 10)

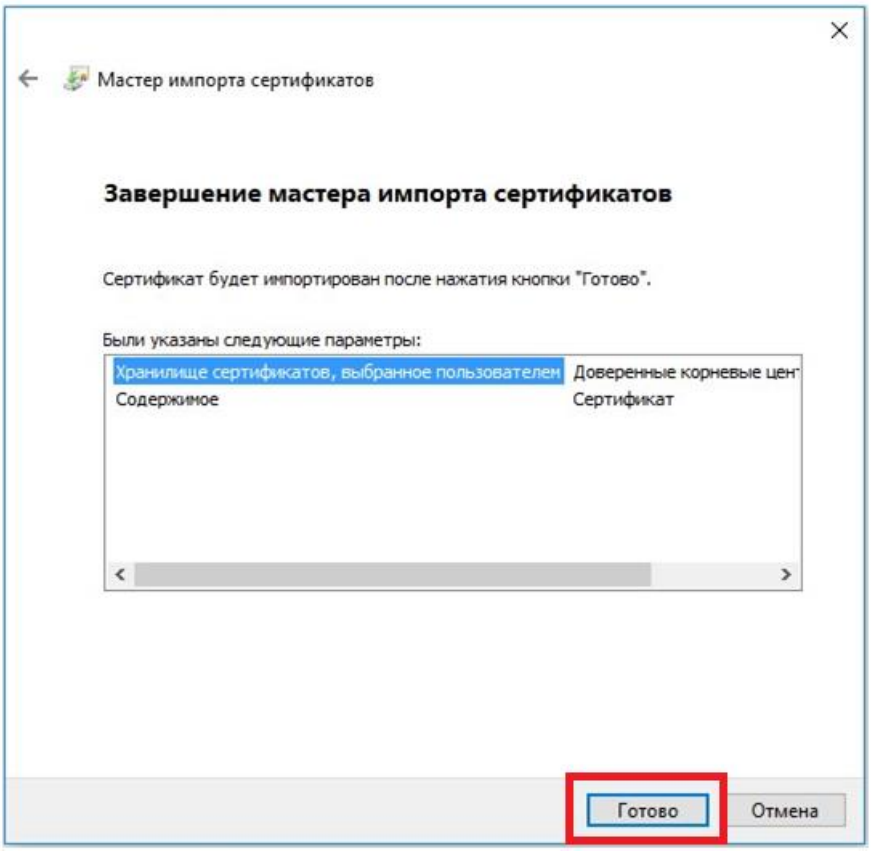


Рисунок 10

После нажатия кнопки «Готово» появится сообщение, что импорт успешно выполнен (Рис. 11).

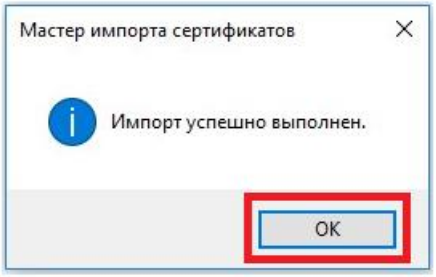


Рисунок 11

Установка корневого сертификата (ГУЦ) завершена.

Для установки сертификатов УЦ ФК для файлов данных сертификатов необходимо повторить аналогичные действия, описанные в пунктах 2 и 3.

В окне «Выбор хранилища сертификата» (рис. 12) выберете хранилище «Промежуточные центры сертификации» и нажмите кнопку «ОК».

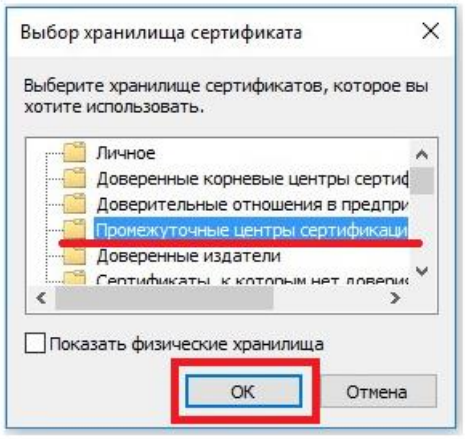


Рисунок 12

После чего повторите действия аналогично описанным в пункте 5. Установка сертификатов УЦ ФК завершена.

Для установки личного сертификата ключа проверки электронной подписи запустите СКЗИ «КриптоПРО» посредством ярлыка (размещен в меню ПУСК – Все программы – КРИПТО-ПРО) (рис. 13)

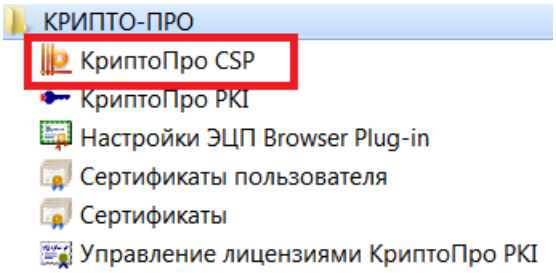


Рисунок 13

1. В появившемся окне выберете вкладку «Сервис» (рис. 14)

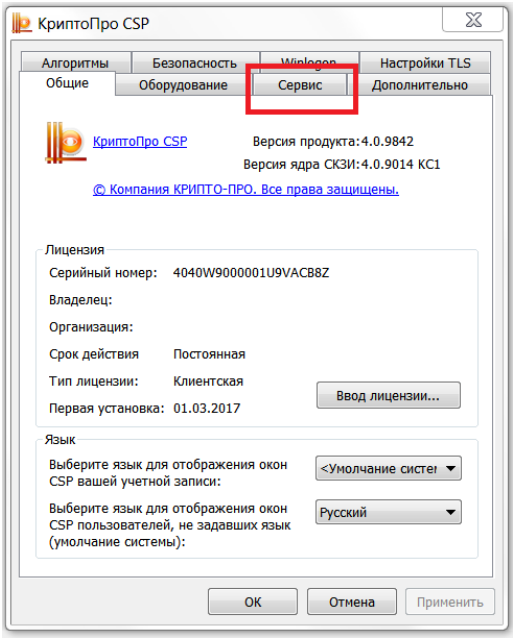


Рисунок 14

2. Затем нажмите кнопку «Установить личный сертификат…» (рис. 15)

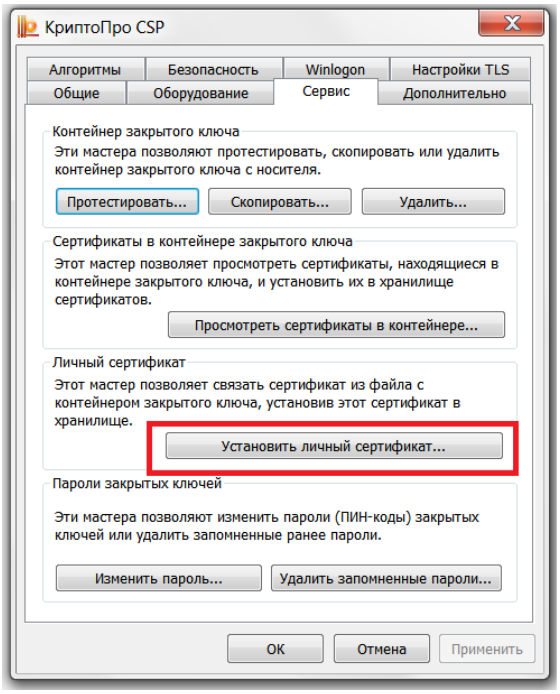


Рисунок 15

3. Запустится мастер установки личного сертификата. С помощью кнопки «Обзор» выберите файл сертификата и нажать на кнопку «Открыть» (рис. 16).

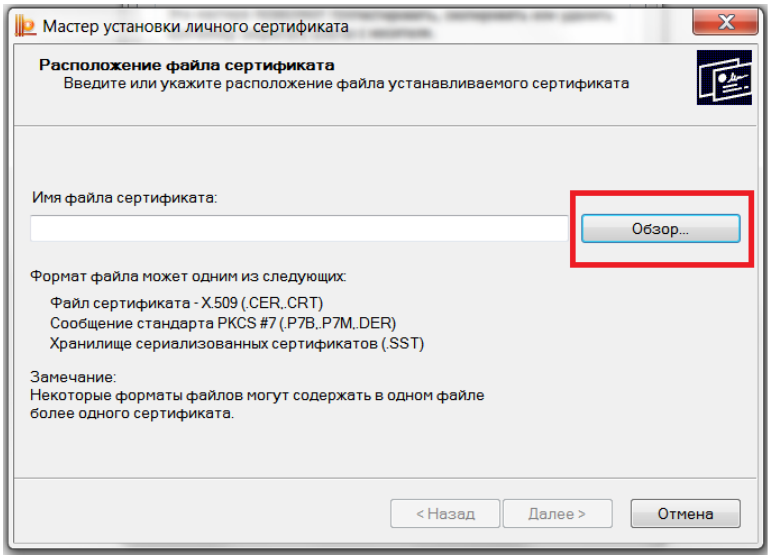


Рисунок 16

Для продолжения установки сертификата нажмите кнопку «Далее».

4. Мастер установки выведет информацию о выбранном сертификате. После ознакомления нажмите кнопку «Далее».

5. Мастер установки предложит выбрать контейнер закрытого ключа, соответствующий выбранному сертификату. Для этого вставьте ключевой носитель

с контейнером закрытого ключа и выберете опцию «Найти контейнер автоматически» (рис. 17).

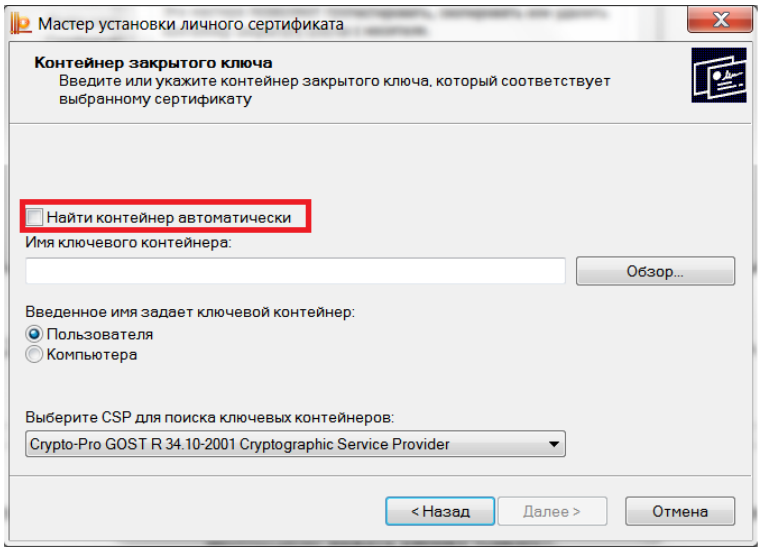


Рисунок 17

В случае, если предоставлен ключевой контейнер, соответствующий устанавливаемому сертификату, мастер автоматически выберет его. Для продолжения установки нажмите кнопку «Далее».

6. На следующем этапе установки необходимо деактивировать опцию «Установить сертификат (цепочку сертификатов) в контейнер» и нажать кнопку «Далее» (рис. 18)

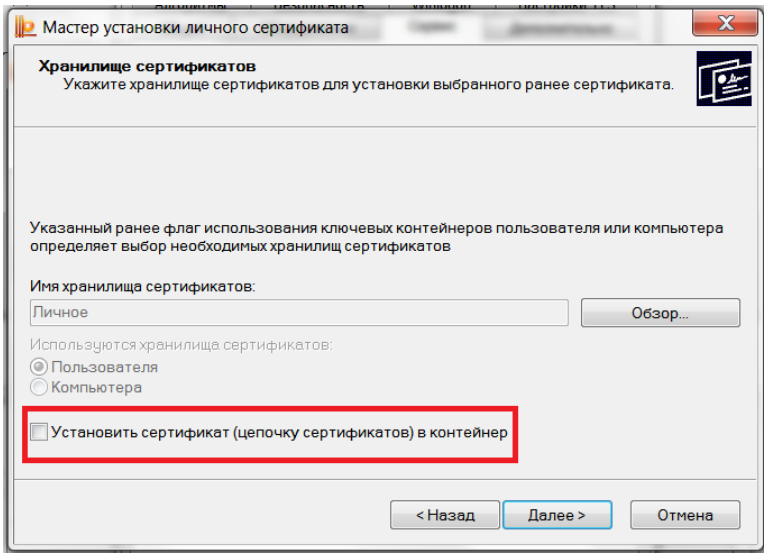


Рисунок 18

8. В завершении мастер установки выведет итоговую таблицу с параметрами установки. Для завершения установки нажмите кнопку «Готово».

Установка сертификата ключа проверки электронной подписи завершена.

1.3 Скачивание, установка и настройка браузера Chromium-Gost и «КриптоПро ЭЦП Browser plug-in»

Для скачивания Chromium-Gost необходимо перейти по ссылке https://github.com/deemru/chromium-gost/releases/latest и в разделе «Assets» выбрать файл в названии которого фигурируют «…windows-amd64-installer.exe» (рис. 19).

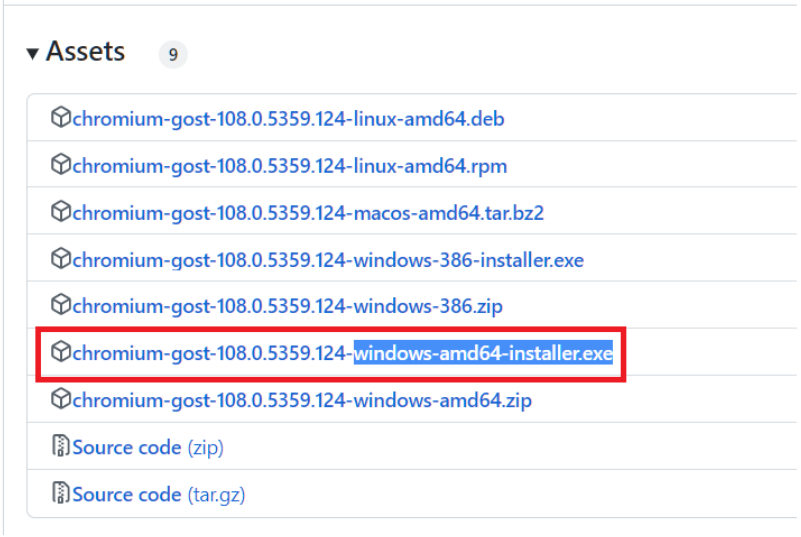


Рисунок 19

Дождитесь окончания загрузки и запустите скачанный файл. Дождитесь окончания установки. По окончании установки на рабочем столе Windows появится ярлык браузера Chromium-Gost (рис. 20)



Рисунок 20

Скачайте «КриптоПро ЭЦП Browser plug-in» по ссылке: https://www.cryptopro.ru/products/cades/plugin/get_2_0. Запустите установочный файл и дождитесь окончания установки.

Запустите Chromium-Gost, использую ярлык на рабочем столе. Затем нажмите на значок с тремя желтыми точками в правом верхнем углу и выберете «Добавлено новое расширение (CryptoPro Extension for CAdeS Browser Plug-in) (рис. 21)

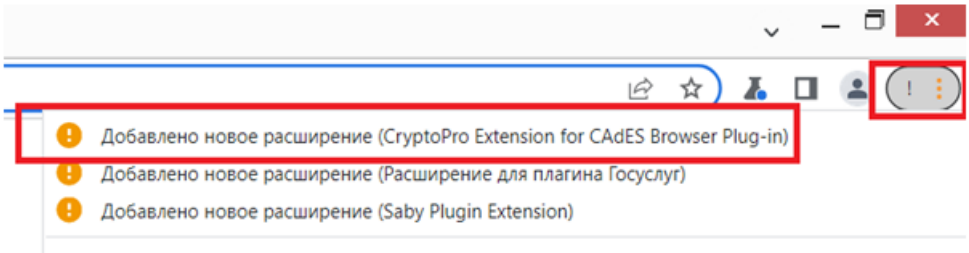


Рисунок 21

В появившемся окне нажмите на кнопку «Включить расширение» (рис. 22).

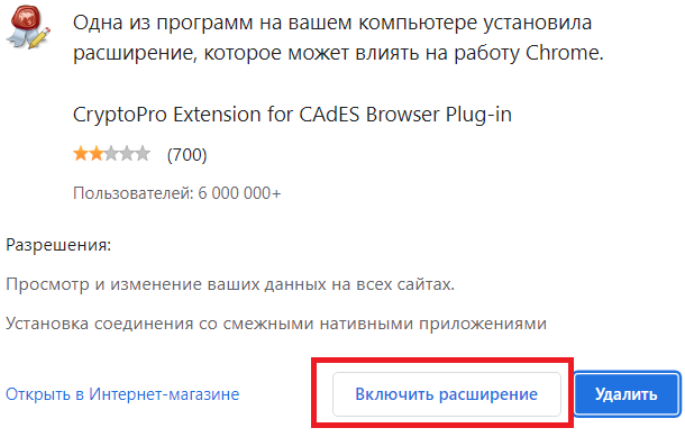


Рисунок 22

Проведите окончательную диагностику работы браузера с плагином, перейдя по ссылке: https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html

Все 4 индикатора в итоге должны быть зеленого цвета (рис. 23).

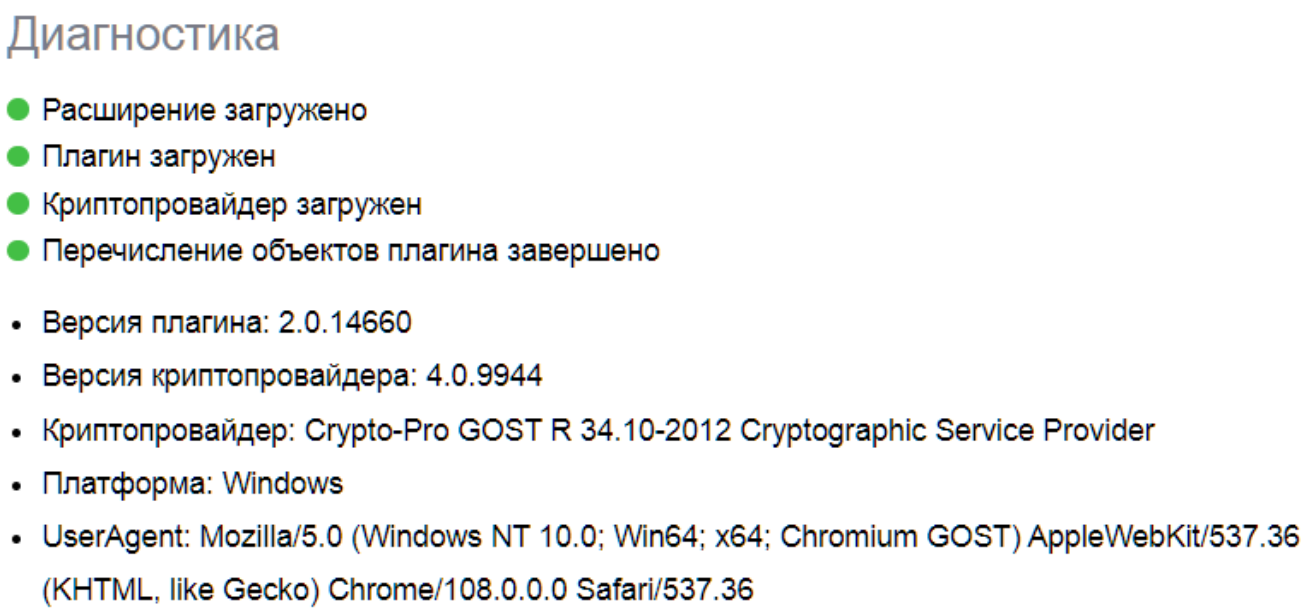


Рисунок 23

Настройка Chromium-Gost закончена.

Вход в СУФД-Портал

После выполнения вышеуказанных мероприятий вход в СУФД-online УФК по Пензенской области осуществляется в браузере Chromium-Gost по ссылке:

https://ufk55.sufd.budget.gov.ru

При вводе данного адреса в адресную строку браузера должно открыться окно с выбором сертификата. Укажите необходимый сертификат из списка и введите пароль от контейнера закрытых ключей. Далее откроется стартовая страница СУФД-online.

Если на рабочей станции в СУФД-online работают пользователи под разными учетными записями (руководитель, главный бухгалтер), то для смены учетной записи необходимо закрыть браузер и зайти заново. Для этого, выходим из СУФД-Портала (рис. 24).

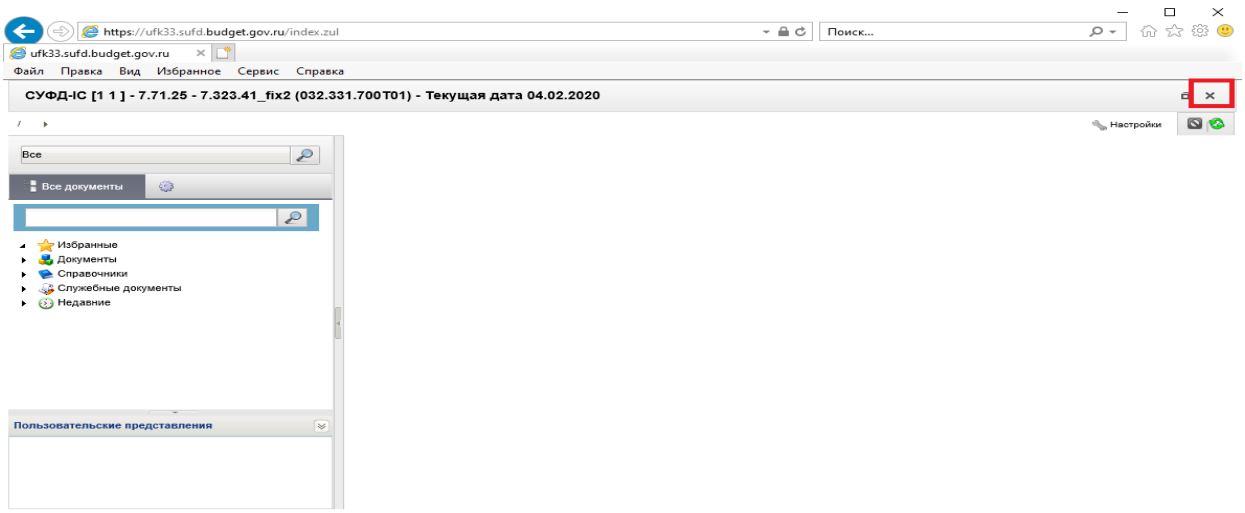


Рисунок 24

После этого появится следующее окно (рис. 25)

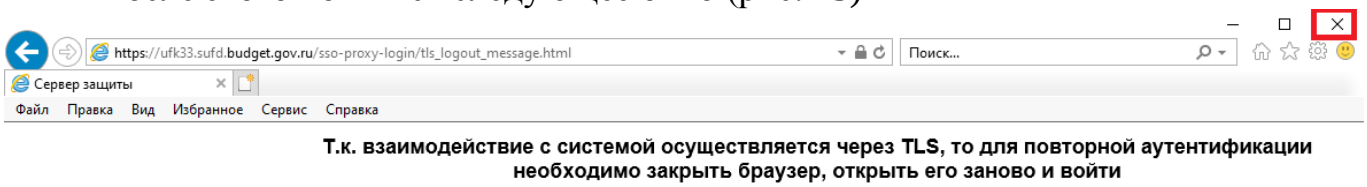


Рисунок 25

Необходимо закрыть Chromium-Gost и повторить процедуру входа в СУФД-online под другим пользователем.

В случае если используемый сертификат для входа в СУФД-online не прикреплен к учетной записи пользователя СУФД-online на экране отобразится следующее окно (рис. 26).

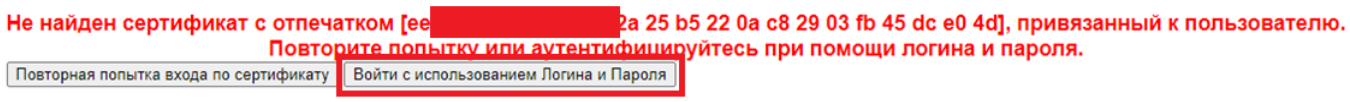


Рисунок 26

Нажмите кнопку «Войти с использованием Логина и Пароля» и в следующем окне введите логин/пароль своей учетной записи (рис. 27).

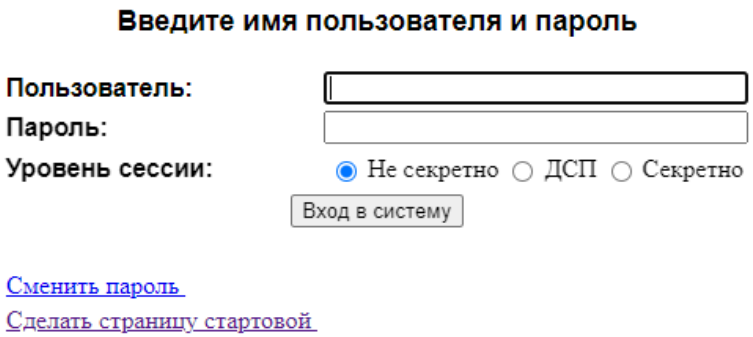


Рисунок 27

Данный вариант авторизации используется для пользователей без права подписи электронных документов. При этом у данных пользователей должен иметься действующий сертификат ключа проверки электронной подписи, выданный Удостоверяющим центром Федерального казначейства.