Межрегиональное операционное УФК

Инструкция по настройке рабочего места для работы в ППО СУФД с использованием TLS-доступа

Оглавление

I. Общие сведения 2

1. Программные и аппаратные требования к рабочему месту пользователя СУФД Портала 2

II. Настройка автоматизированного рабочего места клиента для работы в СУФД Портале с использованием СКЗИ «КриптоПро CSP» (рекомендуется) 5

2. Установка сертификатов 5

Установка корневых и промежуточных сертификатов 5

Установка сертификатов пользователя 7

3. Установка КриптоПро CSP browser plug-in 10

4. Настройка браузера для работы в СУФД Портале 11

Настройка Internet Explorer 11 11

Настройка Яндекс Браузера 14

Настройка Chromium-Gost 15

III. Настройка автоматизированного рабочего места клиента для работы в СУФД Портале через «СКЗИ «Континент TLS-клиент» (не обязательно) 16

1. Настройка «Континент TLS VPN Клиент» 17

IV. Настройка доступа в СУФД Портал 23

I. Общие сведения

Для создания защищенного соединения посредством сетевого протокола TLS организации-клиенту достаточно использовать одно из следующих сертифицированных средств криптографической защиты информации (далее – СКЗИ):

- СКЗИ «КриптоПро CSP» версии 4.0 (рекомендуется);
- СКЗИ «Континент TLS-клиент» версии 2.

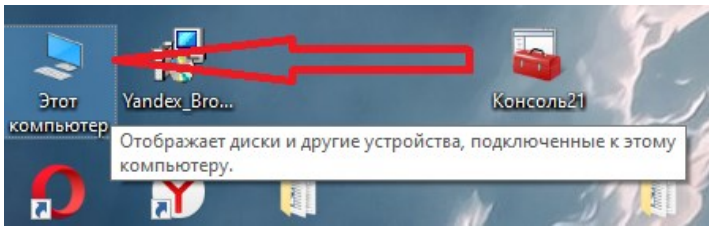
1. Программные и аппаратные требования к рабочему месту пользователя СУФД Портала

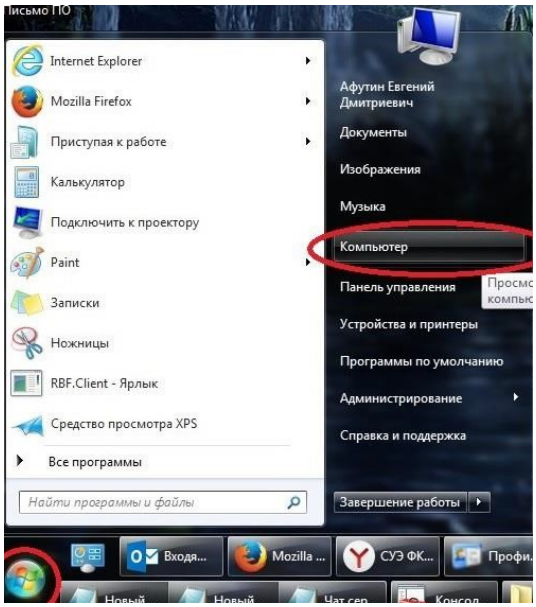
Общее ППО клиентского уровня должно удовлетворять следующим требованиям:

- Операционная система не ниже Microsoft Windows 7;
- СКЗИ «Крипто Про CSP» версия 4.,0;
- КриптоПро CSP browser plug-in версия 2 и выше;
- Доступ к сети Интернет со скоростью не менее 256 Кбит/сек;
- Актуальные версии браузеров, поддерживающие работу Крипто Про CSP browser plug-in:
  - Internet Explorer 11;
  - Яндекс Браузер;
  - Chromium-Gost (для Windows 7 / 8 / 8.1 версия НЕ ВЫШЕ 109).

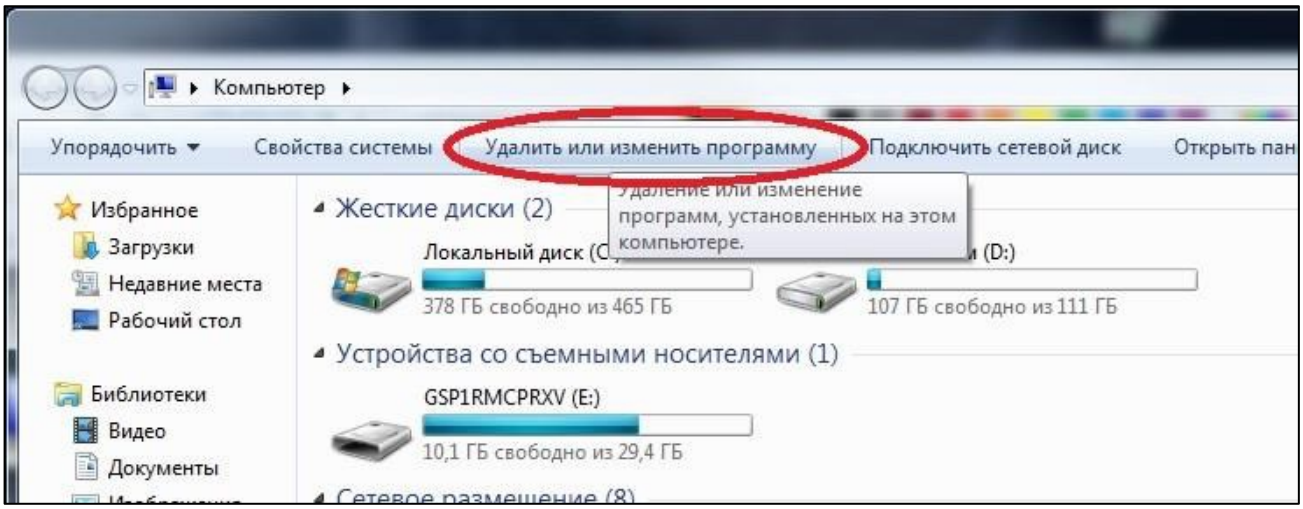
Проверить установлено ли СКЗИ «Крипто Про CSP» версия 4, либо СКЗИ «Континент TLS VPN клиент» версии 2.0 можно следующим образом:

Открыть на рабочем столе ярлык «Компьютер» или в меню «Пуск» - «Компьютер»

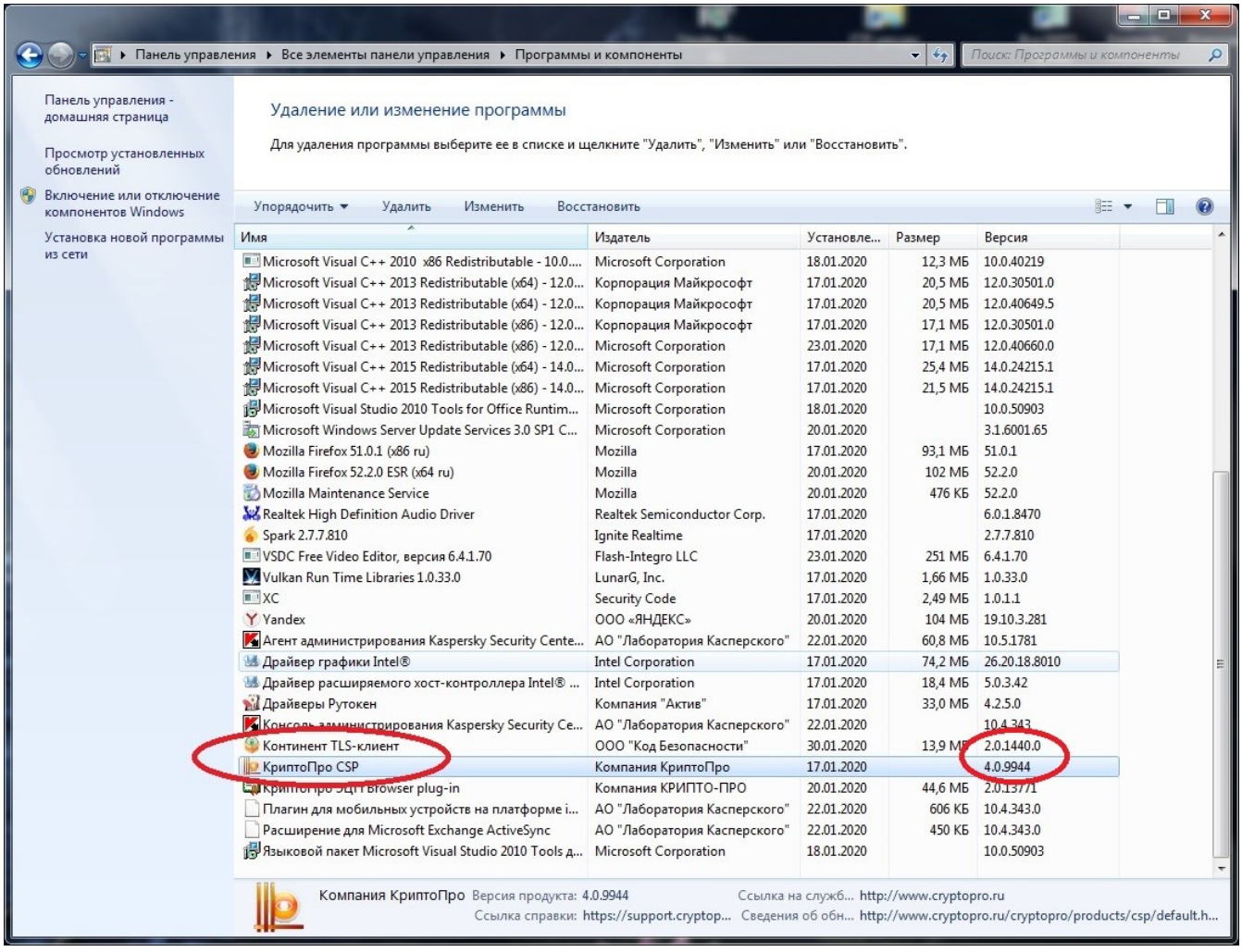




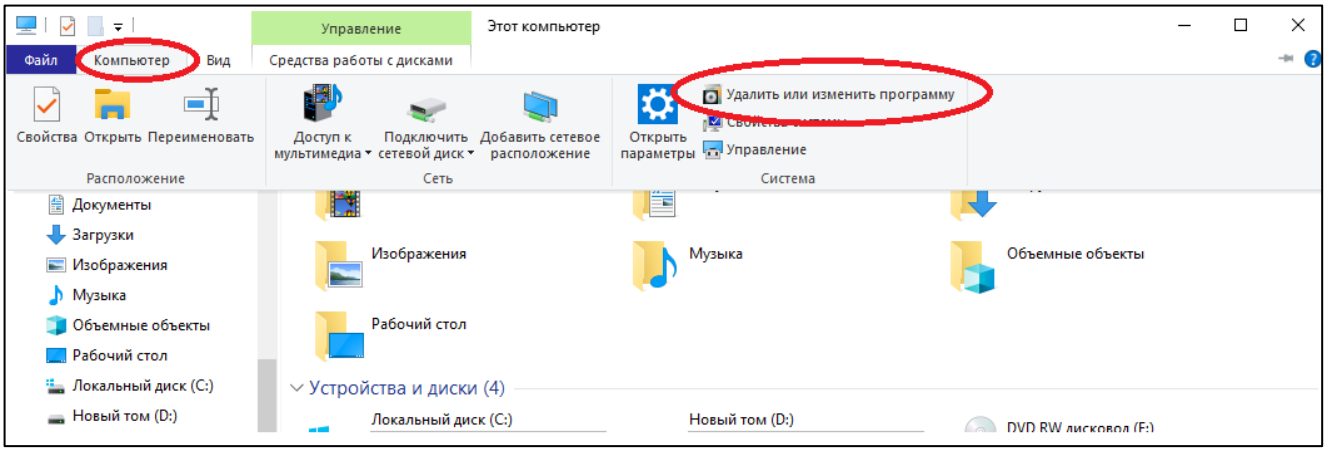
Далее, если у вас **Windows 7**, то открываем вкладку «Компьютер» - «Удалить или изменить программу».



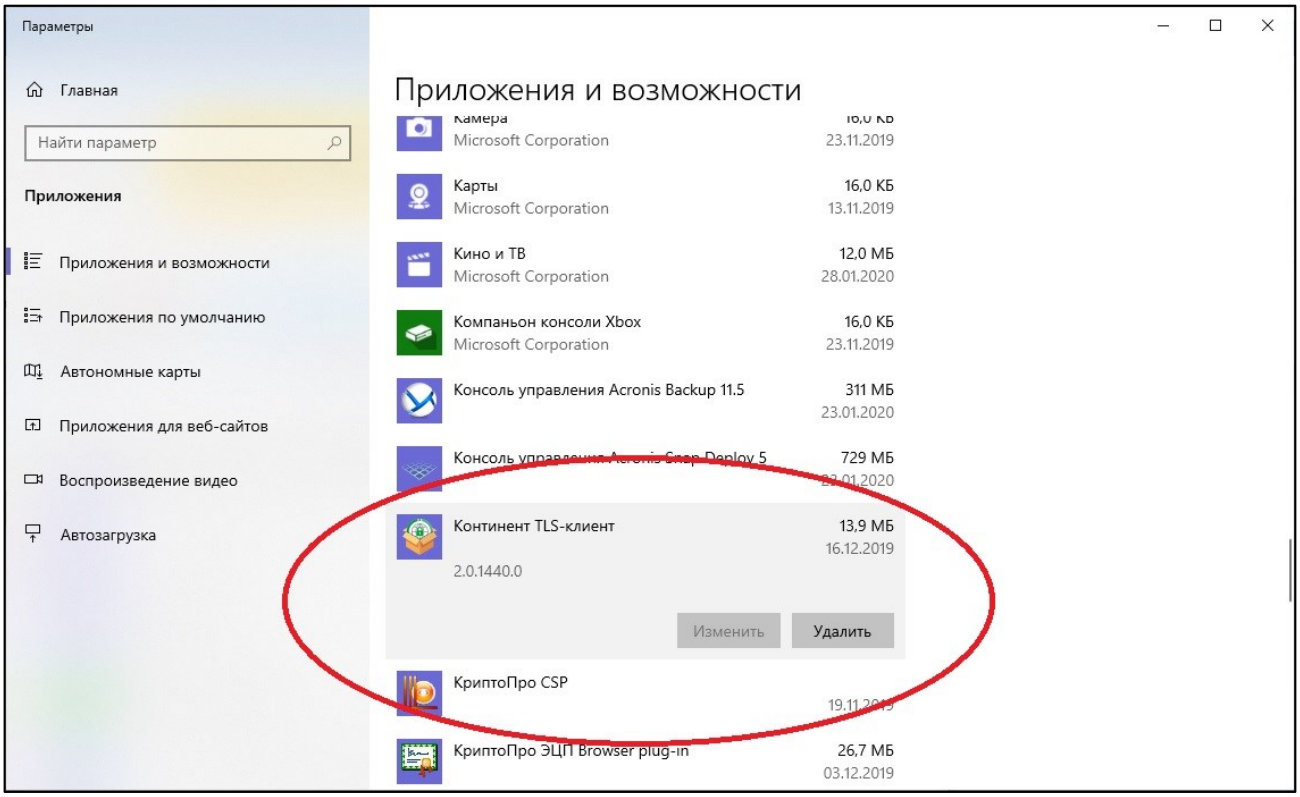
В открывшемся окне проверить наличие программ в списке



Если у вас **Windows 10**, то открываем вкладку «Компьютер» - «Удалить или изменить программу»



В открывшемся окне проверить наличие программ в списке



Если СКЗИ «Крипто Про CSP» не установлено, то его необходимо установить. Дистрибутив СКЗИ «Крипто Про CSP» получается в Межрегиональном операционном УФК (клиентами Межрегионального операционного УФК, находящимися в субъектах Российской Федерации – в соответствующем Управлении Федерального казначейства по субъекту Российской Федерации).

II. Настройка автоматизированного рабочего места клиента для работы в СУФД Портале с использованием СКЗИ «КриптоПро CSP» (рекомендуется)

2. Установка сертификатов

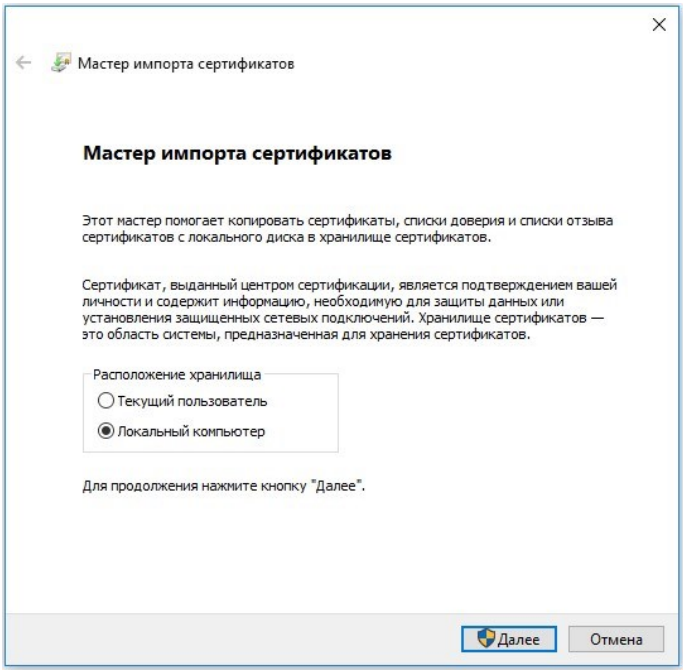
Установка корневых и промежуточных сертификатов

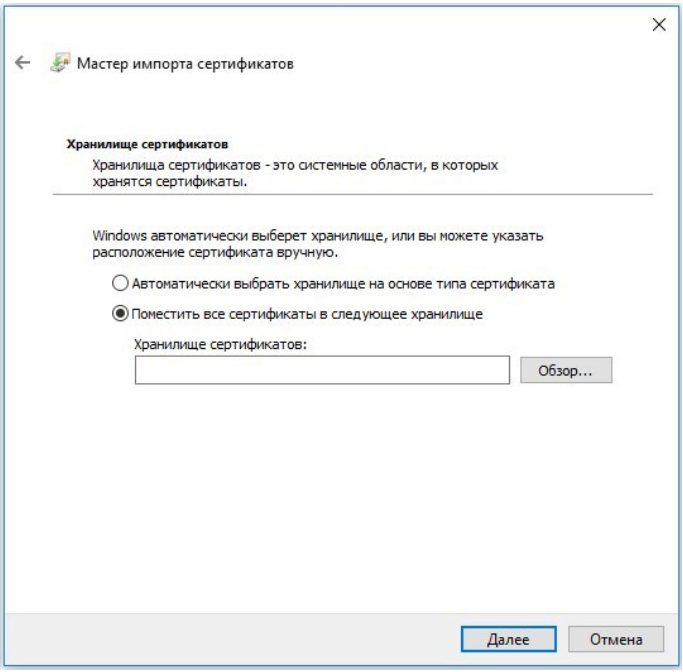
Корневые сертификаты ГУЦ Минцифры России (Минкомсязи) и промежуточные сертификаты УЦ Федерального казначейства размещены на сайте Межрегионального операционного УФК в сети Интернет (moufk.roskazna.gov.ru) в разделе ГИС\Удостоверяющий центр\Корневые сертификаты и списки аннулированных сертификатов.

Их необходимо скачать на рабочее место.

Для установки корневых и промежуточных сертификатов в хранилище сертификатов компьютера средствами операционной системы семейства Windows необходимо:

1. Нажать правой кнопкой мыши на файл сертификата, через контекстное меню выбрать пункт меню «Установить сертификат».
2. На экране отобразится мастер импорта сертификатов. Выбрать хранилище «Локальный компьютер» и нажать кнопку «Далее». В окне «Хранилище сертификата» выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище».

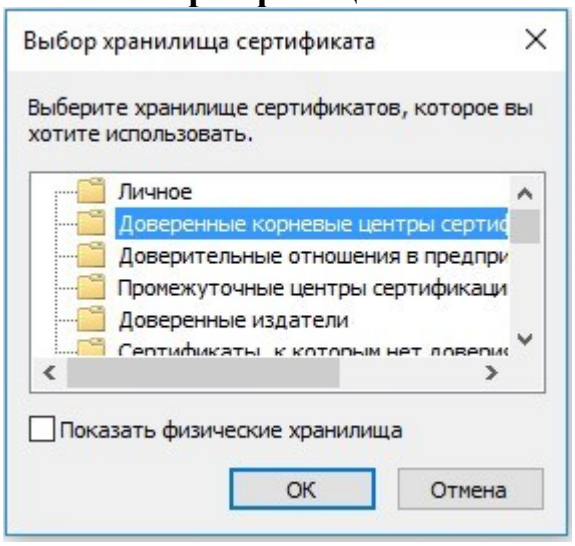




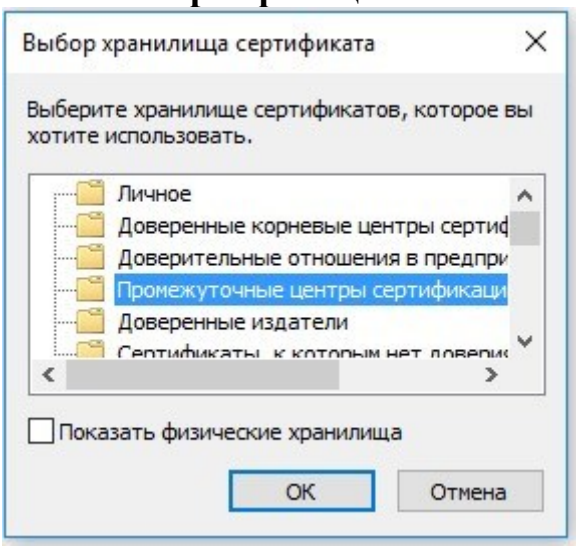
Примечание. В случае если на отсутствует возможность выбора хранилища Локального компьютера, следует обратиться к Вашему системному администратору для выполнения операции с правами локального администратора АРМ.

3. Выбрать хранилище:

Для корневых сертификатов ГУЦ Минцифры (Минкомсвязи) выбирается **«Доверенные корневые центры сертификации»**

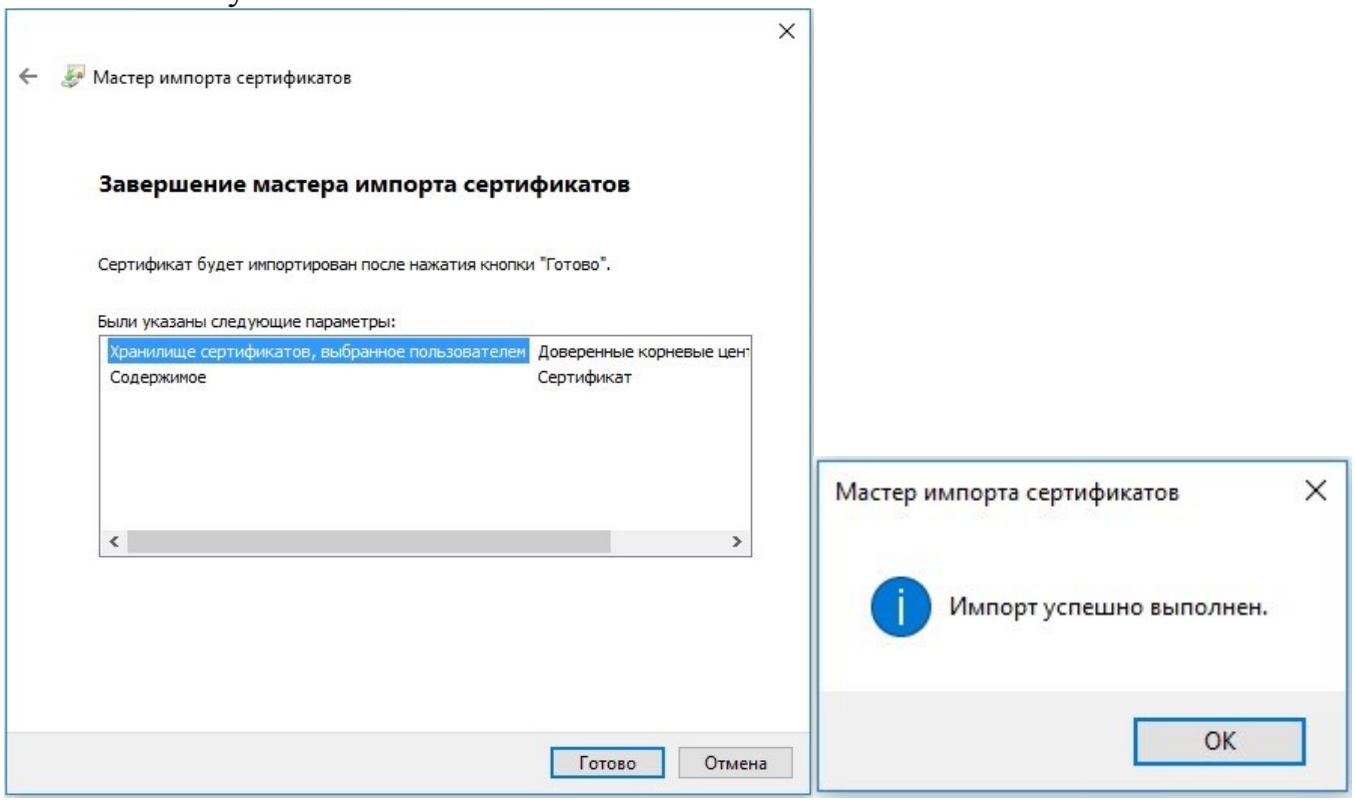


Для промежуточных сертификатов УЦ Федерального казначейства выбирается **«Промежуточные центры сертификации»**



Нажать кнопку «ОК».

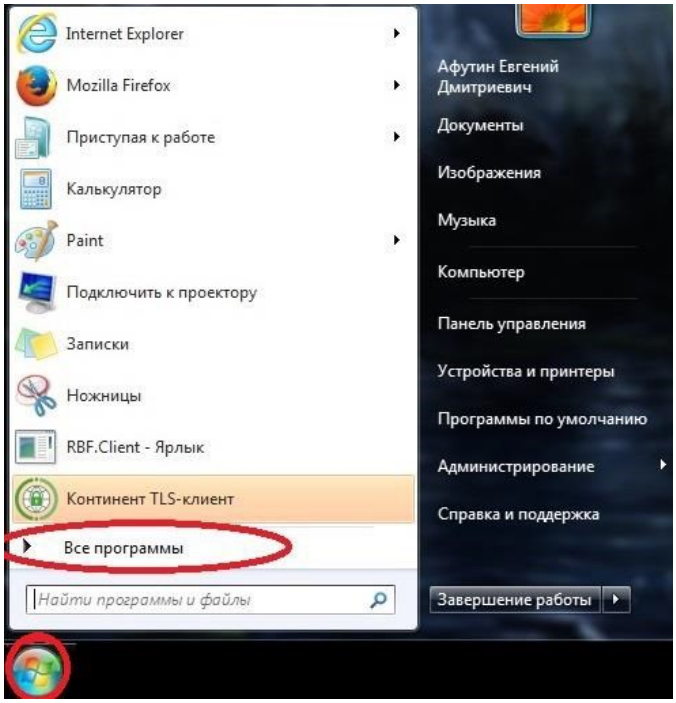
4. Откроется окно завершения работы мастера импорта сертификатов. Нажать кнопку «Готово». Появится сообщение, что импорт успешно выполнен. Нажать кнопку «ОК».

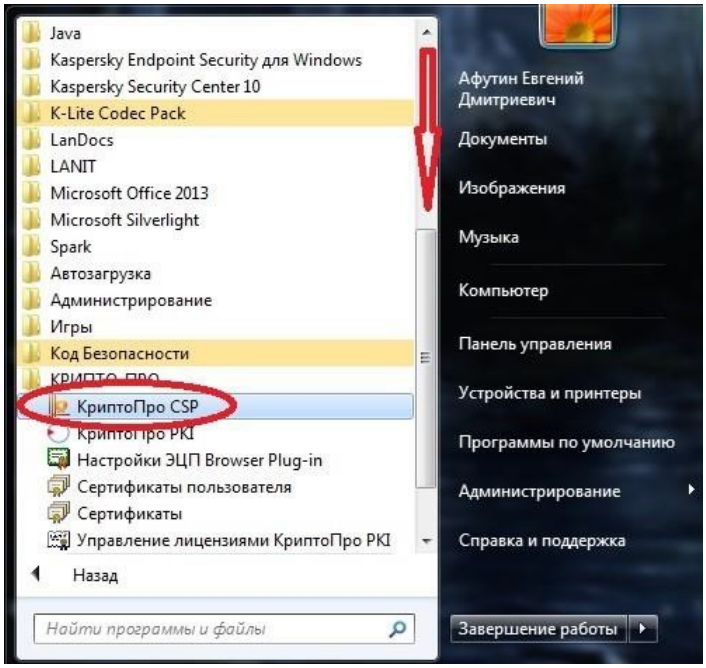


5. Повторить указанные действия для каждого корневого и промежуточного сертификата.

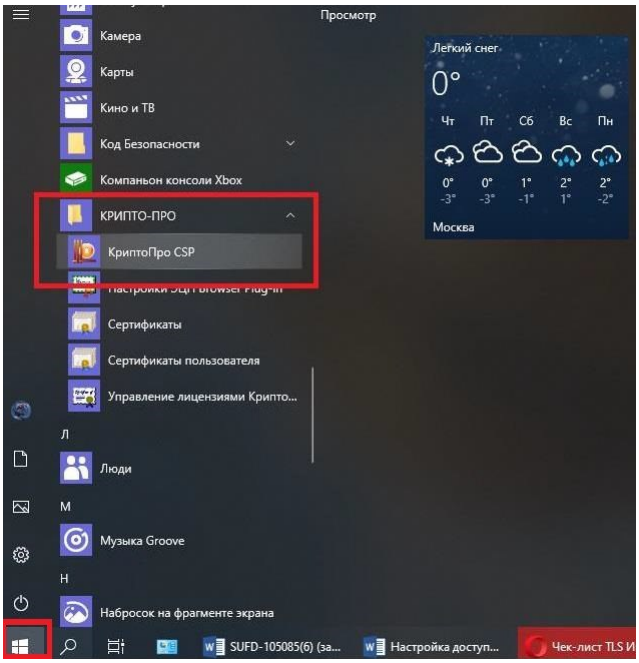
Установка сертификатов пользователя

Если у вас **Windows 7**, то открываем меню «Пуск» - «Все программы» «КРИПТО-ПРО» - «КриптоПро CSP»

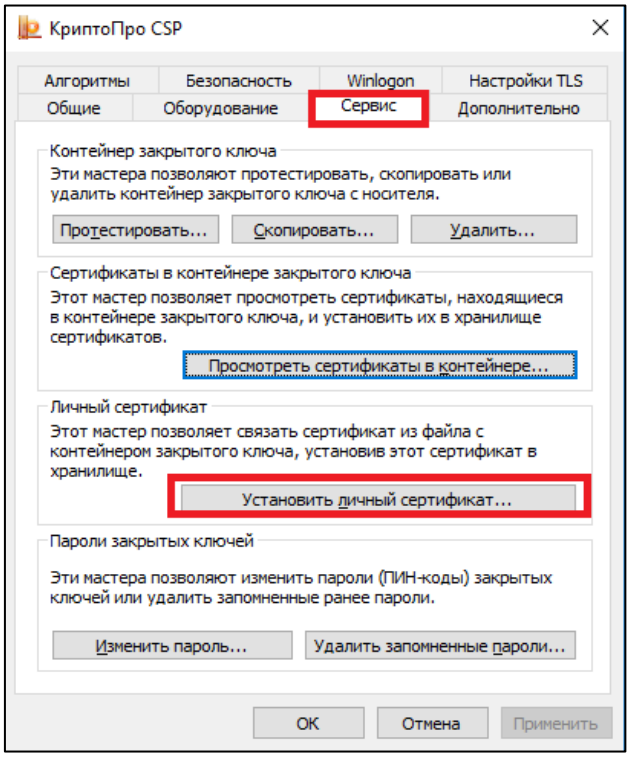


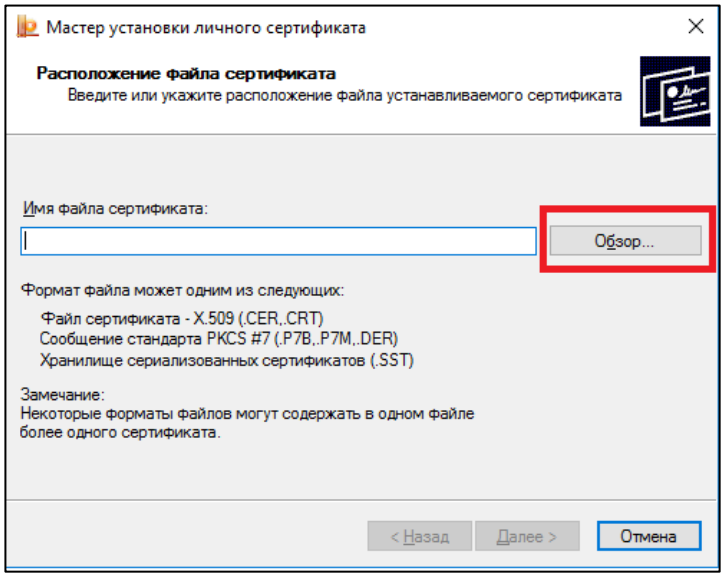


Для **Windows 10** внизу списка выбираем «КРИПТО-ПРО» - «КриптоПро CSP»

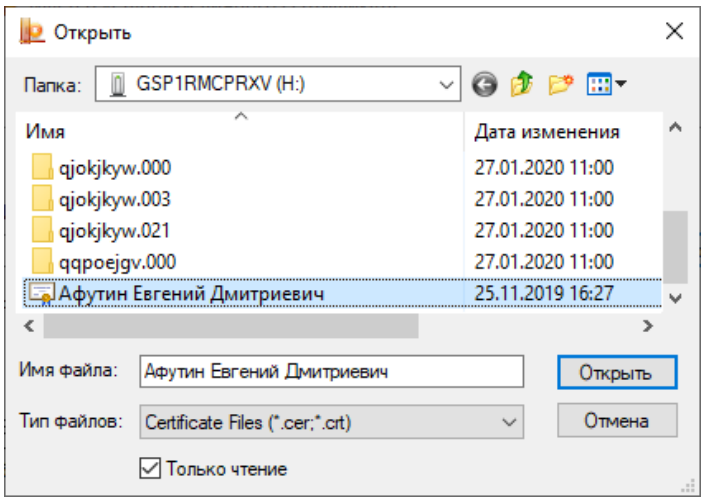


Далее необходимо перейти во вкладку «Сервис», нажать на кнопку «Установить личный сертификат». В появившемся меню нажать на кнопку «Обзор…».



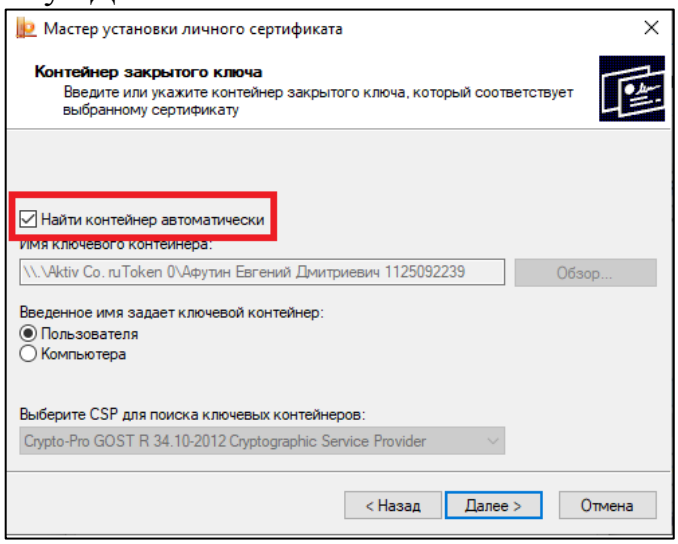


Затем выбрать необходимый сертификат пользователя (это личный сертификат, он находится непосредственно у вас на съёмном носителе). Нажать кнопку «Открыть»

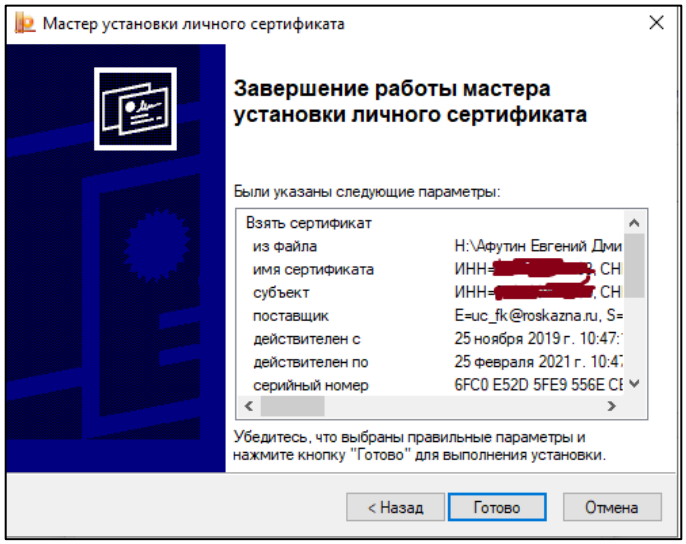


Дважды нажать кнопку «Далее».

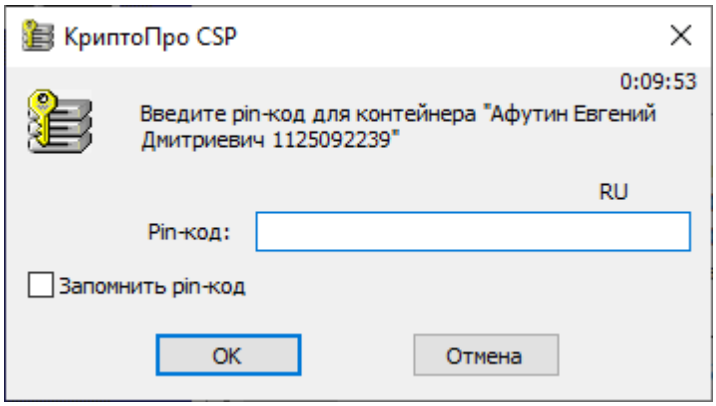
Откроется окно выбора контейнера закрытого ключа, отметить чекбокс «Найти контейнер автоматически». Контейнер должен находиться на съемном носителе. Нажать кнопку «Далее».



Отобразится окно завершения установки. Нажать кнопку «Готово».

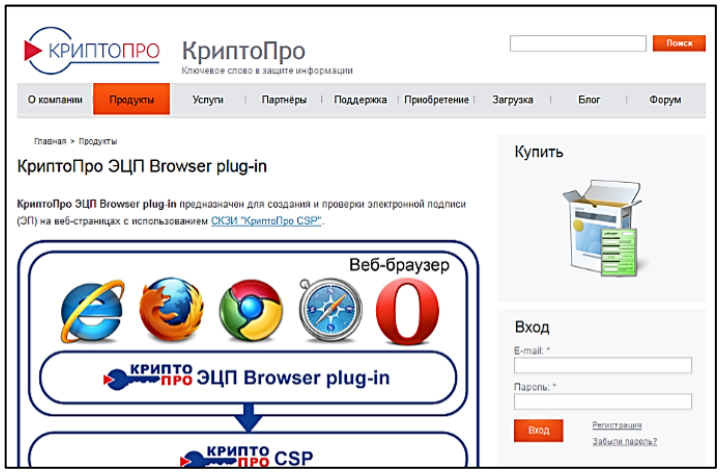


Если появиться окно с вводом пароля, то необходимо указать пароль для закрытого ключа в контейнере и нажать кнопку «ОК»

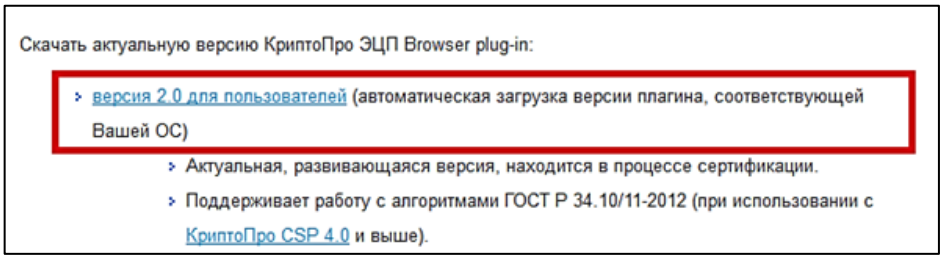


3. Установка КриптоПро CSP browser plug-in

КриптоПро browser plug-in можно скачать по ссылке в сети Интернет https://www.cryptopro.ru/products/cades/plugin. Откроется официальная страница сайта КриптоПро.

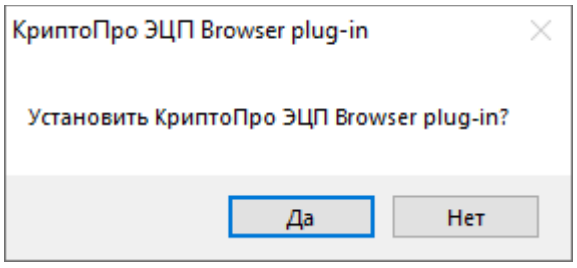


На данной странице необходимо найти строку

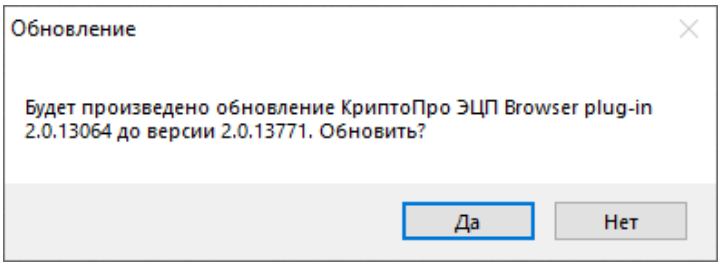


и скачать актуальную версию КриптоПро ЭЦП Browser plug-in.

После скачивания запустите установочный файл «cadesplugin», в появившемся окне нажать кнопку «Да»

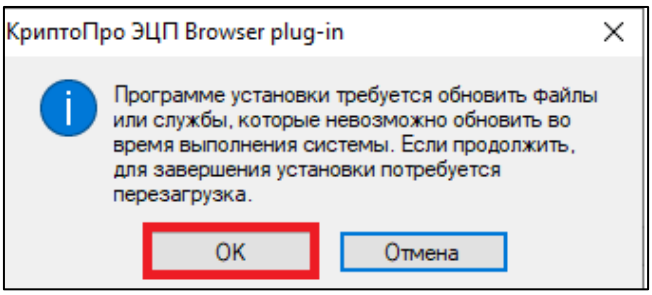


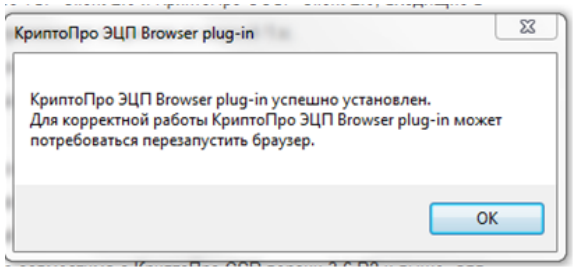
Если появилось окно,.



то необходимо установить новую версию

В процессе установки может появиться сообщение о необходимости перезагрузить компьютер, нажимаем «ОК» и ждем окончания установки



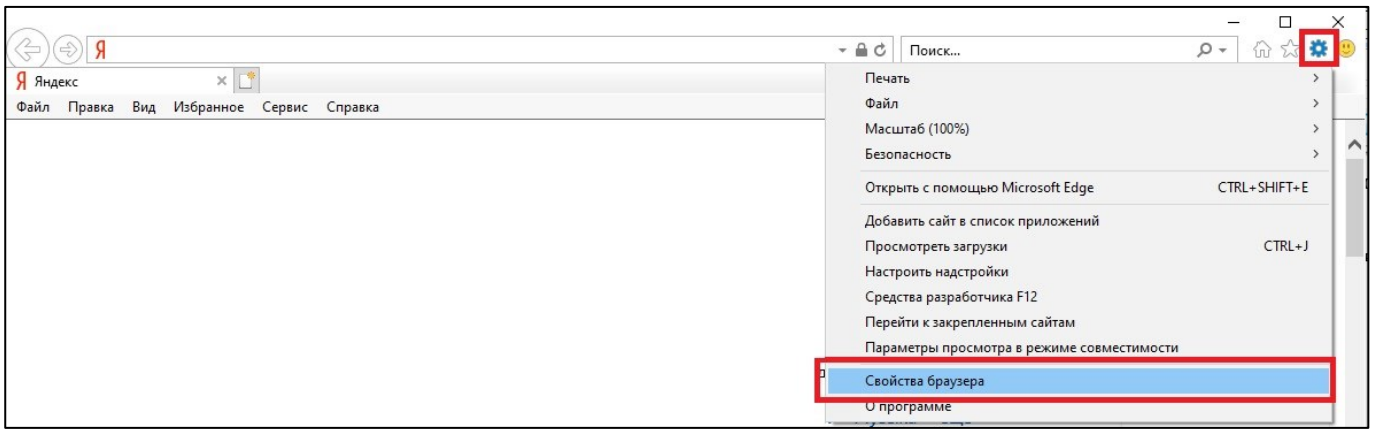


После установки нажимаем кнопку «Ок».

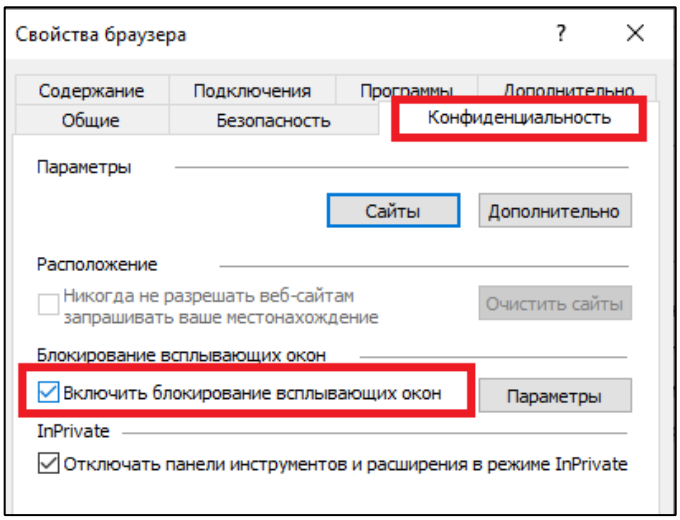
4. Настройка браузера для работы в СУФД Портале

Настройка Internet Explorer 11

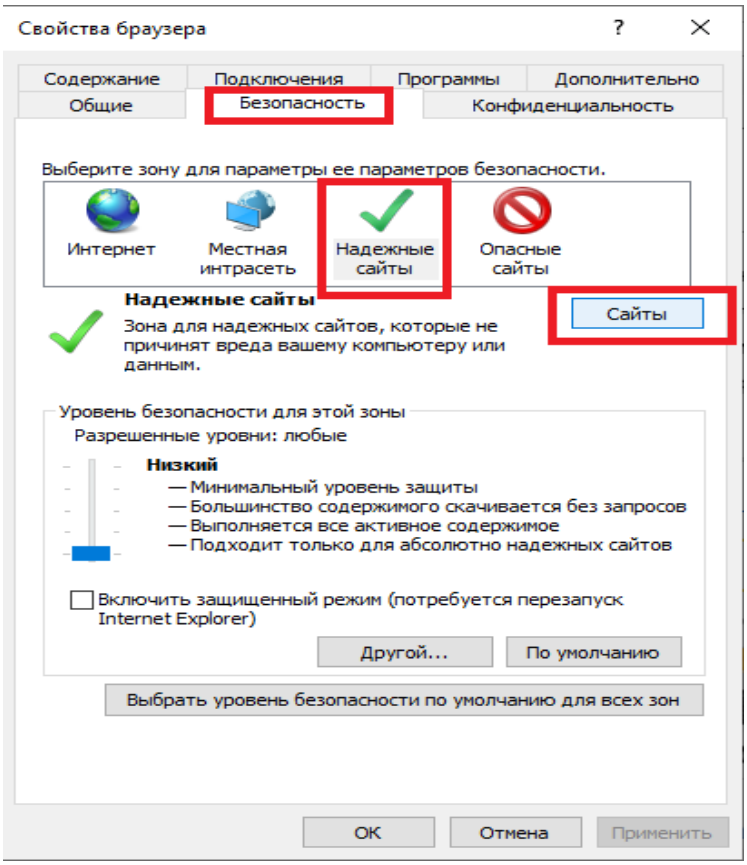
При первом запуске в браузере Internet Explorer необходимо отключить блокировку всплывающих окон. Для этого откройте меню «Настройки» - «Свойства браузера»



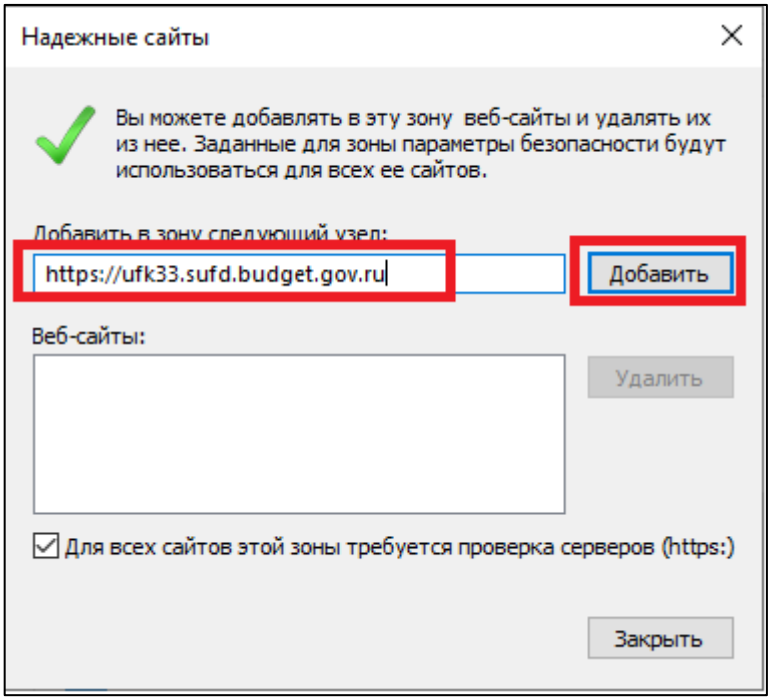
Во вкладке «Конфиденциальность» снять чекбокс с «Включить блокировку всплывающих окон».



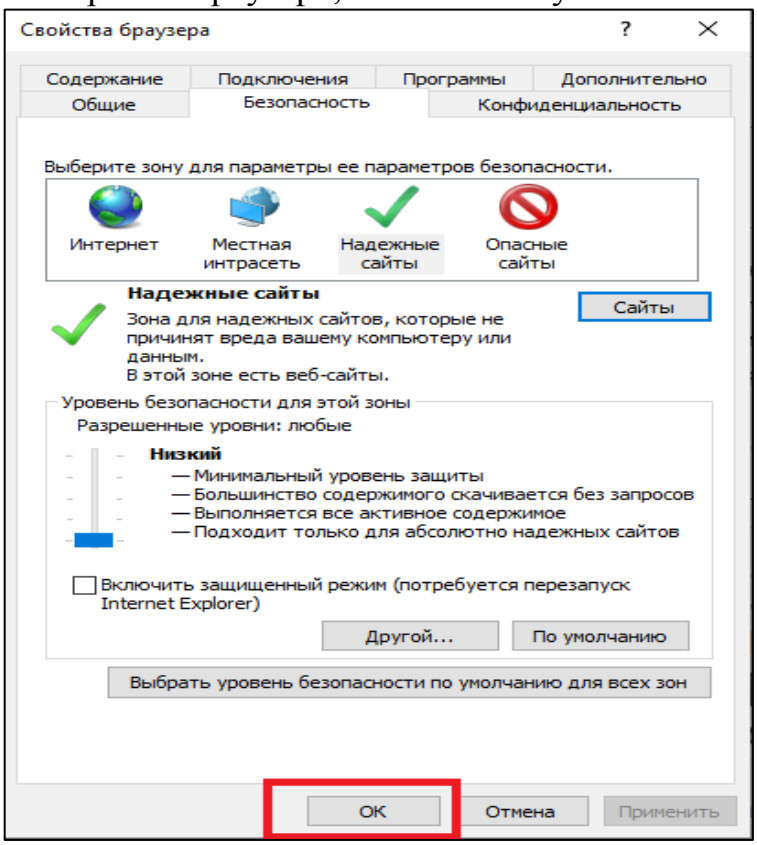
Далее во вкладке «Безопасность» необходимо выбрать «Надежные узлы» и нажать кнопку «Сайты»



В появившемся окне ввести сайт **https://ufk95.sufd.budget.gov.ru** и нажать кнопку «Добавить» Аналогичным образом добавить сайт **http://ufk95.sufd.budget.gov.ru**, предварительно сняв чекбокс с «Для всех сайтов этой зоны требуется проверка серверов (https:)». После этого нажать кнопку «Закрыть».

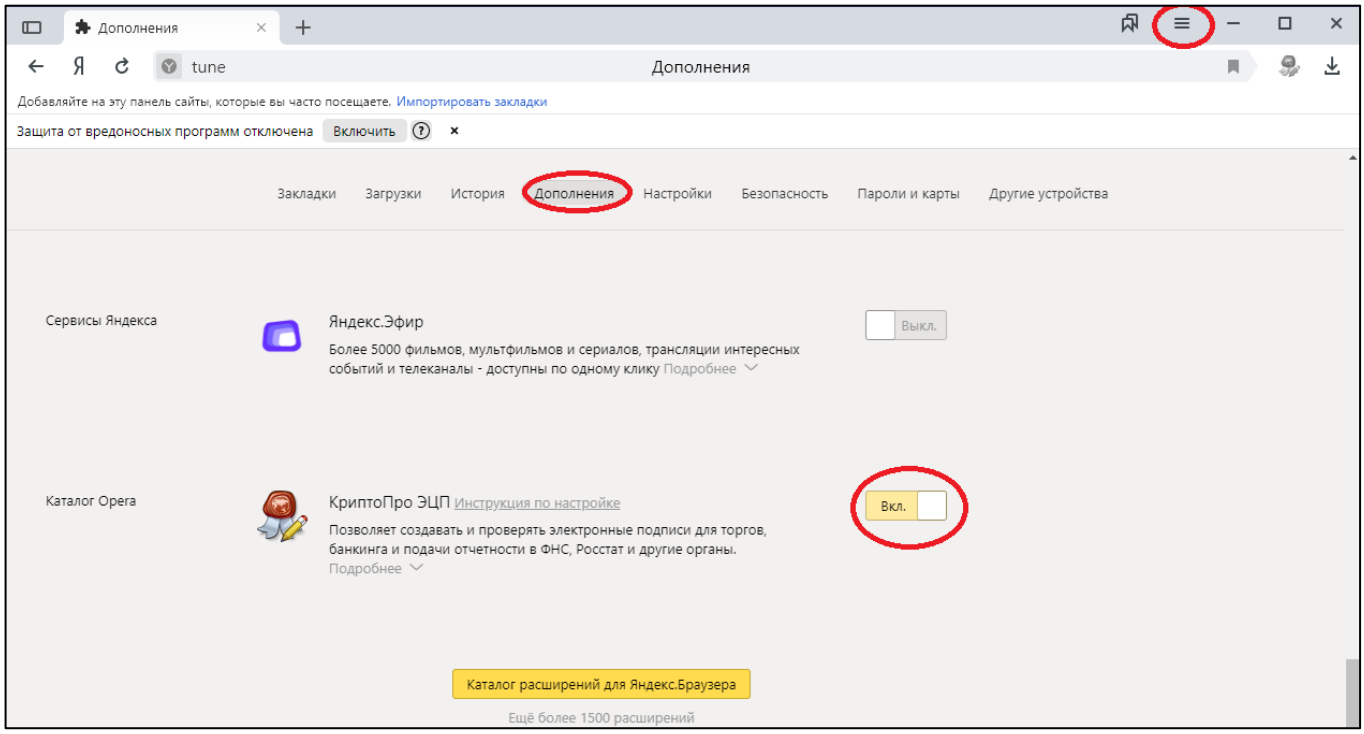


Закрыть окно настройки браузера, нажав кнопку «ОК».

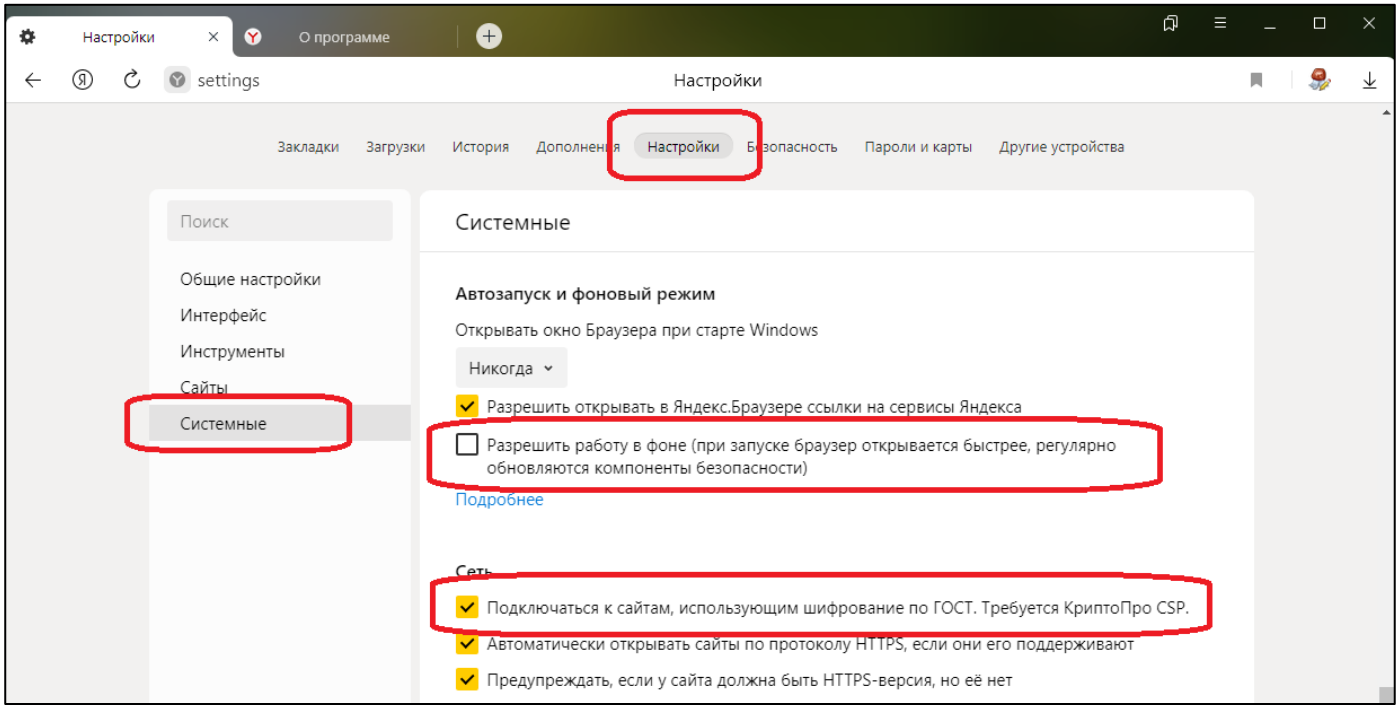


Настройка Яндекс Браузера

При первом запуске Яндекс Браузера необходимо открыть меню настроек « Настройки» - «Дополнения». Из списка выбрать КриптоПро ЭЦП и поставить переключатель на «Вкл».

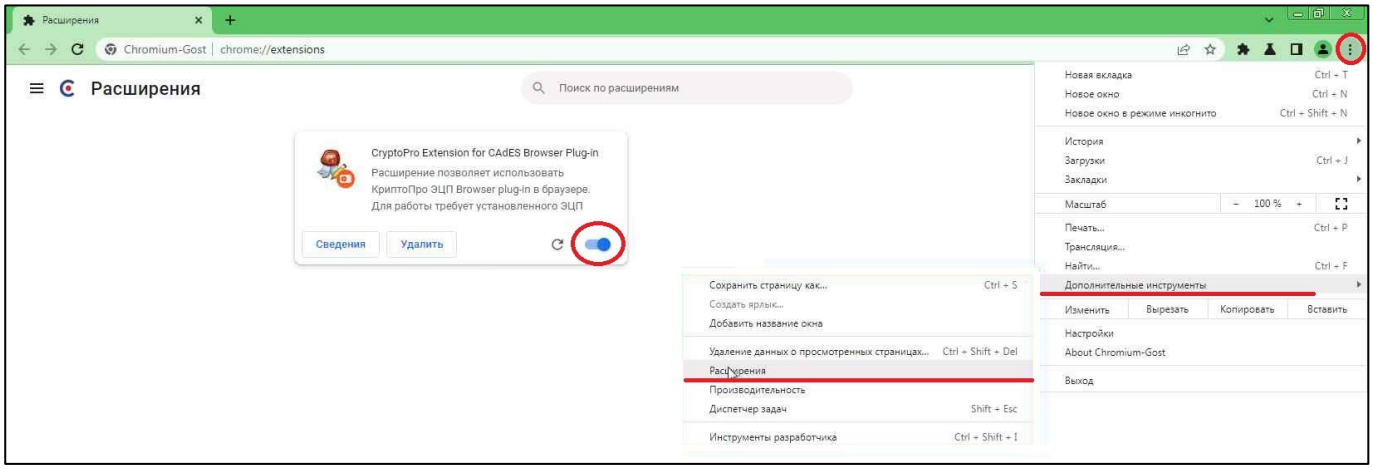


Далее необходимо включить поддержку работы сайтов, использующих шифрование по ГОСТ « «Настройки» - «Системные» поставить отметку «Подключаться к сайтам, использующим шифрование по ГОСТ». А также снять отметку с пункта «Разрешить работу в фоне….»

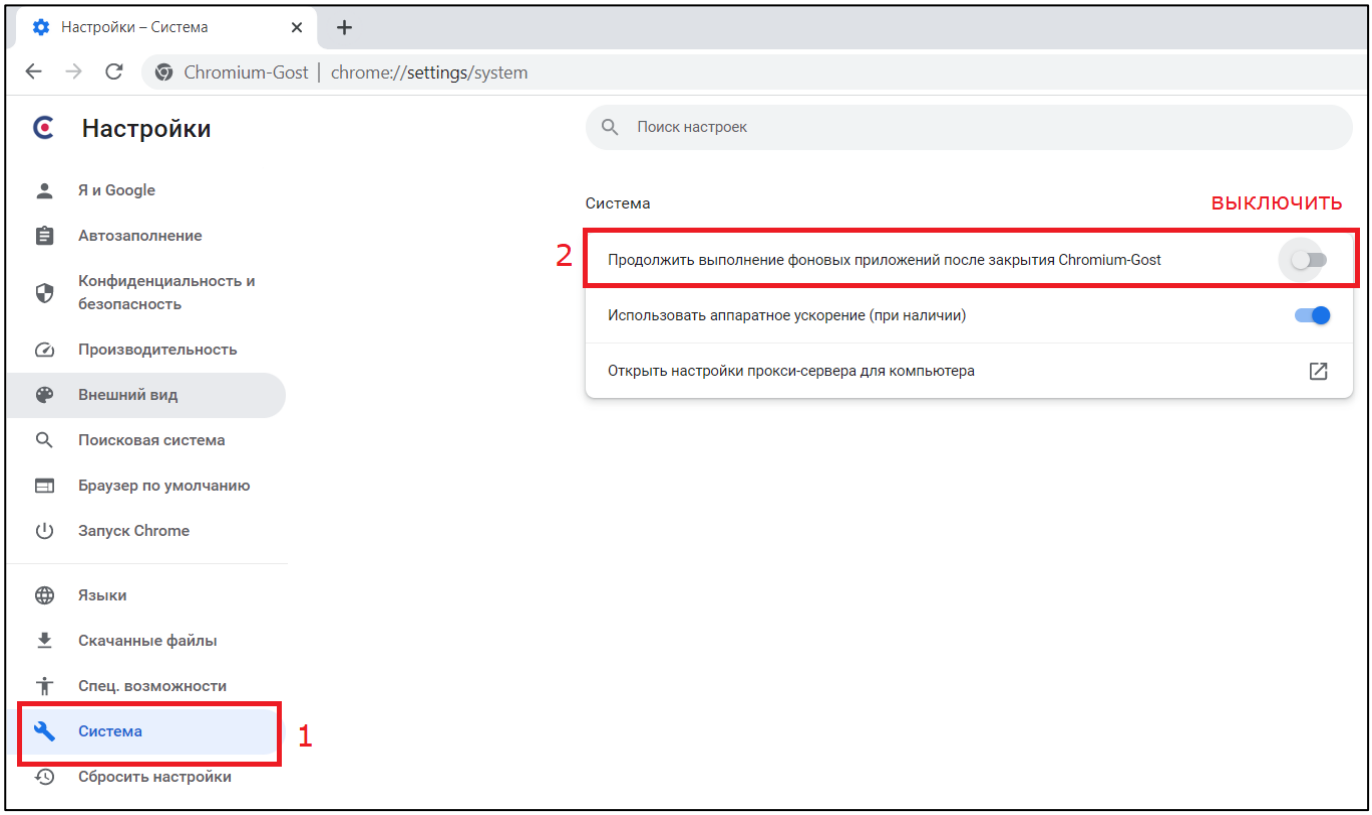


Настройка Chromium-Gost

При первом запуске Chromium-Gost необходимо открыть меню настроек «Дополнительные настройки» - «Расширения». Из списка выбрать CryptoPro Extension for CAdES Browser Plug-in и поставить переключатель на «Вкл».



Также необходимо зайти в «Настройки» - «Система» и снять отметку с пункта «продолжить выполнение фоновых приложений…»



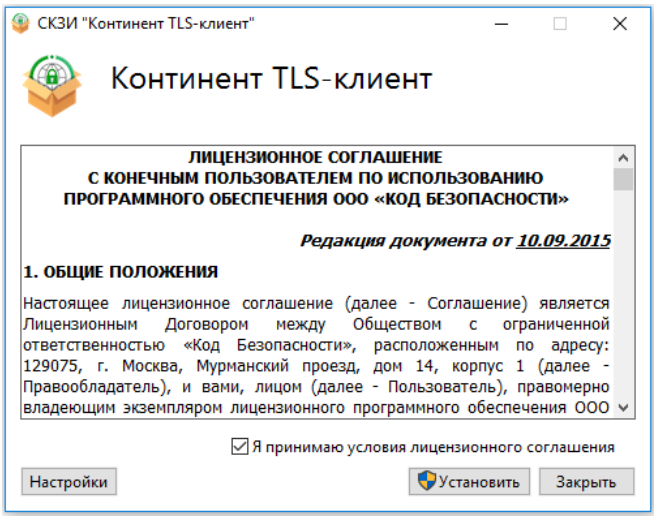
III. Настройка автоматизированного рабочего места клиента для работы в СУФД Портале через «СКЗИ «Континент TLS-клиент» (не обязательно)

При наличии у организации-клиента СКЗИ «Континент TLS-клиент» возможно осуществить его настройку для доступа к СУФД.

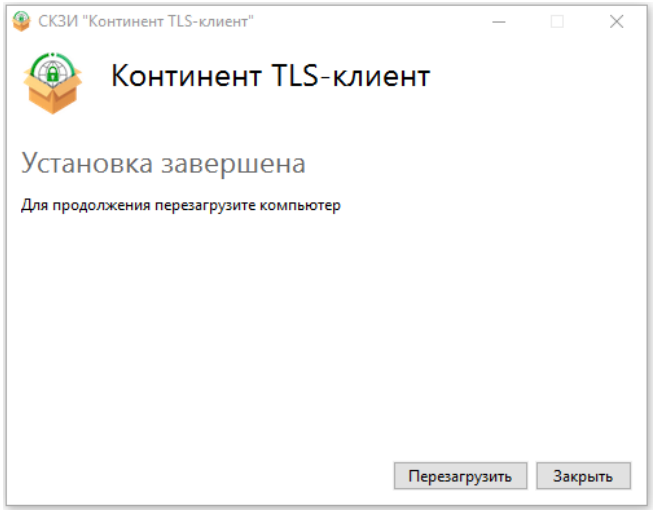
Примечание: Континент TLS Клиент выдавался для взаимодействия с ГИИС «Электронный бюджет».

Для установки СКЗИ «Континент TLS-клиент» необходимо:

1. Запустить файл установки «Континент TLS-клиент.exe»



2. Отметить чекбокс «Я принимаю условия лицензионного соглашения». Нажать кнопку «Установить».
3. Начнется процесс установки.
4. При успешной установке отобразится диалоговое окно «Установка завершена».



5. Нажмите кнопку «Перезагрузить». АРМ перезагрузится.

После перезагрузки необходимо запустить СКЗИ «Континент TLS-клиент», нажав на соответствующий ярлык на рабочем столе

В случае появления окна, информирующего о том, что это демоверсия. Нажмите кнопку «Регистрация». В появившемся окне заполните все поля, отмеченные символом «*». Появится сообщение об успешной регистрации продукта.

1. Настройка «Континент TLS VPN Клиент»

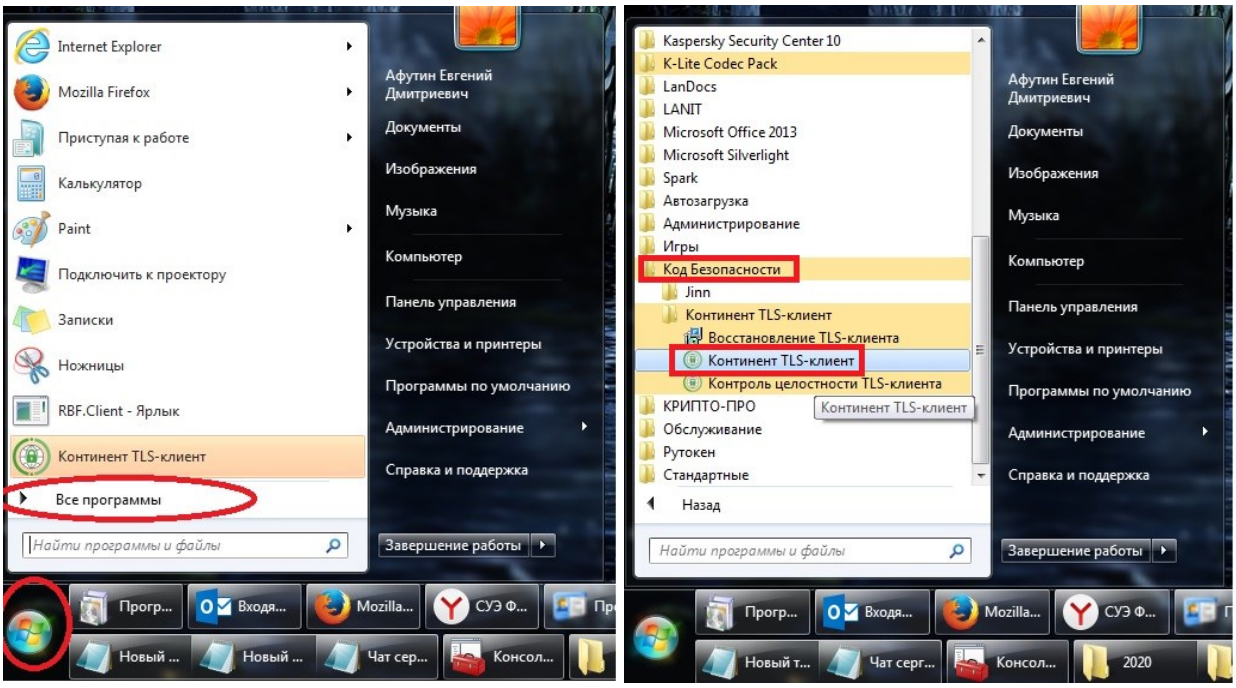
Примечание: настройки, описанным в разделе II также должны быть выполнены.

Для защищенного соединения к СУФД-Порталу через СКЗИ «Континент TLS-клиент» необходимо выполнить следующие настройки.

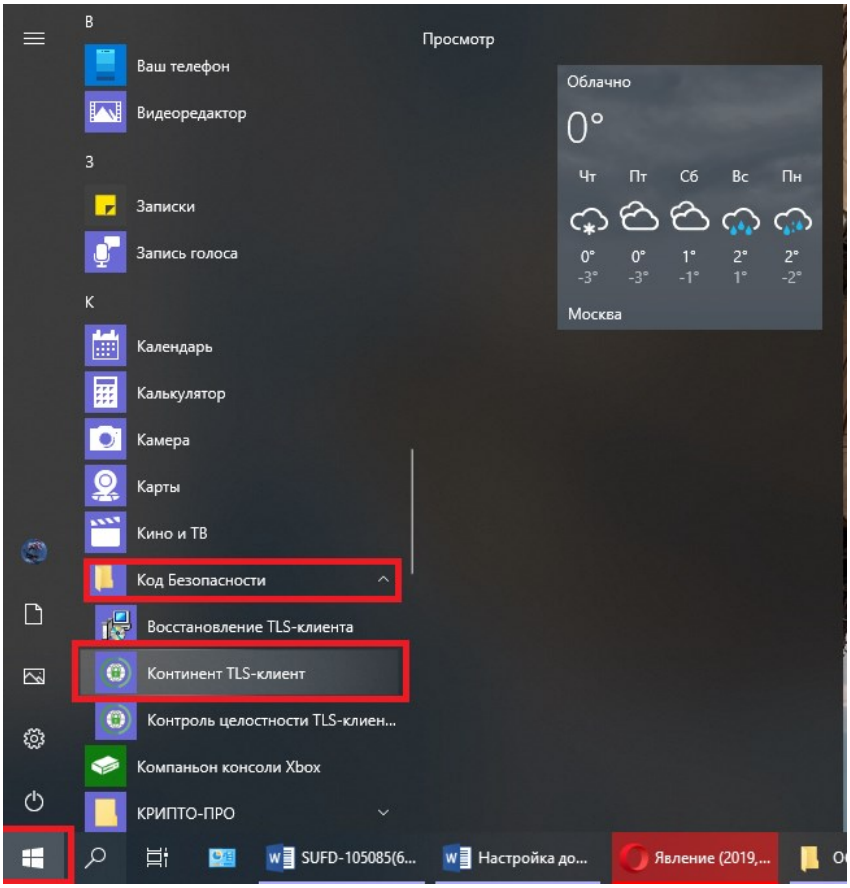
Запустить СКЗИ «Континент TLS-клиент» клиент можно с помощью ярлыка на рабочем столе



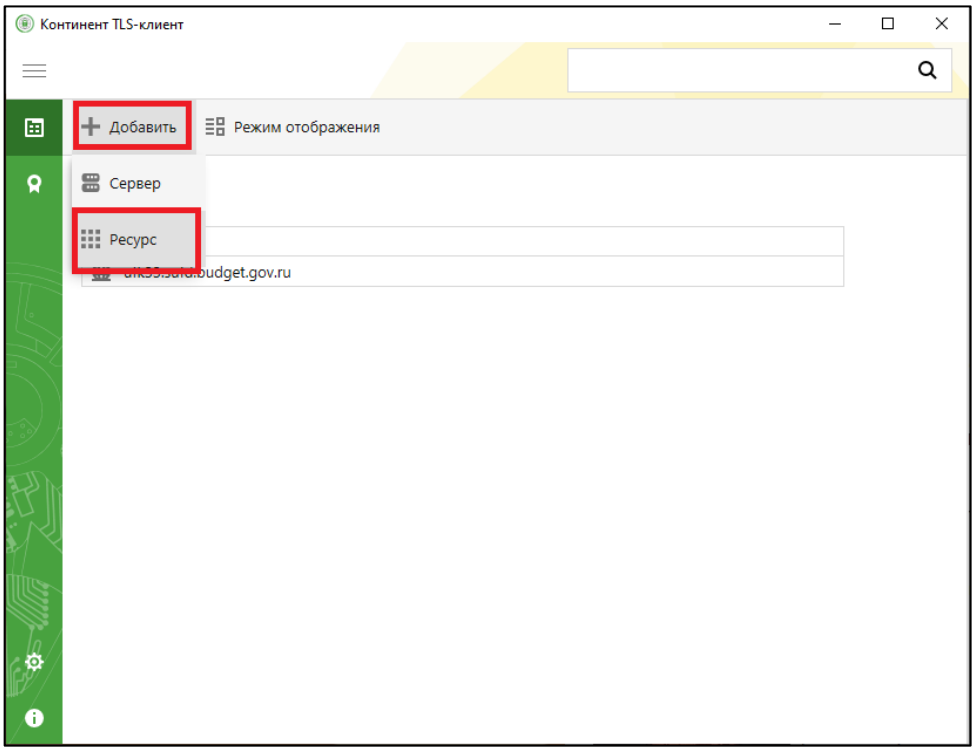
или перейти в меню «Пуск» - «Все программы» - «Код безопасности» - «Континент TLS-клиент»



Если у вас **Windows 10**, то меню выглядит так

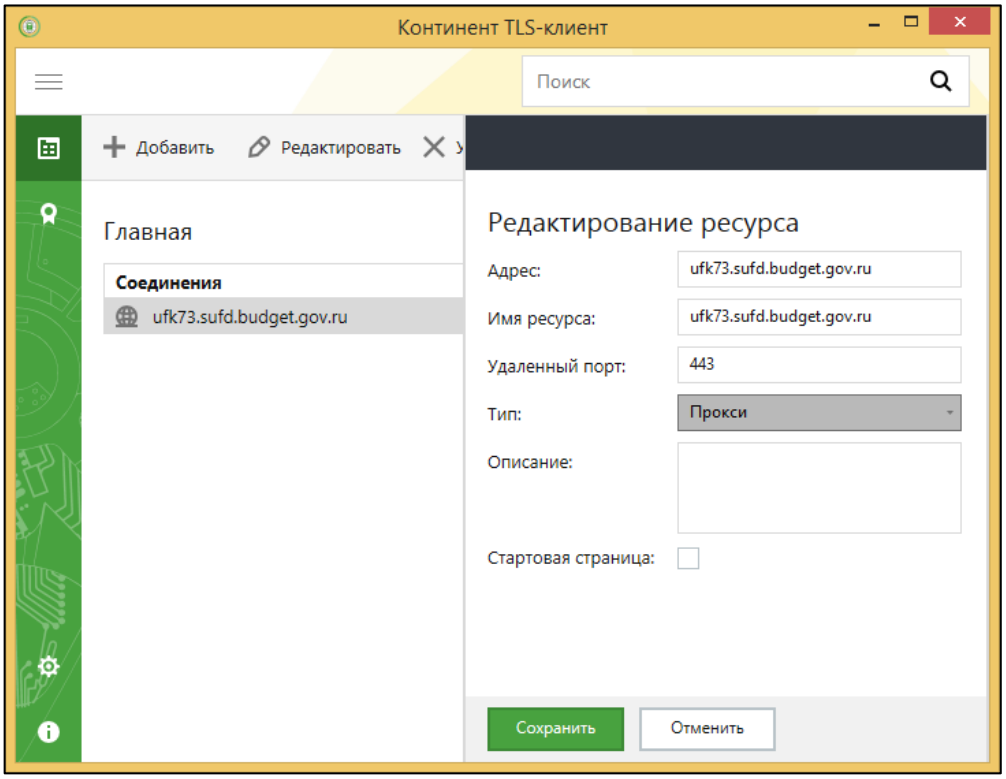


В меню Континент TLS-клиента необходимо нажать на «+ Добавить» и выбрать вкладку «Ресурс»



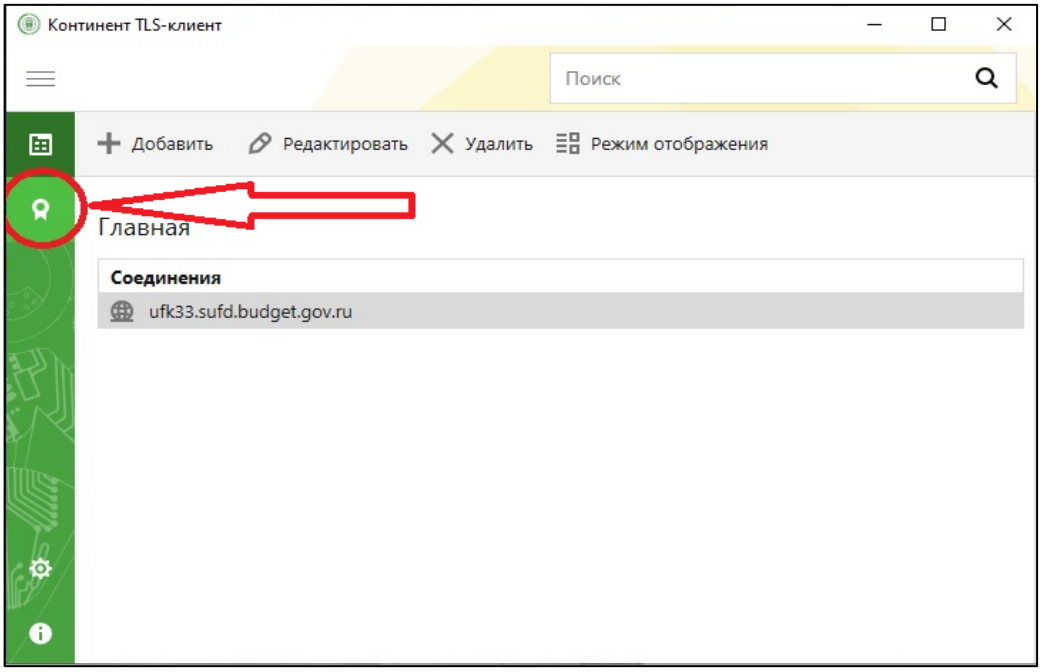
В появившемся окне поля заполняются следующими значениями:

Адрес «ufk95.sufd.budget.gov.ru»;
Имя ресурса: ufk95.sufd.budget.gov.ru;
Удаленный порт: 443.

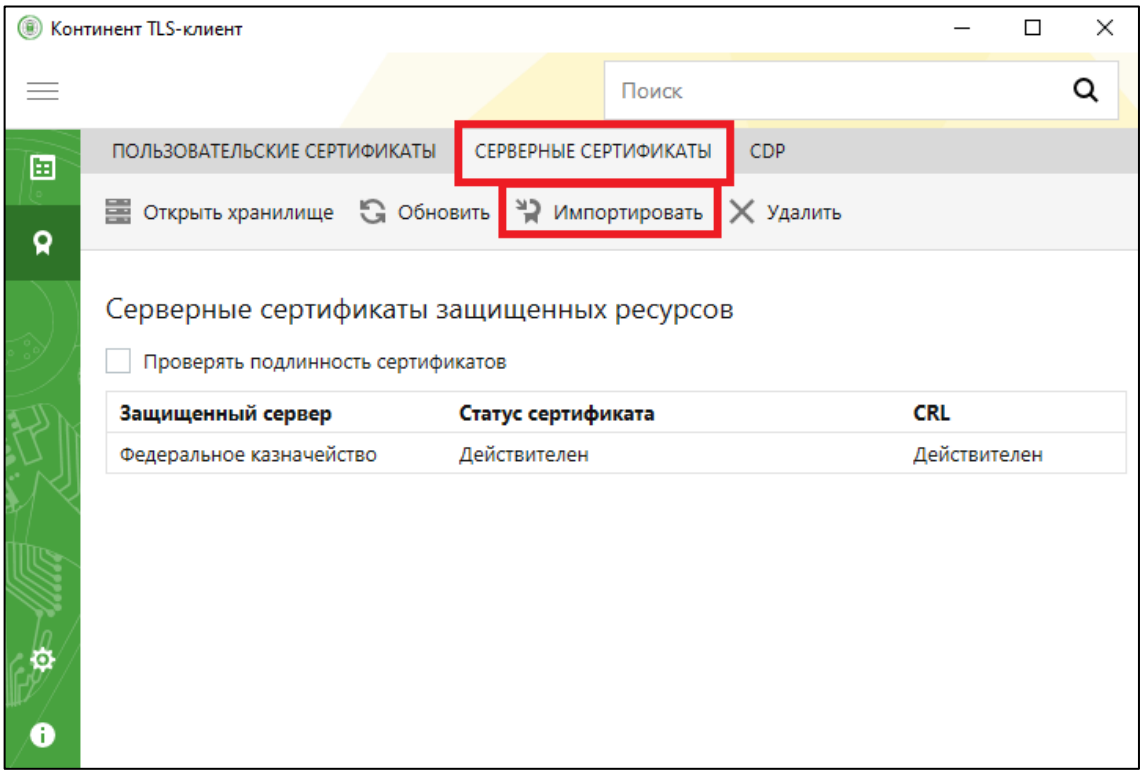


и нажать кнопку сохранить.

Перейти во вкладку «Управление сертификатами»

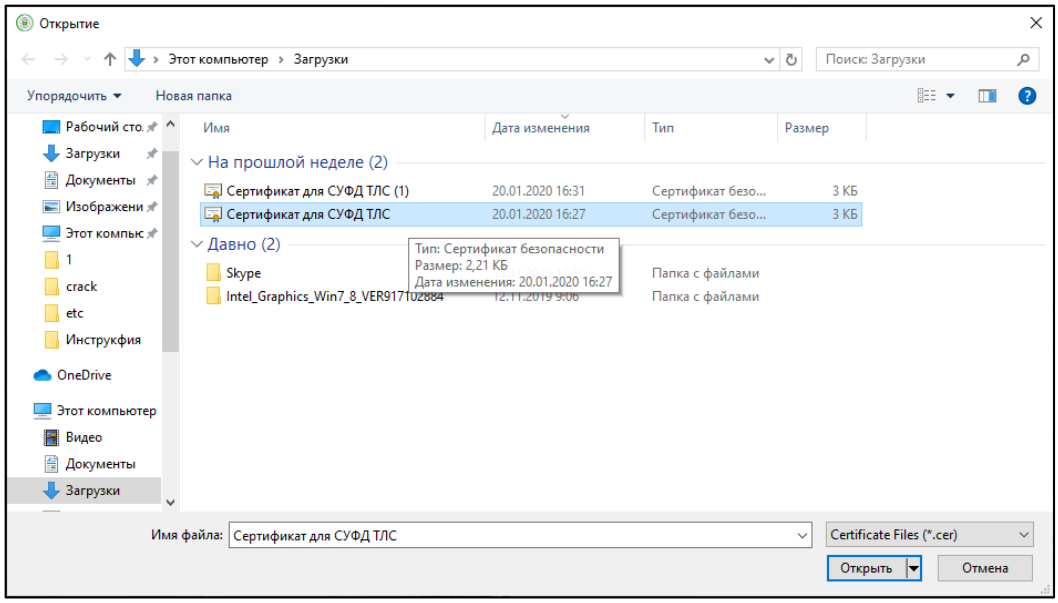


Выбрать раздел «Серверные сертификаты». Нажать на кнопку «Импортировать»

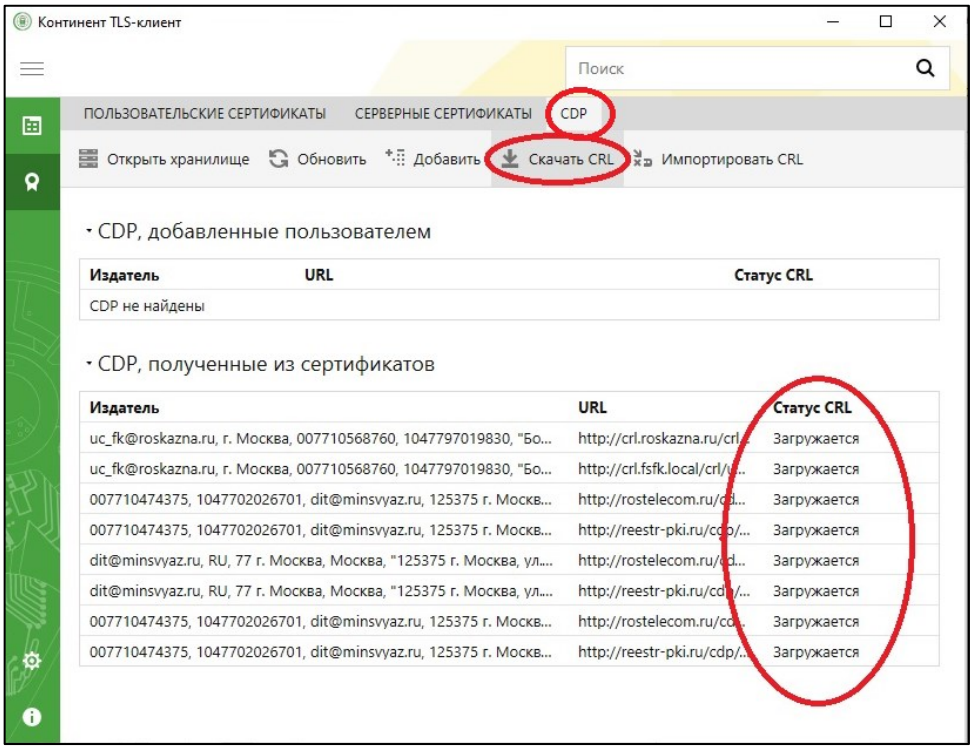


В открывшемся меню выбрать необходимый сертификат сервера для работы в СУФД-портале.

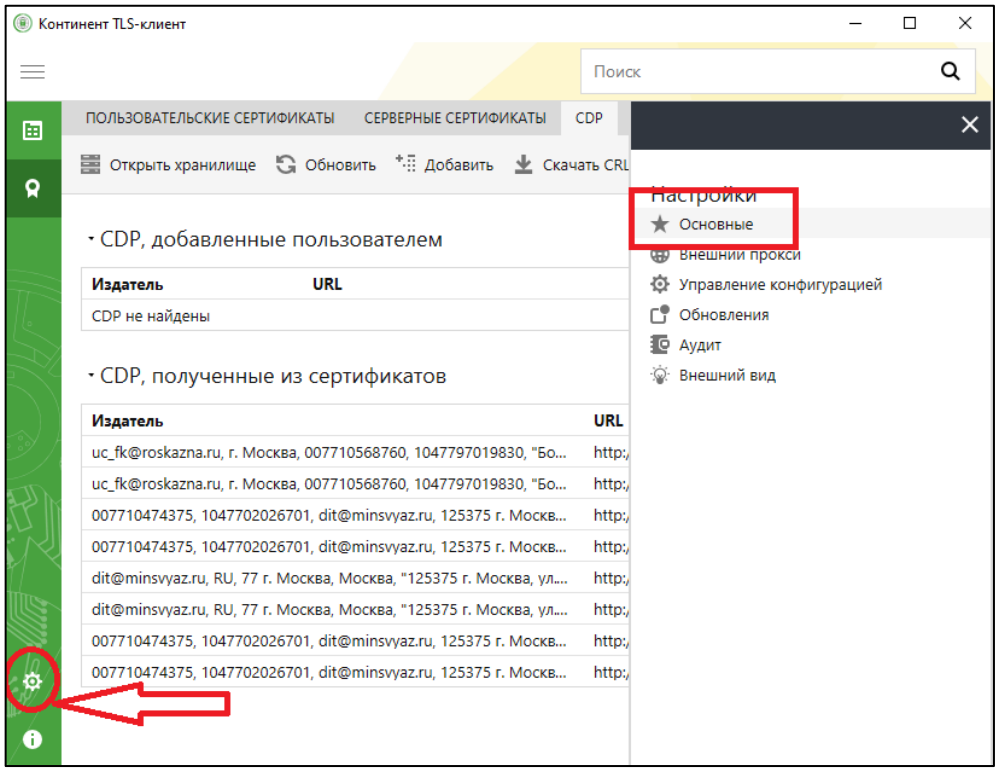
Сертификат сервера СУФД размещен на Межрегионального операционного УФК в сети Интернет (moufk.roskazna.gov.ru) в разделе ГИС/СУФД-онлайн,СЭД.



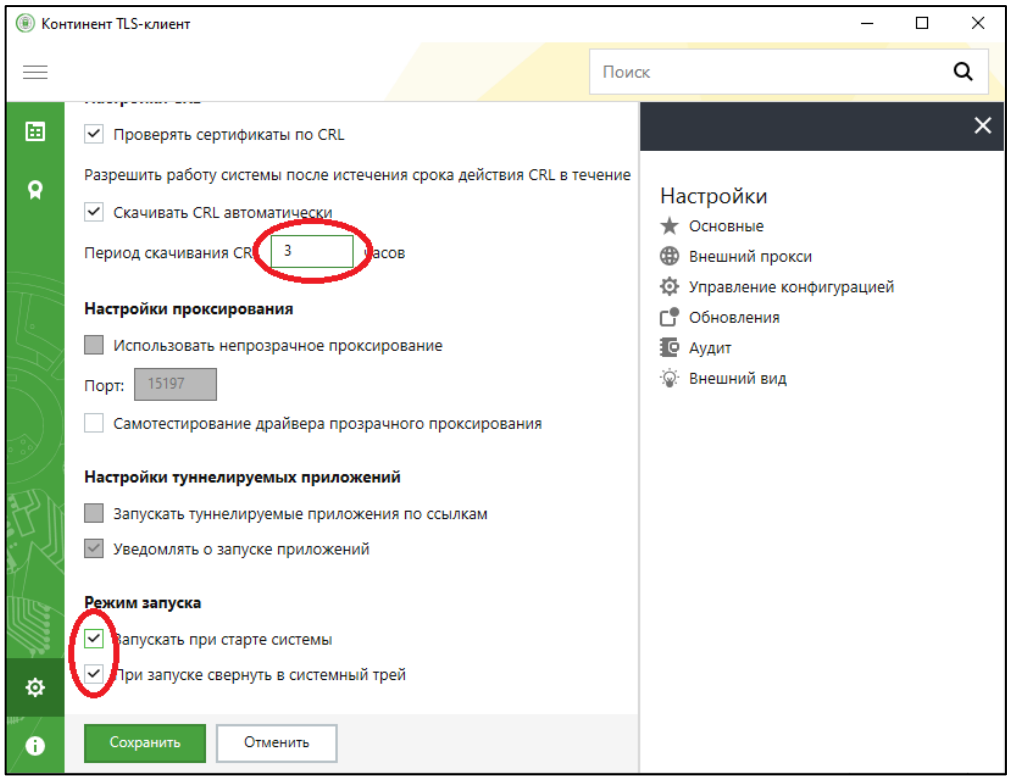
Далее в разделе «CDP» нажать кнопку «Скачать CRL» и дождаться загрузки сертификатов (требуется подключение к сети интернет)



Перейти во вкладку «Настройки» - «Основные»



Указать период скачивания CRL «12 часов» и, пролистав вниз, отметить чекбоксы «Запускать при старте системы» и «При запуске свернуть в системный трей»



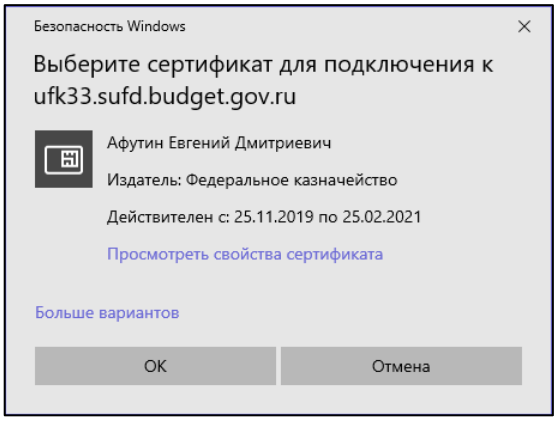
Нажать кнопку сохранить и закрыть окно настройки программы Континент TLS-клиент.

IV. Настройка доступа в СУФД Портал

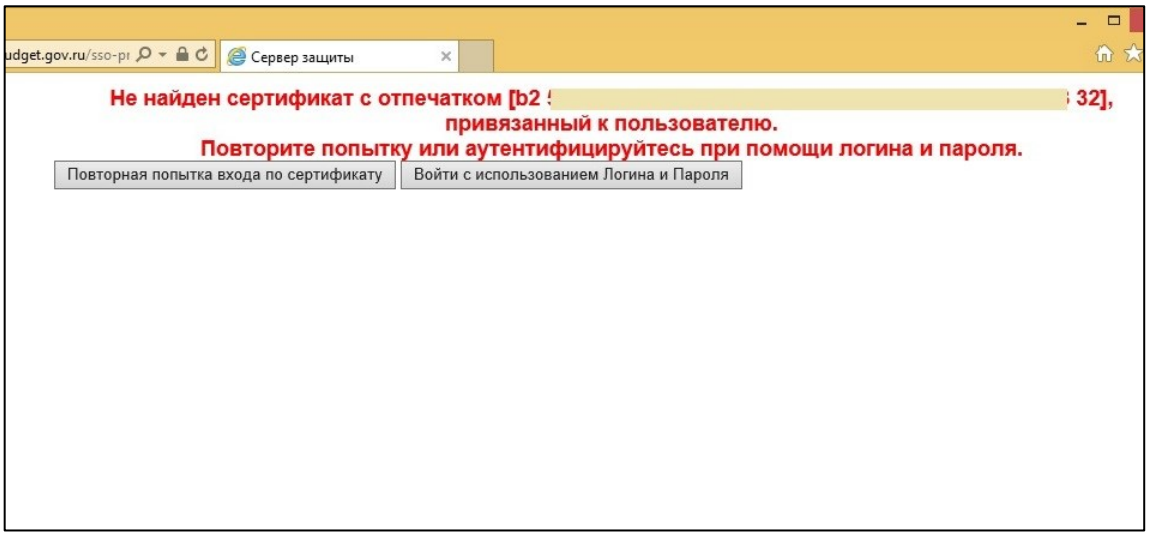
После проведения вышеуказанных процедур вход в СУФД-Портал осуществляется по ссылке:

https://ufk95.sufd.budget.gov.ru

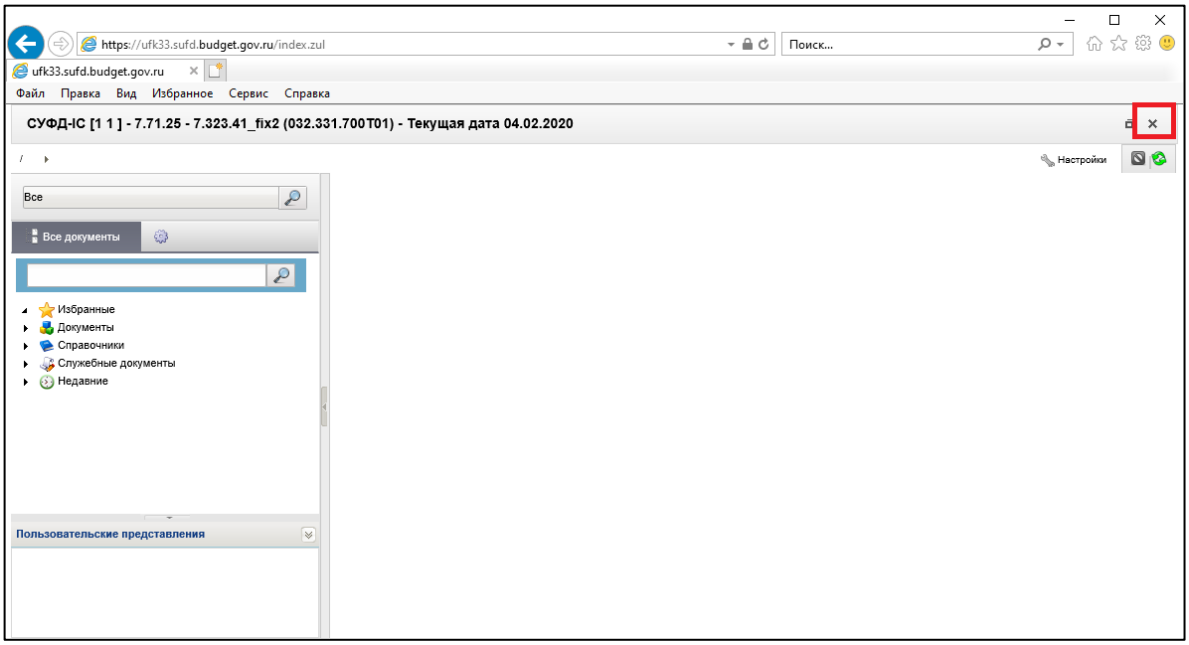
При вводе данного адреса в адресную строку браузера должно открыться следующее окно с выбором сертификата. После ввода пароля откроется стартовая страница **СУФД-Портала**



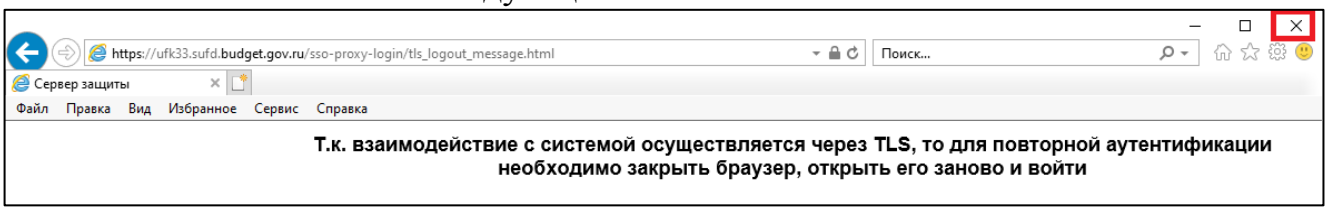
В случае, если сертификат не установлен в систему (например, у пользователей отсутствующих в карточке образцов подписей), необходимо воспользоваться входом по логину и паролю:



Если на рабочей станции в СУФД-Портале работают пользователи под разными учетными записями (руководитель, главный бухгалтер) необходимо сбросить TLS соединение и зайти заново. Для этого, выходим из СУФД-Портала

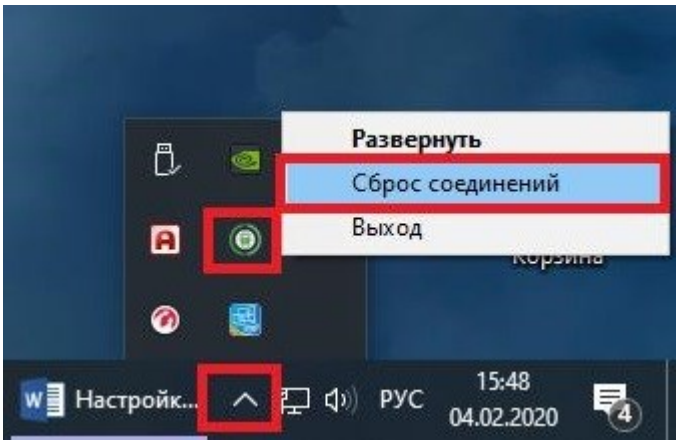


После этого появится следующее окно



Далее необходимо закрыть браузер.
Теперь можно зайти под другим пользователем.

Если используется Континент TLS-клиент, то дополнительно (после закрытия браузера) необходимо в правом нижнем углу нажать **правой** кнопкой на ярлык Континент TLS-клиента и в открывшемся меню выбрать «Сброс соединений»



Одновременно произойдет сброс всех текущих соединений (например, в программе Электронный бюджет).